STAYING AHEAD OF THE GAME

Mobile technologies in retail: A review of benefits and risk

Dr Emmeline Taylor | The Australian National University | December 2013

CONTENTS

ACKNOWLEDGEMENTS

The author would like to thank the Efficient Consumer Response Australasia (ECRA) Loss Prevention Group for commissioning the project, and in particular Checkpoint for providing the resource required for its completion.

A number of staff at the University of Technology Sydney (UTS) contributed to the literature review; in particular Lucy Kaldor, Rodger Watson and Lindsay Asquith, and Lucy Klippan provided graphic design and desktop publishing services for the report.

This report draws upon consultation with stakeholders from the retail sector in Australia. The author wishes to thank them for their input and advice throughout the project. In addition, several global experts were liaised with to gain understanding on the potential for mobile technologies to impact on loss.

- Shrinkage costs the Australian retail industry over $2 billion dollars annually. Shoplifting is estimated to be the main cause with a 45% value share in 2012, followed by employee theft (27%) and admin/non crime losses (21%). New processes and practices can have a huge impact on levels of **shrinkage**, at least until effective security and resilience is built into them.

- Recognising the significant potential for loss, the mobile payment channel must be safe and secure from the outset. There is **no room for trial and error** as characterised the introduction of self-service checkout; the risks are too high. Fraudulent activity, theft and security breaches not only impact the bottom line but can have devastating impacts on customer confidence.

Recognising benefits and opportunity

- Whereas self-service checkout redefined the retailer-customer dynamic, the introduction of mobile platforms will **revolutionise** it. Brick and mortar stores are being transformed by multichannel retail. Whilst benefits and opportunities are numerous, the risks are very real.

- The retail payment market is being flooded with products and there is no clear market leader at present, but currently a key difference is whether mobile communication is facilitated by **cloud-based applications** or **near field communication** (NFC).

Recognising risk

- Mobile scanning and mobile payment create '**disconnect**' in the customer journey presenting new challenges for loss prevention.

- Fraudulent activity could increase with the use of mobile technologies, at least in the early stages of implementation. It is likely that there will be some **migration of fraudsters** to the mobile channel because the security protocols are not yet as mature as e-commerce or in-store payment.

- Ensuring **customer confidence** is paramount and this includes safeguards for **privacy** and **data protection**, investing in **robust technology** and having an established **business continuity plan** for technological issues.

- It is envisaged that mobile scanning and mobile payment will have a modest impact on employee theft, although **collusion** has the potential to increase at validation stage.

- It is envisaged that mobile scanning and mobile payment will have a modest impact on 'customer' theft in the long term, although the diversity of payment types, distribution of POS locations throughout the store, and the perception of ease, could see an **increase in theft** from those entering the store with malicious intent.

- As occurred with self-checkout, there will be a window of opportunity for genuine customers to justify errors in scanning (whether intentional or not); '**techniques of neutralisation**' will include problems with scanning, frustration with the technology or lack of staff on hand to assist with queries and problems.

- Mobile solutions that utilise the customer's device raise issues regarding critical **software updates**; retailers will have little control over ensuring that customers install updates and security patches.

- As customers become more autonomous in scanning and paying, and therefore staff functionalities broaden beyond POS, there is the potential for a **diffusion of responsibility**. Staff might be less inclined to see loss prevention as part of their remit.

- There is potential for the enabling technologies associated with mobile scanning and payment to result in a **diffusion of benefits**; decreasing likelihood of inter-company fraud for example.

- **Validation** of payment is the linchpin of mobile technologies in retail. Whilst disconnect and fluidity will come to characterise in store processes, embedding robust controls in the validation function is paramount.

- **The sophistication of the validation function must evolve** with mobile technologies. Whilst the Australian customer has demonstrated a comparatively high tolerance threshold for bag/receipt checks upon exit, this crude process undermines the fluidity of the mobile customer and could leave a negative impression on legitimate patrons. Alternatives should be explored alongside mobile solutions.

