Accepted version. Final version published as:
Taylor, E. (2016) 'Mobile Payment Technologies in Retail; A Review of Potential Benefits and Risks'. *International Journal of Retail and Distribution Management,* Vol. 44 (2): 159-177

Mobile Payment Technologies in Retail; A Review of Potential Benefits and Risks

Emmeline Taylor

Purpose - Retailers and suppliers are facing the challenge of reconfiguring systems to accommodate increasingly mobile customers expecting multichannel options supporting quick and secure digital payment. This paper harnesses the learning from the implementation of self-checkout and combines it with available information relating to mobile scanning (m-scan) and mobile point of sale (MPOS).
Design/methodology/approach - In review of the literature, the paper provides an overview of different modes of mobile payment systems, and a consideration of some of the benefits that they offer to retailers and their customers. The main focus, drawing upon telephone interviews with retail security professionals in Australia and New Zealand, is on anticipating and mitigating against the potential risks, vulnerabilities and impact on shrinkage.
Findings - With the market being flooded with software and products, retailers are exposed to a compelling case for mobile payment, but it was found that they are not as cognisant of the potential risks.
Research limitations/implications - Further research is needed on the different permutations of mobile POS and how it impacts on the customer journey and rates of internal and external theft.
Practical implications - Suggestions for future empirical research on the risks and vulnerabilities that moving to mobile payment can usher in are provided.
Originality/value – The paper links research from diverse fields, in particular criminology, to elucidate the potential impact of mobile technologies on retail theft and internal technological and process issues, before offering possible solutions.

1. Introduction; Background to Mobile payment in the retail sector

Mobile payment solutions have been much anticipated since the early 2000s but it is only in recent years that their roll out has gathered traction, particularly in the US, Europe and some parts of Asia (Mallat and Tuunainen, 2008). Thus far, mobile payment services have principally been adopted by quick-service oriented industries such as public transportation, service stations, fast-food and beverage vendors. Wider adoption has not been as rapid or widespread as expected (Holmes et al., 2014; Mallat and Tuunainen, 2008) and there are many examples of discontinued mobile payment services such as the SimPay consortium (Ondrus and Pigneur, 2007; Mallat, 2007). Whilst m-shopping sales are relatively modest at

present the industry is gaining pace following improved payment infrastructures in developing markets, and regulatory initiatives to increase non-cash usage and roll-out. In addition, the launch of several new solutions such as Samsung Pay and Apple Pay, digital wallets linking payment cards to mobile phones, are forecast to mainstream adoption. A survey conducted by KPMG found that whilst just 9% of executives in retail, financial services, technology and telecommunications considered mobile payments to already be mainstream, 83% believed they would have seen widespread consumer adoption by 2015 (KPMG, 2011). Worldwide mobile payments volume is projected to grow from $163.1 billion USD in 2012 to $721.4 billion USD in 2017 (Statista, 2015). There is now considerable pressure for industries to rapidly adopt these channels in a way that's attractive and safe for consumers.

Despite the significant changes that m-payment freights into the retail sector, dramatically altering the process by which products pass from retailer to consumer, it has received surprisingly little scholarly attention. As Groß (2015: 222) asserts: 'Whilst m-shopping is steadily gaining popularity, research in the field of m-shopping is still in its infancy'. There is a growing literature inferring the benefits that mobile payment brings to customers, merchants, governments (Raina, 2014), and even to society (Arvidsson, 2014), but a précis overview of vulnerabilities and potential impact on loss is largely missing. The mobile channel represents significant opportunities; diversifying browsing and payment options for customers and streamlining processes for retailers, but it is not without risk. Understanding remains 'fragmented' (Dahlberg et al, 2008) and there is little by way of a research agenda or roadmap. With the market being flooded with software and products, retailers are exposed to a compelling case for mobile payment, but are not as cognisant of the potential risks. High profile incidents have already occurred at mainstream retailers such as Target, which had forty million credit and debit cards compromised in December 2013, along with the personal data of 70 million shoppers, when its MPOS system was hacked. The attack has cost the company in excess of $148 million in breach claims, and potentially more in lost customer confidence and reduced patronage. Improved security has, perhaps unsurprisingly, been identified as a critical success factor for mobile commerce (Raina, 2014; Vrechopoulos et al, 2003) and, similarly, perceived risk by customers has been found to impact negatively on customer adoption (Moth, 2013; Shin and Lee, 2014; Wu and Wang, 2005).

Drawing upon the lessons learnt from the introduction of self-service checkout (SCO), a literature review of the scant academic and industry publications, as well as consultation with a small sample of industry stakeholders, this paper suggests what some of the key areas for consideration might be in order to manage risks and mitigate loss. The paper aims to generate discussion about the potential vulnerabilities generated by mobile technologies in retail, providing a platform from which to investigate the palpability of envisaged security risks, rather than provide an evaluation of specific approaches.

2. Methodology

This paper is based on a literature review of academic research papers, industry documentation and reports. Key search terms were used to search online journals, industry publications and web resources. The search terms included: 'mobile commerce', 'mobile payment', 'm-pay', 'm-pos' and 'contactless payment' to identify literature relating to mobile payment solutions. Reflecting the relatively new adoption of mobile payment in the retail sector, there was a lack of academic literature that specifically addressed loss in its various incarnations. Rather, the focus was largely on the technical aspects of the technology and implementation models (for example see Ondrus and Pigneur, 2006); sales and marketing opportunities; and analysis of stakeholder and customer acceptance (for example see Au and Kauffman, 2008; Mallat, 2007) (Groß, 2015).

In addition to the literature review, consultation took place with senior industry professionals working within loss prevention, asset protection, and business development with a focus on fast-moving consumer goods (FMCGs), predominantly in the food and grocery sector. Ten individuals, representing seven different companies, were consulted in Australia and New Zealand via telephone interview. Due to sensitivities regarding competitors, the interviewees provided insight into their business activities and concerns on the proviso that no identifying information was revealed about them. The interviews took place between mid-August and the end of September 2013 and explored the key considerations for industry stakeholders (primarily retailers) when initiating mobile-payment, particularly in terms of loss mitigation. The interviewees were recruited via a retail consortium focused on loss prevention based in Australia. The security experts provided valuable insight to understanding the possible

vulnerabilities and risks associated with MPOS at a crucial and pivotal time of roll out. They highlighted the pressure to quickly adopt new channels in order to stay relevant, but noted the tension with ensuring that adequate securities were in place. Whilst the sample of interviewees is small, the stakeholders provided vital insight into the tension and difficulties associated with embracing new technological innovation and safeguarding their business against shrinkage, in particular online fraud.

3. Defining Mobile Payment

Phrases such as 'mobile payment', 'mobile commerce' and 'contactless payment' are often used, but in reality these terms can encompass a vast array of scenarios. In essence, a 'mobile payment' is any transaction in which a mobile device, such as a mobile phone, tablet, or PDA (personal digital assistant) is used to initiate, authorize and/or confirm an exchange of financial value in return for goods and services (Au and Koffman, 2008; Blochlinger, 2012). More specifically, mobile payments have been defined as:

> [A] type of electronic payment transaction procedure in which at least the payer employs mobile communication techniques in conjunction with mobile devices for the initiation, authorization or realization of payment (Au and Koffman, 2008: 141).

> [A] transfer of funds in return for goods or services in which a mobile device is functionally involved in executing and confirming payment (Raina, 2014: 186).

There are many different types of mobile payment, but the technologies used to deliver them can broadly be categorised into two main types; remote m-payments and proximity payments (Agarwal et al, 2007). Remote payments require customers to register for a service, usually involving the download of an application, and then use it on their mobile device to pay for items. Customers may have value stored in a prepaid account or draw funds directly from a bank account. Payment service providers (PSPs) such as Google, PayPal, and GoPago use a cloud-based remote approach to in-store mobile payment. Alternatively, proximity payments require the customer to present a credit card, mobile phone or tablet device at a payment terminal, usually holding it within a few centimetres, in order to complete the transaction. The payment is facilitated by Near Field Communication (NFC) and is often referred to as a 'contactless payment'. In order to further clarify the confusing and rapidly expanding mobile

payments market, a distinction has been drawn between three categories; mobile commerce, mobile acceptance and mobile wallets (J.P. Morgan, 2013).

Mobile commerce, a subset of e-commerce (Coursaris and Hassanein, 2002), is conducted over a mobile device enabling the 'the delivery of electronic commerce capabilities directly into the consumer's hand, anywhere, via wireless technology' (Global Mobile Commerce Forum, 1997). It currently represents approximately 12% of total e-commerce sales in the US and is steadily growing (comScore cited in J.P. Morgan, 2013). *Mobile payment acceptance* refers to the conversion of a mobile device (e.g. smart phone, tablet or PDA) into a POS system by fitting it with temporary or permanent hardware enabling the retailer to accept card-based payments. For example, a store device, such as a magnetic strip reader, can be connected to a customer's smartphone, often via the audio jack, to create an external bar code scanner or to process payment from a debit or credit card. The *mobile wallet* can be defined as an application hosted by a mobile device that enables customers to use it for payment instead of a credit or debit card. There are a number of different wallet providers, some using proximity technology such as near-field communication (NFC), either embedded in the device or a sticker, while others are remote or cloud-based.

4. The case for mobile payment: innovation, benefits and opportunity

Mobile payment instruments have the potential to redefine bricks-and-mortar stores; making checkout simpler and faster, as well as integrating the online channel into the store for improved inventory control, marketing, reward schemes and customer service. Yang (2010) has outlined several ways in which m-shopping can optimise customer experience in brick-and-mortar stores, including: providing a customized, real-time interaction channel between retailers and consumers; delivering non-intrusive tailored mobile marketing; assisting customers in making smart purchasing decisions; as well as facilitating many retail processes, including payment. The advent of m-shopping is regarded as 'a green field opportunity' (Interviewee 9), and furthermore, one that needed to be embraced if retailers were to stay relevant and current. As one security manager explained:

> It's a prime opportunity to move to mobile. Stay with fixed POS and it'll be costly. The mobile platform is agile and can be combined with other technologies - another reason why moving to m-pay is advantageous. (Interviewee 6).

Industry and trade publications reflect the excitement about the sales and marketing opportunities that MPOS can offer. As an integral part of multichannel retail, mobile technologies can provide a range of touch points to connect with, entice and retain customers. Fiore and Kim (2007: 421) assert that contemporary 'shopping experiences involve more than consumer acquisition of goods' and mobile devices offer functions not available with plastic cards, such as using geo-location technology to alert consumers of deals at nearby stores. In other words, mobile retailing is perceived to be 'a large-scale game changing innovation' (Interviewee 2). MPOS brings myriad ways in which the retailer can build services around the transaction, such as automated offers, reviews and feedback, targeted marketing, 'check-ins' and social discovery.

There was a clear sense from consultation with industry stakeholders in Australia and New Zealand that the introduction of mobile payment technologies was driven by the customer looking to instil a more hedonic and convenient element to the utilitarian nature of shopping:

> The shopper is looking to enhance their experience. Shoppers now have less time and they want a more convenient and easier way of doing things. You have to make experience pleasurable and that's what we try do we do (Interviewee 8).

> It's [a] demand driven thing … Different sectors have a lot of other MPAY types e.g. bus tickets, Starbucks™ in the States, whole apps for different retailers (Interviewee 3).

The consensus amongst interviewees was that there was a compelling case for diversifying payment options beyond traditional staffed checkouts and SCO, and that there was a certain inevitability to mobile technologies; 'the end game is that one day, in one or two years time, it'll all be shopped on mobile and paid on mobile' (Interviewee 5). Some of the main benefits

of mobile payment options include margin improvements, increased conversion, enhancing loyalty programs, and real-time analytics.

Staff costs often exceed 20 percent of retail sales (ONS 2005) and so the productive use of labour is a critical issue for most retailers. As with SCO, there is the potential for retailers to use MPOS as a way to leverage savings on staff and given the relatively high costs of staff in some countries such as Australia[1] this was particularly pertinent for interviewees. For example, it has been estimated that it costs USD $1 to check out a USD $100 spend. If one store clerk can effectively manage four or more SCO lanes, 75% or more of that cost can be returned to the bottom line for each transaction completed (IBM, 2008). Rather than an overall reduction in staff, retailers can redeploy staff to perform value-added customer service that increases sales (Haas and Kenning, 2014). The potential to reinvest staff time into the provision of a range of services for customers was viewed as a key benefit amongst stakeholders.

MPOS can streamline the shopping experience for the customer by not only providing enhanced information about a product (details, reviews, availability etc.), but by being able to complete the purchase immediately on the shop floor without having to queue or find a payment station. There was consensus amongst stakeholders that this held great promise for driving sales conversion. In addition to payment, mobile systems can be used by retailers to collect feedback customer behaviour and feedback to enhance customer relationship management (CRM). One interviewee highlighted the integration of loyalty programs and offers with an increased mobility for customers was the main benefit for the food and grocery industry; 'payments and loyalty info is brought together into a single spot' (Interviewee 2). In summary benefits relate to the use of customer-owned mobile devices as virtual shopping assistants, the increase in the number of touch points through which retailers can communicate with their customers, and the ability to compile rich consumer profiles for precision marketing. Despite the purported benefits, the use of mobile payments by the retail sector has been forestalled by the uncertainty of their advantages. In particular there are a

[1] At the time of writing the full-time adult minimum wage was $16.37 per hour or $622.20 per week in Australia, compared to £6.31 per hour ($10.65 AUD) in the UK.

number of issues around consumer adoption and whether they can deliver on promises of convenience, versatility and most importantly, security.