Responding to risks

- Mobile retail solutions offer many potential **benefits** and retailers are increasingly presented with a compelling case to embrace innovation in order to stay relevant in a multichannel shopping environment. However, there are **risks** that could impact the bottom line and retailers must mitigate for these to ensure they maintain a positive point of differentiation from competitors.

- Australian retailers taking advantage of a diversified payment ecosystem, must **embed loss prevention** and mitigation into their operational strategy from the outset.

- Developing a **research agenda** that recognises local context; customer confidence, data protection, and a roll out strategy closely aligned with loss prevention are key areas requiring attention.

- The creation of a **roadmap** and **toolkit** to mitigate the potential risks brought about by mobile payment channels is essential.

01. PROJECT SCOPE AND RESEARCH AIMS

The aim of this report is to harness the learning from the implementation of self-checkout (SCO) and combine this with available information relating to mobile scanning (m-scan) and mobile point of sale (m-POS). The report provides an overview of benefits, risks and key considerations for industry stakeholders regarding the utilisation of mobile technologies in the retail sector.

Whilst there is a growing literature attending to the benefits of mobile payment, a précis overview of vulnerabilities and impact on loss is largely missing. It is clear that understanding remains 'fragmented'[1] , particularly in relation to 'shrinkage'[2] 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.

The report provides an overview of some of the different modes of mobile payment systems, a consideration of the benefits that they offer to retailers and their customers, before focusing on the potential risks and vulnerabilities. The full methodology can be found in the Appendix.

The report culminates in a list of recommendations for developing a robust approach to mobile payment technologies as well as providing an agenda for future research focused on understanding loss mitigation.

Aims and Objectives

- Outline what mobile scanning and mobile POS is and the various guises it can take in the retail sector.
- Draw upon relevant research from the introduction of SCO with regards to loss and apply the relevant lessons to mobile POS technology.
- Consult with loss prevention professionals, industry partners and academic experts to gain insight into mobile payment opportunities and risks.
- Provide insight on the key considerations for industry stakeholders (primarily retailers) in moving to m-scan and m-POS with regards loss mitigation.

The way in which customers select their purchases and pay for them is rapidly changing. As new technologies emerge onto the market, retailers and suppliers are facing the challenge of reconfiguring systems to accommodate increasingly mobile customers who expect multichannel options supporting quick and secure digital payment. Mobile commerce has been a hot topic since the early 2000s but it is only in recent years that its roll out has gathered traction, particularly in the US, Europe and some parts of Asia.

Whereas SCO redefined the retailer-customer dynamic, the introduction of mobile platforms is set to revolutionise it. 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. Multichannel retail will ultimately bridge the gap between virtual and physical stores.

2.1 Defining mobile payment

The umbrella terms 'mobile payment', 'mobile commerce' and 'contactless payment' are often used, but in reality these terms encompass a vast array of scenarios. In essence, a 'mobile payment' is any payment where a mobile device is used to initiate, authorize and/or confirm an exchange of financial value in return for goods and services. Mobile payments can be defined as:

A payment that is carried out with a handheld device such as a mobile phone, tablet or a PDA (personal digital assistant) by taking advantage of wireless and other communication technologies.[3]

New technologies represent significant opportunities; diversifying browsing and payment options for customers and streamlining processes for retailers, but they are not without risk. Whilst the traditional staffed checkout will in all likelihood continue for the foreseeable future, a range of other methods are becoming more popular. The use of emerging technologies in the supply chain and at the point of sale (POS) are set to dramatically change the process by which products pass from retailer to consumer.

2.2 Types of mobile payment

The main technologies used to deliver mobile payments are:

- Mobile Over the Air Payments ¬ employing technology such as WAP, SMS messaging, IVR (Interactive Voice Response) and USSD (Unstructured Supplementary Service Data)

- Contactless Mobile Payments ¬ often referred to as mobile proximity payments, such as NFC (Near Field Communications).

In order to further clarify the confusing and rapidly expanding mobile payments market, a distinction is drawn between three categories; mobile commerce, mobile acceptance and mobile wallets[4].

Mobile Commerce

Mobile commerce, or M-Commerce, is often used as a generic term to describe the many variants of mobile payments such as payment using a tablet/handheld device, using cloud-based software, Near Field Communication (NFC) or other communication. It has been defined as 'the delivery of electronic commerce capabilities directly into the consumer's hand, anywhere, via wireless technology'[5].

Mobile Payment Acceptance

Mobile Payment Acceptance refers to the use of a customer-owned device to make payment (e.g. smart phone, tablet or PDA). The smartphone or tablet device is fitted with temporary or permanent hardware to facilitate transaction. The device consists of; mobile payment application; consumer mobile device; and hardware accessory capable of reading account data from a payment card[6].

Mobile Wallets

Mobile wallets use smartphone applications to enable customers to use their device for payment instead of a credit or debit card. There are a number of different wallet providers, and, perhaps most importantly, some wallet products use proximity such as near-field communication (NFC) while others are remote or cloud-based.

Proximity: Near field communications (NFC)

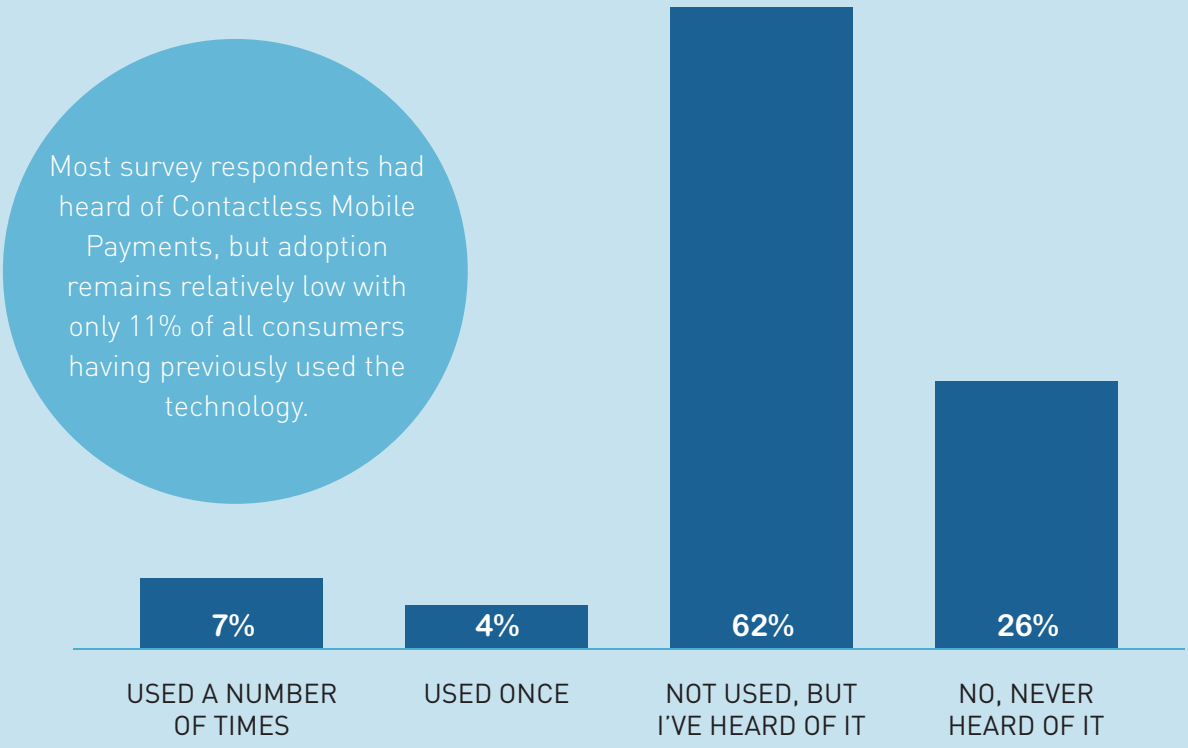
Near-field communication (NFC) allows exchange of data over short distances quickly and simply without any physical contact, i.e. 'contactless payment'. The consumer places their NFC-enabled device close to the payment terminals (usually within 10cms) to permit the exchange of information and authorisation[7].