5. Identifying Vulnerabilities, Problems and Risks

Available information on MPOS and multichannel retail has largely focused on the positive marketing and sales opportunities they present. In a review of the literature relating to mobile shopping, Groß (2015: 232) identified that most 'studies suffer from a pro-innovation bias', and in order to 'overcome that deficit, potential obstacles have to first be identified'. There has been little written about implementation processes and best practice, and virtually nothing pertaining to the impact on shrinkage and how to respond with loss mitigation strategies. Despite consistent findings 'that consumers are highly sensitive to issues of […] risk, privacy, network security, transaction protection, and trust' (Groß, 2015: 226), as outlined in a number of studies (see Kim et al., 2009; Wong et al., 2012), there is little understanding of the risks involved with m-shopping, particularly in terms of shrinkage and fraud. In consultation with the security experts working in loss prevention for large national retailers in Australia and New Zealand, there was a clear sense that new technologies had to be embraced if the company was to stay relevant, and this always involved risks. As one security manager stated 'evolution is really about managing risk. Otherwise you would never do anything different' (Interviewee 1).

Costing the industry an estimated USD $119 billion annually, shrinkage has been defined as 'intended sales outcome that was not and cannot be realised' (Beck and Peacock, 2009). It is typically categorised into four main sources: External theft, Internal theft, Internal errors / Process or administrative errors, and; Inter-company fraud, but there is little consensus on which of these accounts for the most loss (Chapman and Templar, 2006). The Centre for Retail Crime's Global Retail Theft Barometer (GRTB) finds external theft to be the biggest contributor to loss (43.2%), followed by employee theft (35%), internal error (16.2%) and inter-company fraud (5.6%). However, the National Retail Security Survey (NRSS) places employee theft at the vanguard, as does the National Retail Federation, 2011.

A certain amount of trial and error was involved at the point of implementation, as one security manager stated 'it might be a "suck and see" process' (Interviewee 1) whilst another,

in reference to key learning from the implementation of SCO, cautioned that the use of MPOS had to emerge using 'stepping stones' and 'not a big bang' transformation due to the level of unknown (Interviewee 9). There was a sense that current security practices would provide a level of safeguarding for new processes: 'with any new technology there is inherent risk that exists specific to that technology, but a lot of what we are already doing will help' (Interviewee 4).

In assessing the introduction of mobile payment, it is envisaged that it could have a particular impact on two sources of shrink; 'External theft' and 'Process or administrative errors'. The latter is broadened to include technological issues that occur with mobile scanners and MPOS (such as network/Wi-Fi interruption, battery failure and inability to scan items), and in order to capture these, is renamed 'Internal technological and process issues'. In terms of inter-company fraud, there is little to suggest that mobile technology should have any impact. However, the validation technologies and processes potentially implemented to enable the use of MPOS payment options might result in a diffusion of benefits that reduces the incidence of inter-company fraud through ease of detection. However, the category of 'fraudulent activity' is added to reflect the potential for fraudsters to take advantage of the mobile channel. There are also concerns around MPOS that are not directly related to shrinkage, but will have an impact on store profitability and bottom line. An additional risk category 'Brand protection and consumer confidence' is included in this paper. This covers the important area of ensuring consumer confidence in new technology systems, such as effective security mechanisms and respecting customer privacy and data protection.

5.1 External theft

There are many different techniques used by shoplifters (see Hayes and Cardone, 2006; Gill, 2007 for an overview of commonly used strategies) that are 'limited only by the imagination' (Hayes and Cardone, 2006: 305). A rough distinction can be drawn between techniques that attempt to conceal the item to be stolen, and those that do not. Many studies show that concealment usually occurs throughout the store; in the aisles or in a blind-spot (Gill, 2007), and not at the checkout where security mechanisms are often focused. However, 'self-checkout fraud' (customers not scanning items, or scanning an item for less than its price) does occur. Furthermore, a correlating decrease in staff (as occurred with SCO) reduces the

number of 'capable guardians' (Felson, 1994: 30) that can identify, and importantly intervene, when an item has been misappropriated.

Mobile scanning and MPOS increase the autonomy of the customer, with some systems relying on them to correctly scan all items selected for purchase. The focus is 'on a shopping experience' as one security manager contended; 'it's got to be easier, convenient, a smaller queue, in and out of the store in no time at all. But within that there is a loss element – if we're making it easier and more attractive to shop, well, what happens to loss?' (Interviewee 8). If mobile technologies make things easier for legitimate shoppers, they might also be creating opportunities for 'aberrant consumer behaviour' (Bamfield, 2012: 39). As Lo (1994) argues 'like shopping preferences, the key in shoplifting behaviour [is] accessibility to opportunity'.

Since the autonomy for scanning and payment has opened up a new avenue by which shop thieves can conduct their offence, a key question for criminologists and security experts is whether this represents 'tactical displacement' (Repetto, 1976; Hakim and Rengert, 1981), whereby those with criminal intentions simply steal by a different means. If this is the case, there will be no real net change in the amount of store theft. However, if new scan and payment systems open up a window of opportunity for a new cohort of thieves that otherwise would not have stolen goods, then a store could expect their overall shrinkage rates to increase. Furthermore, it would appear that whilst some individuals enter the store with the intent of stealing other customers are leaving with goods they haven't paid for due to frustration or difficulty with the interface. As new methods of scanning and payment are launched there is the potential for a heightened level of theft occurring due to difficulties in operability. In a recent survey of nearly 5000 customers, it was found that a sixth admitted to being dishonest when asked to enter an item manually (reported in Harding, 2012).

One industry report suggests that use of smartphones as payment devices may actually decrease the risk of customer theft from retailers, since authentication and authorization processes may become more sophisticated than those of existing payment methods (Medich et al, 2011) as consumers demand greater protection. However, mobile technologies used for scanning (whether on a store or customer-owned device) throw open the possibility of

scanning as the customer navigates the aisles. The issue that arises here is that loss prevention and security methods that have built up around having a specified area for scanning and payment are no longer as relevant in the mobile retail world. Surveillance becomes difficult and control is potentially ruptured. There is a need therefore to establish new means of verification, which is further explored below.

5.1.1 'Walking'

It has been suggested that SCO increases the occurrence of 'walking' whereby a thief leaves the store with goods they have not paid for without any attempt to stop at SCO or staffed lanes to make payment (Bamfield, 2012). The reason for this relatively brazen technique of shoplifting is that the SCO aisles are often designed to enable the free flow of customers through them, often accompanied with a reduced staff presence. As such, the self-service area may permit thieves to exit more easily, particularly if staff are occupied with another customer. Research has often shown that thieves will deliberately create disturbances or distract store staff in order to facilitate an accomplice stealing items (for example, see Bamfield, 2012; Gill, 2007). In terms of SCO this is easily done by requesting help from the store clerk enabling the thief to walk out of the store, as has been reported in previous studies (Beck, 2011). In terms of mobile scanning and payment, this could equally present an opportunity to thieves if they are channelled through relatively unmonitored spaces to process their items. However, it is worthwhile recalling that if MPOS simply replaces the use of a credit or debit card at the checkout, mobile payments should not impact on the likelihood of theft. It could however, contribute towards the 'mime of payment', i.e. a 'customer' presents their mobile device to the NFC scanner and acts as thought the value of the purchase has been debited but this could already be acted out using a card payment or even cash. Techniques of verification will be paramount to ensure that staff are alerted when a customer attempts to leave the store with items that have not been paid for.

5.1.2 'Sweethearting'

'Sweethearting' refers to the unauthorised giving away of goods without charge to a "sweetheart" customer such as a friend, co-worker or family member. It has been estimated to cost the industry nearly $80 billion dollars annually (Brady et al, 2012). There is a lack of research exploring the prevalence of sweethhearting but a recent National Retail Security

Survey (2011) provided estimates on the level of theft via collusion between employees and customers. According to the survey, 96% of the 140 retail companies surveyed reported some incident of internal theft through collusion with someone who was not an employee of the company. Further demonstrating the prevalence of this type of theft, a 2012 survey of 800 customers and employees found that 67% said they had participated in sweethearting in the previous two months (Brady et al, 2012).

Collusion theft is particularly hard to detect. Some stores employ security guards or other staff to periodically check customer receipts at exits, but this can impact on the positive customer experience for legitimate shoppers who feel unduly accused by the process. A more technical approach involves computer-aided algorithmic software to monitor checkouts and flag when items have not been scanned. Suspicious behaviours such as stacking items on top of one another, covering up the barcode or bypassing the scanner and placing the item directly into a shopping bag are typical sweethearting techniques. However, the onset of mobile scanning and paying in-situ decreases the ability of wrap-around security features monitoring transactions as outlined above. Whilst normally considered the purview of staffed checkout, mobile technologies could continue, or even heighten the risk of sweethearting where there is interaction between customer and staff at payment and validation stages.

5.2 Fraudulent activity

Mobile payments are still in their infancy and as such the true extent of fraud issues has yet to be defined, but the consultation revealed this to be a key focus. However, the industry stakeholders reported feeling largely confident that new technologies and methods of payment would not be rolled out until there was certainty that they were safe and secure; 'mobile payment applications will have gone through the due diligence of ensuring it is a secure site. The last thing we want is to end up on *Current Affairs*. [We are] very diligent in terms of credit card fraud and payment' (Interviewee 2). It has been predicted that more fraudsters will migrate to the mobile channel because the security protocols are not yet as mature as e-commerce or in-store payment (Hayes, 2013), thereby presenting 'lower hanging fruit for attackers' (Frisby et al., 2012: 10). There are many different ways that the mobile channel can be used to facilitate fraudulent activity, just some of them are outlined below.

5.2.1 Fraud against subscribers

This could include the possible theft of credit or balances through technical means or even employee involvement. When data is held directly on the device (handset, SD card or SIM), or on the network, extra protection is needed to ensure that communications are protected against eavesdropping, interception and manipulation. A network adversary can intercept or even modify communications to and from an app. as it uses wireless communication (Frisby, et al., 2012). This was a key concern for some of the interviewees. For example, one security expert claimed 'logically in order to transmit wirelessly, you must be able to detect the signal remotely. So can [a fraudster] decipher the transaction? That's the key risk' (Interviewee 9).

Shoulder surfing is a security attack where information such as passwords or personal identification numbers (PINs) are obtained by watching the user enter them into a device, and then stealing the card or device to use it fraudulently. Furthermore, the uncertainty around MPOS in its early roll out might increase repudiation fraud, whereby a subscriber claims that a transaction was not made by them. For example, claiming that their phone had been stolen or intercepted. In the event of a dispute, the responsibility usually lies with the merchant to prove that the cardholder did authorise the purchase.

A 'card not present' is a payment that is processed when the cardholder is not physically present with the card. Many networks consider mobile solutions to be card not present transactions. As one security manager alluded; 'As we move towards mobile payment how do we make sure the card is present for the transaction? … It opens up risk to fraud and stolen cards' (Interviewee 6). This was of particular concern in Australia where it was reported that 'the merchant wears the risk when card not present' (Interviewee 6). This has significance for retailers with an increase in charge backs posing a threat to their bottom line. However a number of anti-fraud payment management companies have emerged specialising in multichannel payment systems to identify and reduce fraudulent activities. Recognising that security is currently a major barrier to mobile payment, some major providers are looking to enhance their protection policy for merchants. For example, in October 2013, PayPal announced that it will accept financial liability in Australia (up to AUD $20,000) for sellers that have been targeted by fraudulent campaigns as long as they can provide proof of shipping and proper practice (Cowen, 2013).

5.2.2 Malicious apps (malware)

Whilst app stores are actively monitored to identify and remove malicious software, users are often duped into installing malware apps that manage to bypass the checks. Therefore, some mobile phones that are running POS apps will have malware installed (Frisby et al, 2012). This in turn raises the issue around the lack of control that retailers have over the customer's device to guarantee security, but also to ensure that updates to apps and security patches are installed in a timely fashion. Researchers have demonstrated how MPOS terminals can be comprised via multiple attack techniques using, for example, micro USBs, Bluetooth and a malicious programmable smartcard (see Ring, 2014). Furthermore, many MPOS attacks are carried out using relatively unsophisticated malware, often brought ready to use on the black market. Of concern is the finding from a recent Online Payment Fraud Trends survey of U.S. and Canadian online merchants, which demonstrated that the majority were unaware of the level of fraud taking place through mobile channels. When asked about fraud in the mobile channel (defined as either commerce on a mobile-optimised website or through a mobile app), 92% of merchants reported that they did not know their mobile fraud rates, 7% perceived that mobile fraud rates were the same or lower than online fraud, and 1% perceived mobile fraud to be slightly higher (CyberSource Corporation, 2012).

5.2.3 Insider fraudulent attacks

It has been found that a significant proportion of credit card fraud arises due to insider attacks i.e. from individuals that are authorised operators of the POS system. For example, in restaurants where the payment is processed out of view of the card owner, employees might write down card details or skim the card details during the transaction. It is possible that such insider attacks might be made easier with MPOS, at least in the short-term before protective security solutions have matured.

5.3 Internal technological and process issues

Mobile technologies introduce a raft of new considerations that could potentially impact on the bottom line. In particular, technology failures can produce negative customer experiences, frustrate staff and ultimately impact on sales. The following outlines some of the risks tat could potentially arise with a shift to mobile retail scanning and payment.

5.3.1 Wireless network infrastructure and recharging devices

If retailers are to embrace mobility as an integral part of their strategies, they will need to outfit their stores with reliable public Wi-Fi access as a cornerstone of those strategies since wireless network infrastructure is 'one of the pillar technologies' (Ngai and Gunasekaran, 2007: 5; Staton, 2001) of m-commerce. As Groß (2015: 229) outlines 'Outside a building, mobile devices have nearly unlimited access to mobile internet and a good GPS signal strength. However, inside the building they require both permanent internet access and a GPS signal. This connection is often lost, thereby disrupting the service'. Whilst investment in Wi-Fi infrastructure is critical, ensuring that it continues to operate without failure is imperative. Problems with connectivity, or loss of connection during scanning, or even more seriously midway through payment could result in substantial customer dissatisfaction, not to mention increased 'abandonment'. The limitation of reliable internet access is a crucial barrier to acceptance and continual use of m-shopping services (Fang et al., 2012).