Vendors such as Lenovo and Samsung are building NFC into tablets and phones, but some are predicting that NFC has a limited shelf-life with some providers moving away from NFC-enabled devices in favour of QR-code devices[8]. However, some retailers are using stickers to bypass the need for mobile phones to have built in capability.

Remote: Cloud-based mobile payment

A cloud-based wallet consists of an app on a smartphone. Users register for the service and then use it to pay for items in just one or two clicks. In some cases, customers may have a stored value held in a prepaid account or draw funds directly from a bank account. Payment service providers (PSPs) such as Google, PayPal, GlobalPay and GoPago use a cloud-based approach to in-store mobile payment. In some POS retail situations, the cloud wallet requires cardholders to enter a PIN into their wallet app from the receipt to complete the transaction. Some have argued that this is 'clumsier' than NFC, but it has seen much higher transaction volume initially because merchants do not have to radically change their POS infrastructure.[9]

Awareness and use of Contactless Mobile payments



Source: eDigital Research (2013)

2.3 Mobile scanning and POS scenarios

There are many different permutations of scanning and POS in the world of mobile retail technologies. These can be broadly categorised into three different scenarios:

Store-owned – customer-operated

Store-owned hardware may include handheld scanner and a touchscreen tablet affixed to a shopping cart. When shopping/scanning is completed, the customer takes the scanner, along with pre-bagged items, to a POS kiosk/checkout station (can be staffed or fully self-service). The scanner is 'docked' and purchase information is downloaded.

Customers pay by any method available (card, cash, NFC), are issued with a receipt and leave the store.

Examples:

- The Metro Group Future Store Initiative[10].
- Fresh and Easy supermarket (USA)[11]

Store-owned – store-operated

A staff member approaches customer anywhere in the store with a device (e.g. tablet) connected to Wi-Fi which can browse the store catalogue, select items and process payment from the customer. There are many sales and marketing functions associated with this method, including social networking.

Alternatively, a store device (e.g. 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.

Examples:

- AOpen eTile in-store tablet[12]
- Nordstrom flagship store (USA)[13]

Customer-owned – customer-operated

Scanning and payment:

Customers use an 'app' to convert their smartphone into a scanner. The list of scanned items and the price is downloaded using a QR Code or other method at a paystation. Where NFC is present customers can make contactless payments using their smartphone as a wallet; otherwise with cash or card (contactless or swipe). This mode of mobile POS has particularly compelling marketing possibilities e.g. Walmart creates consumer

profiles to enhance customer relationship management (CRM), and to target real-time in-store virtual coupons.

Examples:

- Qthru[14]
- Walmart 'Scan & Go' (USA)[15]

Payment only:

Mobile POS system in which consumers download software onto their phones and then tap their device against a reader at checkout to make a purchase.