Furthermore, m-shopping introduces the issue of ensuring that devices are fully charged and ready to go. For the store-owned devices this has a number of solutions. For example, the 'home' of the device could be a recharge point with an automated locking device disabling the equipment until the battery has passed a certain threshold (determined by the store on average length of usage). However, for the customer-owned device, such as a mobile phone, further challenges arise as the same amount of control cannot be administered to ensure battery life for the duration of the shop. It is recommended that options that utilise the customers own device have a feature built in which flags to a customer how much 'shopping time' they have left in terms of battery life (based on analytics of how much battery is typically used). These challenges need to be incorporated into business continuity strategies if mobile scanning and MPOS is to become an integrated feature of bricks-and-mortar stores.

5.3.2 EAS tagging and age-related products

Currently the deactivation of EAS or the removal of hard tags requires an intervention that will interrupt the fluidity of mobile scanning and payment. The tension between enhanced mobility of the customer and security hardware was a recurrent theme in consultation with security professionals, with one remarking; 'a key issue is RFID / EAS tags on products.

When customers scan their own goods, how do we manage products and the removal of the tags? We need a speedy and efficient process … This is an area to overcome and is critical' (Interviewee 4). There is a need to move towards security devices that can be deactivated upon validation of the payment being processed. Similarly, products that require customers to be of a minimum age for purchase, such as alcohol, currently require intervention from a member of staff to verify their eligibility. There are a number of solutions to this, such as registering details at the time of setting up a store account, or enabling systems to recognise age verification documents (such as a driving license).

5.4 Brand protection and consumer confidence

There are numerous considerations for retailers with regards to the impact on their brand's culture when adopting new technologies and processes and it is more important than ever to understand customer demographics and profiles. Similar to SCO there will be different levels of demand from different consumer groups, and customers will adapt to new processes at different rates, but overall customers will always gravitate towards convenience. It is perhaps not surprising that previous research has highlighted trust as a significant factor influencing a customer's willingness to conduct electronic commerce and MPOS transactions (Gefen et al., 2003; Jarvenpaa et al., 2000). A key aspect of earning this trust is ensuring that sufficient security mechanisms are in place. Research has illustrated that customers worry about their liability if their mobile device is lost, stolen or otherwise compromised, and express significant concern that their smartphone will become a greater target for theft if it evolves into a mobile wallet. While some consumers are enthused by the idea of using mobile wallets for low-risk, easily replaceable items like loyalty and membership cards, coupons, and paperless tickets, they are less comfortable with storing cash on their mobile phones, or using them for high value purchases (Bothun et al., 2013). There are a number of measures that retailers can take to increase confidence and safeguard data should a customer's device be stolen or compromised. These include, providing consumers with the ability to wipe their device clean and replace their mobile wallets easily and instantly, embedding identity verification technology and high-tech protection measures, such as requiring a PIN or signature movement. Or, storing data stored remotely in the cloud, rather than on the device. A recent survey by a financial services company (Weed and Sutin, 2013) found that PIN-based authentication with a mobile wallet had much stronger appeal amongst consumers than

NFC, most likely due to the familiarity of authenticating financial transactions via this method. PayPal has adopted this model in its trials with retailers including Home Depot, Foot Locker and JCPenney (Walsh, 2013).

6. Responding to risks: Techniques of payment validation and security

Security solutions need to play an integral part in product protection in the multichannel retail environment of the future, particularly as customers and POS become more mobile. There is a need to strike a balance between streamlining processes for the legitimate mobile customer, and ensuring effective security to protect against losses. As one security manager lamented; 'it can feel like you're being treated like a criminal walking through [self-checkout]. There's the [store name] model where it asks you to sign in blood that you wont do anything wrong' (Interviewee 8). From a loss prevention perspective, the peripheral technologies that enable mobile POS systems, such as EAS, RFID and weight scales, can also be deployed as powerful tools for shrinkage management.

Validation of payment is the linchpin of mobile technologies in retail. It is central to ensuring that mobile scanning and MPOS are implemented within a loss mitigation framework. There are multiple options that this validation can take; each with their own advantages and disadvantages.

6.1 Bag and receipt checks

Whilst relatively common in some countries such as Australia, this practice has the potential to create a negative retail experience. Customers might feel that they are being targeted because they are deemed to look suspicious, they might feel embarrassed if buying items of a personal nature or inconvenienced, particularly if carrying heavy shopping bags. Furthermore, professional shoplifters are most likely to conceal items upon their person rather than in shopping bags, somewhat defeating the object of searches or even 'help' the shoplifter by providing a predictable process. Staff can also become complacent about looking for suspicious activity via any other means.

6.2 Product weight confirmation plates

As with SCO, weight confirmation techniques can be an effective security mechanism for ensuring that products placed in a customer's bag correspond to those being scanned.

However, the scales often have a large margin for area and contribute to frustration amongst customers, particularly when bagging goods. A recent survey revealed that some customers rate self-service checkout as one of the most irritating features of modern life, in part due to these errors.[2]

6.3 Radio frequency identification (RFID)

RFID can be placed on individual items to enable them to be tracked electronically as they move through the supply chain. The tags transfer the information via wireless communication without the need for inter-visibility or physical contact (for an example in the supermarket sector see Gozycki et al, 2004). RFID embedded in a counter/platform at the POS kiosk can register all items in the shopper's bag or basket virtually instantaneously and deactivate tags of registered items.[3] When used at exit points, RFID-enabled security antennae detect tagged items that pass through the store without having been scanned. One security expert regarded RFID as an inevitable development, although recognising that this was much easier and cheaper to do at unit level in apparel, than with FMCGs:

> RFID, that's the technological jump that will occur. I walk out of a store having used a POS but in that basket I have something I haven't paid for, the RFID flags that the product has not been paid for. Make sure you're in front of the curve.' (Interviewee 9)

Studies of the application of RFID for loss prevention have claimed that it can control shrinkage in a number of ways by reducing fraudulent returns (what King and Dennis (2006) refer to as 'de-shopping'), improving supply chain security and reducing theft (Narsing, 2005). A recent publication detailed a new system for preventing 'ticket-switching' in apparel stores, whereby the shoplifter removes the price tag, bar code or packaging and replaces it with one of a lower value. The solution utilised item-level RFID-tagging items in combination with authentication protocols (Zhou and Piramuthu, 2013).

[2] A poll of 700 adults conducted by computer maker Ordissimo, asked what features of modern life irritated people the most. The self-service checkout emerged as a clear winner with 34 per cent of respondents rating it the worst.

[3] A recent RFID self-payment kiosk technology permits an RFID reader to identify the contents of a shopper's basket in approximately one second (Swedberg, 2013).

Research into current patents and patent applications reveals some shrinkage-related innovations in RFID, such as a system for integrating bar code and RFID tag technologies in retail dispenser shelving to provide real-time shelf inventory status; this same technology could have utility in monitoring shoplifting behaviours such as shelf-sweeping (Burnside and Ryan, 2013). One of the barriers to item-level RFID adoption in retail has been the cost of the labels, which for many retailers have been prohibitive (Clodfelter, 2011). However, within the apparel industry there has been an increase in retailers placing item-level RFID tags throughout the store to enable complete real-time visibility of all items (Zhou and Piramuthu, 2013). With improved technology and significant reductions in per-label prices in recent years, it is predicted that RFID will become more mainstream, driving costs down but further research is needed on suitable models for adoption and how best to integrate into legacy systems (Ngai and Gunasekaran, 2007)

6.4 Training

The consultation with security experts in the retail sector found that non-technical processes, in the form of ongoing training, was regarded as the key defence against shrinkage:

> '[The] best results are achieved with trained team members; I don't want to sound like Captain Obvious, but truly there's something in that' (Interviewee 1)
>
> 'The great emphasis is on staff training. One of the key learnings is to provide refresher training' (Interviewee 2).
>
> 'We have a vigorous training program to reduce shrinkage, we need attentive attendants to manage the risks. There also needs to be weight validation and security systems built in, but [it] comes down to attentive operators to reduce losses. Customer facing, confident and diligent, to pick up on deliberate actions by the customer (Interviewee 4).

The need for refresher training was a recurrent theme in the interviews. This was because the introduction of new functionalities in the retail environment was considered to be an arms race against those with malicious intent. As one security manager stated; 'Crooks grow with it [new technologies] - always keeping ahead. They're very technical these days' (Interview 4) and similarly, another remarked that it's important to always 'make sure you're in front of the curve' (Interviewee 9). Importantly, training should ensure that all employees feel equally responsible for identifying, targeting and preventing retail crime. Consultation with loss

prevention managers revealed concern about the fragmentation of responsibility across manufacturers of new mobile technologies, developers of operating systems, application designers, mobile network operators, and the retailer. In particular there was uncertainty about who would be responsible for the security of the system and for losses incurred.

In relation to SCO, it has been found that clerks and cashiers staffing SCOs are increasingly acting in the capacity of security guards, monitoring the checkout lanes for suspicious activity and theft, rather than in a more traditional point-of-sale role (Andrews, 2009). This new emphasis on security and the loopholes of new technologies must be reflected in training (Beck, 2011). As customers become more autonomous in scanning and paying, staff will no longer feel a direct responsibility for loss prevention. Employees might presume that a customer has paid someone or somewhere else and not feel that it is their role to intervene should issues arise. A 'diffusion of responsibility' could ensue whereby individuals defer to one another or to technologies such as CCTV to detect theft and instigate a response (for example see Taylor and Gill, 2014 in relation to CCTV).

6.5 Store Layout

A 2012 study of offender perceptions of risk within retail store environments involved interviews with convicted thieves on how store layout influenced their intention to steal (Cardone and Hayes, 2012). The research found that rational would-be thieves weigh up the risks and benefits communicated by different retail interiors in their decision to steal. The study identified that the main categories of visual cues that were cited as potential deterrents to shoplifters were those pertaining to natural surveillance (e.g. presence of blind spots, being noticed by others, number of customers in store, store layout and size, item location); guardianship levels (presence, quality and quantity of CCTV and whether it was being monitored); formal surveillance (e.g. security, attentiveness of security, uniformed security, undercover detectives); and 'target accessibility' (presence of protective locks, cables, glass cases etc.). One of the key messages is the importance of clearly communicating to would-be thieves the risks of shoplifting.

It has been suggested in relation to SCO that retailers need to create 'zones of control' around the POS that 'maximise modes of surveillance and the design of the SCO space, to impact

upon perceived risk and likelihood of apprehension' (Beck, 2011:211). Recommendations for the creation of zones of control around SCOs include creating SCO areas which feel 'enclosed', control customer movement and limits entrance and exit; carefully monitored checkout locations (staff surveillance; CCTV and video analytics; technological monitoring through till-based alerts and alarms), and ensuring that self-scan supervisors are appropriately trained and responsible for a manageable maximum number of self-scan kiosks at a time. In the multichannel retail environment of the future, however, it potentially becomes harder to create zones of control using situational crime prevention techniques. Since the mobile customer journey creates considerable disconnect in the predictability of location for potentially high-risk activities such as checkout. Traditional checkouts have the benefit of linear predictability (although of course with its own loss problems); the customer would browse the store, select items for purchase, take them to staffed or self-checkout, scan the items, bag them and then pay for the goods before leaving. It is particularly important to recognise that in this scenario, scanning, payment and validation all take place mainly in one predetermined location. Mobile technologies disrupt the predictability of this pattern by enabling product selection, scanning, payment and validation to occur at different locations throughout the store. The fluidity of the customer journey creates uncertainty and raises challenges for loss prevention. For example, where should CCTV cameras be located throughout the store and how can validation processes be implemented without impacting negatively on the legitimate customers' experience? One of the crucial challenges for loss prevention with the introduction of MPOS will be to understand the physical journey undertaken by a customer as they shop. As customers get mobile, so the safeguards and protections must do so too.

7. Concluding remarks and implications for future research

Whereas SCO redefined the retailer-customer dynamic, the introduction of mobile platforms is set to revolutionise it with. It has been claimed that 'the mobile payment will become an uncontested mode for paying goods' in the near future (Raina, 2014: 188). But it is not just the retailer-customer relationship that requires attention, the onset of mobile opportunities will potentially transform brick and mortar stores, presenting opportunities for innovations such as 'endless aisle', 'click and collect', and the 'mobile wallet' with integrated loyalty

platforms. The integration of mobile scanning and mobile payment into seamless multichannel retail offers up many potential benefits as identified, but retailers must be cognisant of the risks to ensure they maintain a positive point of differentiation from competitors, since trust and security are key determinants in customer take up of new technologies (Groß, 2015; Kim et al., 2009; Wong et al., 2012). Retailers are increasingly presented with a compelling case to embrace technological innovations, such as MPOS, in order to stay relevant in an increasingly technologically sophisticated environment. However, key to this process is ensuring that customers are confident about the security of mobile systems.

There are clearly concerns about data protection and privacy when customers use their mobile devices and it has been reported that many individuals are holding back on utilising technological innovations because of security concerns (Moth, 2013; Wu and Wang, 2005), despite the appeal of quick and simple transactions (Jih and Lee, 2003). The convergence of variety of data sources into one domain requires enhanced security protocols. Further research is needed to explore the ways in which mobile technologies open up new avenues of risk and vulnerability, and how best to safeguard against them, in order to ensure customer adoption. There are clear managerial implications when introducing mobile systems, and more broadly, any new technology. Future academic research would do well to focus on the benefits and risks of early adoption. Furthermore, whilst this paper has focused on retail, the concerns and risks will vary by sector. This is an important area for future investigation.