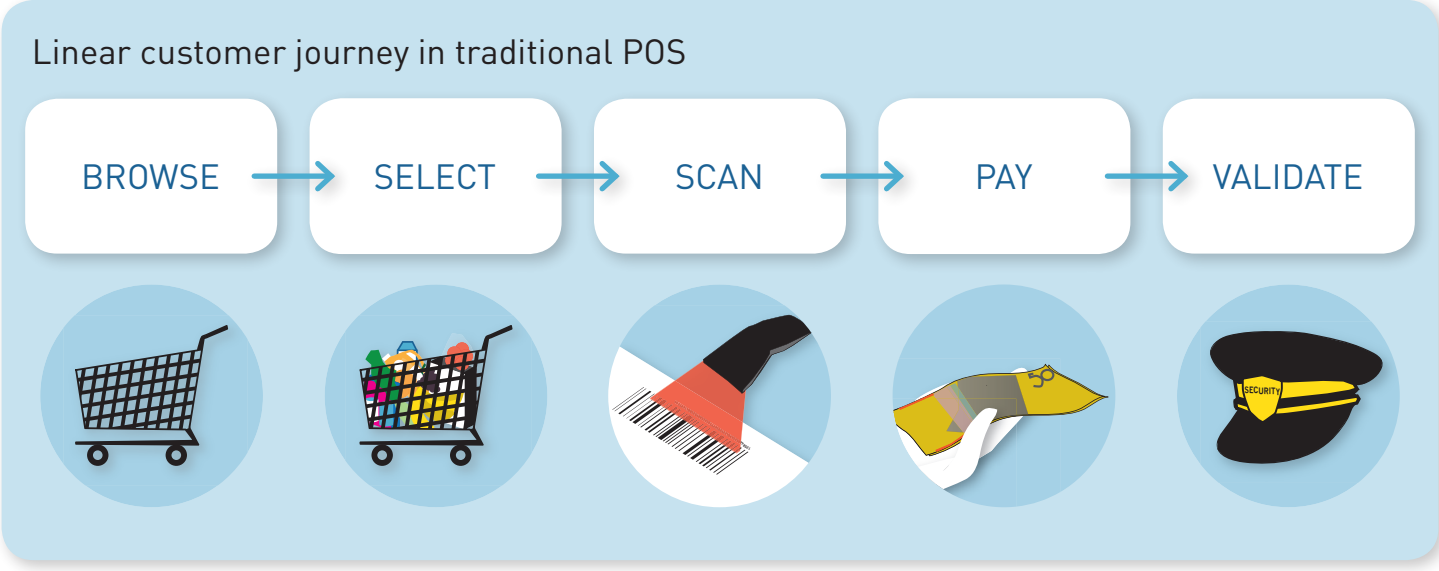
Examples:

- Merchant Customer Exchange (consortium of US retailers including Wal-Mart, Best Buy, 7-11, Target, Dunkin Donuts, & Gap.)

2.4 Reconfiguring the customer journey

There are many different ways in which mobile payment can impact on the customer journey. Identifying the product for purchase, scanning, paying for the item and validating payment could undergo substantial disconnect. Traditional checkouts had the benefit of linear predictability (although of course with its own loss problems).