There are many ways in which mobile scanning and POS present challenges for the retail environment of the future and there are many lessons to be learnt from the quick take up of self-service checkout in order to prevent loss and protect the bottom line. If retailers want to stay relevant in the multichannel shopping environment, they need to evolve and adapt to technological innovation. In order to do this, they must be able to navigate the complexities of the payments ecosystem effectively if they are to mitigate loss. Any solution must pay attention to the context and specific environment with which it is operating since 'solutions are dependent upon environment' (Interviewee 9). A multi-disciplinary approach that aligns the security function with business development, ITS, and marketing, for example, is needed in order to roll out mobile systems effectively and securely. There is clearly further research

needed on the different permutations of mobile POS and how it impacts on the customer journey and rates of internal and external theft.

References

Andrews, C.K. (2009) `Do-It-Yourself': Self-checkouts, Supermarkets, and the Self-Service Trend in American Business'. Available at: http://drum.lib.umd.edu//handle/1903/9593 (accessed: 21.10.13)

Agarwal, S., Khapra M., Uchat N., and Menezes, B. (2007) 'Security Issues in Mobile Payment Systems', Proceedings of the 5th International Conference on E-Governance, Hyderabad, India.

Bamfield, J. (2012) *Shopping and Crime*. Palgrave Macmillan: Basingstoke.

Beck, A. (2011) 'Self-scan checkouts and retail loss: Understanding the risk and minimising the threat', *Security Journal*, Vol. 24 No.3, pp.199–215.

Beck, A. and Peacock, C. (2009) *New Loss Prevention: Redefining Shrinkage Management*, Basingstoke: Palgrave Macmillan.

Blochlinger, M. (2012) 'Mobile Payment Systems', In B. Stiller et al. (Eds), *Internet Economics VI - Technical Report*. Department of Informatics (IFI), University of Zurich. Available at: www.csg.uzh.ch/teaching/hs11/inteco/extern/IFI-2012.02.pdf#page=41 (accessed 28.10.13).

Bothun, D., Glisson, S., Haas, R., Isaac, C. and Lieberman, M. (2013) 'Consumer Intelligence Series; Opening the Mobile Wallet', PricewaterhouseCoopers LLP. Available at: http://www.pwc.com/sg/en/tice/assets/tmtnews201304/pwc-consumer-intelligence-series-mobile-wallet.pdf (accessed: 14.01.14).

Brady, M.K., Voorhees, C.M. and Brusco, M.J. (2012) 'Service Sweethearting: Its Antecedents and Customer Consequences', *Journal of Marketing*, Vol. 76 No.2, pp.81-98.

Burnside, W. D., and Ryan, J. M. (2013). Shelf-monitoring system. United States of America. Available at: www.google.com/patents/WO2013032697A3?cl=en (accessed 14.01.14).

Cardone, C., and Hayes, R. (2012) 'Shoplifter Perceptions of Store Environments: An Analysis of how Physical Cues in the Retail Interior Shape Shoplifter Behavior', *Journal of Applied Security Research*, Vol.7 No.1, pp.22–58.

Chapman, P. and Templar, S. (2006) 'Methods for measuring shrinkage', *Security Journal*, Vol.19 No.4, pp.228-240.

Clodfelter, R. (2011) 'Point of Sale Technologies at Retail Stores: what will the future be like?', In E. Pantano and H. J. P. Timmermans (Eds.), *Advanced Technologies Management for Retailing: Frameworks and Cases*.

Coursaris, C. and Hassanein, K. (2002) 'Understanding m-commerce', *Quarterly Journal of Electronic Commerce* Vol. 3 No.3, pp. 247–271.

Cowen, P. (2013) 'PayPal to absorb fraud cost for Aussie sellers', *SC Magazine*. Available at: www.scmagazine. com.au/News/355708,paypal-to-weather-fraud-cost-for-aussie-sellers.aspx (accessed: 16.10.13)

CyberSource Corporation (2012) *2012 Online Fraud Report; Online Payment Fraud Trends*, Merchant Practices and Benchmarks. Available at: https://www.jpmorgan.com (accessed: 14.01.14).

Dahlberg, T., Mallat, N., Ondrus, J. and Zmijewska, A. (2008) 'Past, present and future of mobile payments research: A literature review', *Electronic Commerce Research and Applications* 7, pp.165–181.

ECR Europe (2011) *The Impact and Control of Shrinkage at Self-Scan Checkouts*. An ECR Europe White Paper.

European Commission (2012) *Green paper: Towards an integrated European market for card, internet and mobile payments*. Available at: http://ec.europa.eu/competition/sectors/financial_services/payments_en.html (accessed: 08.01.2014).

Evans, J. and Dayle, E. (2009) 'Self Scanning: Profit or Loss?', Presentation at the RILA Auditing and Safety conference, Orlando, Florida.

Fang, B., Liao, S., Xu, K., Cheng, H., Zhu, C. and Chen, H. (2012) 'A novel mobile recommender system for indoor shopping', *Expert Systems with Applications*, Vol. 39 No. 15, pp. 11992-12000.

Felson, M. (1994) *Crime and Everyday Life: Insights and Implications for Society*. Thousand Oaks, CA: Pine Forge Press.

Fiore, A.M. and Kim, J. (2007) 'An integrative framework capturing experiential and utilitarian shopping experience', *International Journal of Retail & Distribution Management*, Vol.35 No.6, pp.421-442.

Frisby, W., Moench, B., Recht, B. and Ristenpart, T. (2012) 'Security Analysis of Smartphone Point-of-Sale Systems'. Available at: http://pages.cs.wisc.edu/~rist/papers/pos.pdf (accessed: 16.10.13).

Gefen, D., Karahanna, E., Straub, D. W. (2003) 'Trust and TAM in online shopping: an integrated model', *MIS Quarterly* Vol.27 No.1, pp.51-90.

Gill, M. (2007) *Shoplifters on shop theft: implications for retailers*. Perpetuity Research and Consultancy International (PRCI) Ltd: Leicester.

Global Mobile Commerce Forum: Inaugural Plenary Conference. London, UK (10 November 1997).

Gozycki, M., Johnson, M. E., and Lee, H. (2004) 'Woolworths "Chips" Away at Inventory Shrinkage through RFID Initiative', Center for Digital Strategies; Trustees of Dartmouth College and Stanford Global Supply Chain Management Forum.

Groß, M. (2015) 'Mobile shopping: a classification framework and literature review', *International Journal of Retail & Distribution Management*, Vol. 43 Iss 3 pp. 221 – 241.

Guha, A. (May 2013) 'Spotlight on Australia: Consumer Payments Revolution', *Insights from J.P. Morgan*. Available at: www.jpmorgan.com (accessed: 14.01.14).

Haas, A. and Kenning, P. (2014) 'Utilitarian and Hedonic Motivators of Shoppers' Decision to Consult with Sales people', *Journal of Retailing* Vol. 90 No.3, pp.428–441.

Hakim, S. and Rengert, G. F. (1981) *Crime Spillover*. California: Sage.

Harding, E. (2012) 'How cheating at checkouts is turning us into a nation of self-service shoplifters', *DailyMail*. Available at: http://www.dailymail.co.uk/news/article-2135284/How-cheating-checkouts-turning-nation-self-service-shoplifters.html (accessed: 13.01.13).

Hayes, R. and Cardone, C. (2006) 'Shoptheft' In M. Gill (Ed.) *The Handbook of Security*. Palgrave Macmillan Ltd: Basingstoke.

Hayes, F. (2013) 'Mobile Retailers Hit Hardest By Payment-Card Fraud - And Many Have Given Up', *FierceMobileRetail*. Available at: www.fierceretail.com (accessed: 21.10.13).

Holmes, A., Byrne, A. and Rowley, J. (2014) 'Mobile shopping behaviour: insights into attitudes, shopping process involvement and location', *International Journal of Retail & Distribution Management*. Vol. 42 No. 1, pp. 25-39.

IBM (2008) *Shrink and self-checkout: trends, technology and tips*. New York: IBM. Available at: ftp://ftp.software.ibm.com/software/retail/marketing/pdf/sco/RTE03002-USEN-00.pdf (accessed: 21.10.13).

Jarvenpaa, S.L., Lang, K.R., Takeda, Y. and Tuunainen, V.K. (2003) *Mobile commerce at crossroads*, Communications of the ACM Vol.46 No.12, pp. 41-44.

Jih, W.J.K. and Lee, S.F. (2003), 'An Exploratory analysis of relationships between cellular phone uses' shopping motivators and lifestyle indicators', *Journal of Computer Information Systems*, Vol. 44 No. 2, pp. 65-73.

Kim, J., Ma, Y.J. and Park, J. (2009) 'Are US consumers ready to adopt mobile technology for fashion goods? An integrated theoretical approach', *Journal of Fashion Marketing and Management*, Vol. 13 No. 2, pp. 215-230.

KPMG (2011) *2011 KPMG Mobile Payments Outlook*. Available at: http://www.kpmg.com/SK/sk/IssuesAndInsights/ArticlesPublications/Documents/2011-mobile-payments-outlook.pdf 9accessed: 09.01.2014).

Krasny, J. (2012) 'Theft Is Up To Five Times Higher In Self-Checkout Lanes', *Business Insider*. Available at: http://www.businessinsider.com.au/theft-is-higher-in-self-checkout-lanes-2012-4 (accessed: 13.01.14).

Mallat, N. and Tuunainen, V.K. (2008) 'Exploring Merchant Adoption of Mobile Payment Systems: An Empirical Study', *E-Service Journal*, Vol.6 No.2, pp.24-57.

Medich, C., Halter, R., Mcglothin, B., Jett, M., Vicente-tamarin, F., Throckmorton, G., and Stokely, D. (2011). *Mobile Retailing Blueprint: a comprehensive guide for navigating the mobile landscape*. USA.

Moth, D. (2013) 'Security and fraud concerns are biggest barriers to mobile payment adoption', *econsultancy.com*. Available at: http://econsultancy.com/au (accessed: 30.10.13).

Narsing, A. (2005). 'RFID And Supply Chain Management: An Assessment Of Its Economic, Technical, And Productive Viability In Global Operations', *Journal of Applied Business Research* Vol.21 No.2, pp.75-80.

Ngai, E. and Gunasekaran, A. (2007) 'A review for mobile commerce research and applications', *Decision Support Systems* Vol. 43, pp.3–15.

Ondrus, J. and Pigneur, Y. (2007) 'Towards a holistic analysis of mobile payments: A multiple perspectives approach', *Electronic Commerce Research and Applications* 5 pp.246–257.

ONS (2005). Office for National Statistics, *Annual Business Inquiry*, 2005.

Raina, V.K. (2014) 'Overview of Mobile Payment: Technologies and Security' In F. Liebana, F. Munoz-Leiva, and J. Sanchez-Fernandez (Eds) *Electronic Payment Systems for Competitive Advantage in E-Commerce*. IGI Global.

Repetto, T.A. (1976) 'Crime prevention and the displacement phenomenon', *Crime and Delinquency* Vol.22, pp.166-177.

Ring, T. (2014) 'Millions of consumers at risk from mobile POS flaws', S C Magazine. Available at: http://www.scmagazineuk.com/millions-of-consumers-at-risk-from-mobile-pos-flaws/article/341323/ (accessed: 09.03.2015).

Sha, D. Y. (2012) 'Improving service quality of retail store by innovative digital content technology', IEEE *International Conference on Computer Science and Automation Engineering*. June 2012.

Shin and Lee (2014) 'The Effects Of Technology Readiness And Technology Acceptance On NFC Mobile Payment Services In Korea', *The Journal of Applied Business Research,* Vol.30 No.6, pp.1615-1626.

Staton, R. (2001) 'The Mobile Internet: What is it? How will it be built? and what services will it deliver?', *International Review of Law, Computers and Technology,* Vol.15 No.1, pp.59-71.

Swedberg, C. (2013) 'IER's Expedited Self Payment Kiosk Speeds Up Checkouts', *RFID Journal*. Available at: http://www.rfidjournal.com/articles/view?10667/2 (accessed: 21.10.13).

Statista (2015) "Global mobile payment transaction volume from 2010 to 2017 (in billion U.S. dollars)", *Statista*. Available at: http://www.statista.com/statistics/226530/mobile-payment-transaction-volume-forecast/ (accessed: 17.09.2015)

Taylor, E. (2014) *Staying Ahead of the Game; new mobile technologies in retail, benefits and risks*. A report for Efficient Consumer Response Australasia (ECRA).

Vrechopoulos, A., Constantiou, I., Sideris, I., Doukidis, G. and Mylonopoulos, N. (2003), "The critical role of consumer behaviour research in mobile commerce", *International Journal of Mobile Communications,* Vol.1 No.3, pp.239-340.

Walsh, M. (2013) 'Mobile Payments Still Lack Clear Winner', *OnlineMediaDaily*. Available at: http://www. mediapost.com/publications/article/196184/mobile-payments-still-lack-clear-winner.html#axzz2NztxVkN6 (accessed: 21.10.13).

Weed, G. and Sutin, M. (2013) *Credit Card Monitor Q2 2013; Mobile Wallets and the Potential Consumer Roadblock to NFC Advance.* Available at: http://w3.phoenixmi.com/wp-content/uploads/2013/09/Mobile-Wallet-Charts.pdf (accessed: 14.01.14).

Wong, C.H., Lee, H.S., Lim, Y.H., Chua, B.H., Chai, B.H. and Tan, G.W.H. (2012), 'Predicting the consumers' intention to adopt mobile shopping: an emerging market perspective', *International Journal of Network and Mobile Technologies,* Vol. 3 No. 4, pp.24-39.

Wu, J.H. and Wang, S.C. (2005), 'What drives mobile commerce? An empirical evaluation of the revised technology acceptance model', *Information & Management* Vol.42 No.5, pp.719-729.

Yang, K. (2010) 'Determinants of US consumer mobile shopping services adoption: implications for designing mobile shopping services', *Journal of Consumer Marketing* Vol.27 No.3, pp.262-270.

Zhou, W. and Piramuthu, S. (2013) 'Preventing ticket-switching of RFID-tagged items in apparel retail stores', *Decision Support Systems,* Vol.55 No.3, pp.802–810.