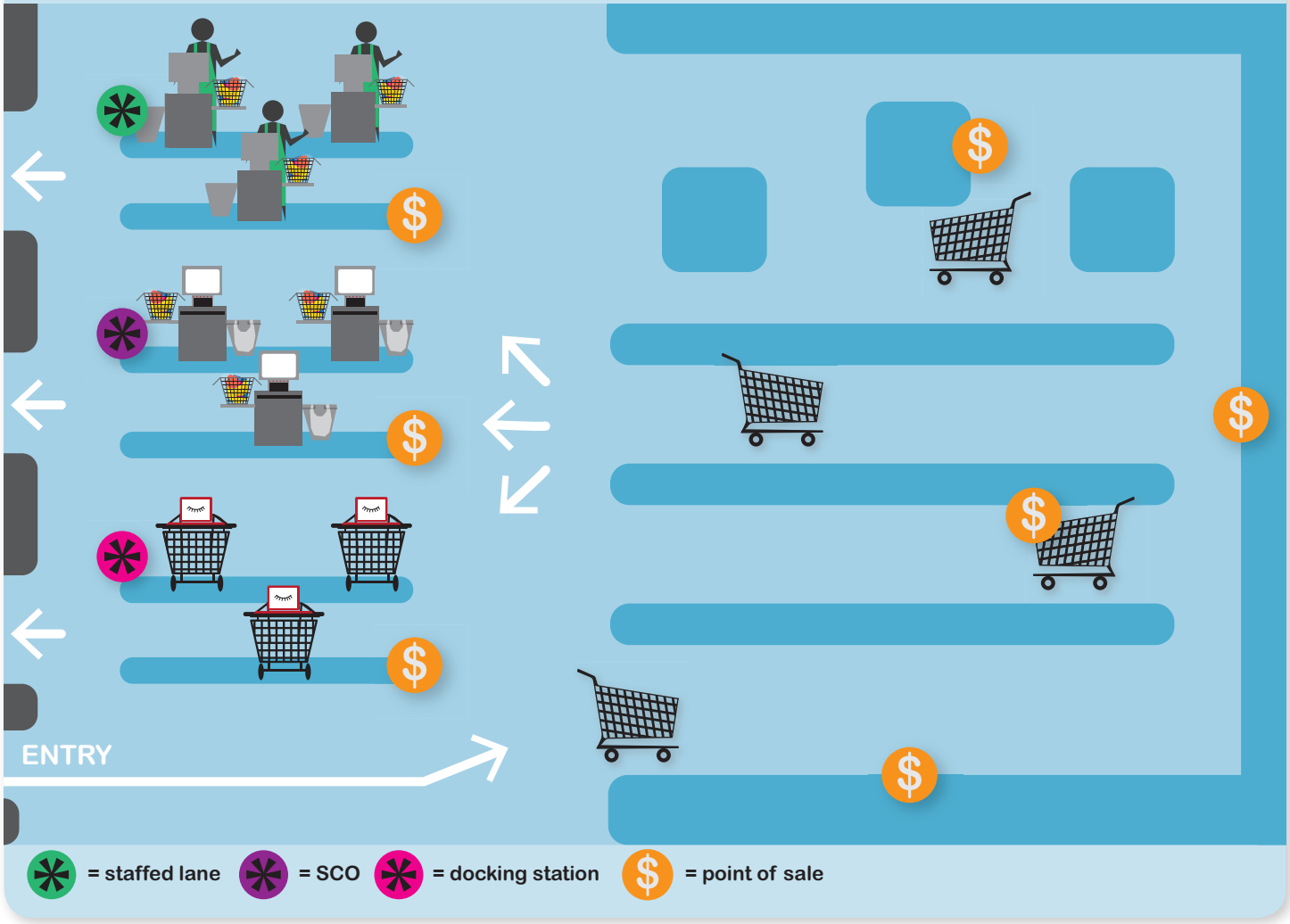
The customer would browse the store, select items for purchase, take them to staffed or self-checkout, scan the items, bag them and then pay for the goods before leaving. It is particularly important to recognise that in this scenario, scanning, payment and validation all take place mainly in one predetermined 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 mobile payment will be to understand the physical journey undertaken by a customer as they shop. Globally, there is considerable variation in m-scan and m-POS systems, and therefore in the movement of customers within the store.

The customer journey and 'disconnect' in a mobile retail environment



The image depicts a multi-payment ecosystem with traditional staffed lanes, SCO, mobile device docking stations and payment kiosks, as well as on the floor customer assistants taking payment in the aisle. In addition, there could be express lane delis or fast-food outlets within the store where customers can place orders on tablet devices, make payment, and be alerted by SMS or similar when the item/service is ready for collection.

Understanding the value proposition offered by different mobile methods is important for retailers. NFC requires customers to be channelled through certain points for payment (checkouts or kiosks for example) in order to come within 10cm of a reader, and therefore present opportunities for retaining control over movement. Store-owned mobile devices and customer cloud-based applications can be processed anywhere that the device has a signal; there is not necessarily the same 'touch points' required. This can present a challenge for retailers wishing to retain control over POS and payment verification, although not insurmountable.

Multi-site POS diversifies processes thereby potentially weakening control. The reconfigured customer journey requires different safeguards to mitigate against loss.

2.5 Self-service checkout

Self-checkout (SCO) revolutionised the relationship between the customer and retailer. Since launching in the retail environment in 1992, it has become a familiar part of the retail landscape, particularly in supermarkets. SCO initiated the transferral of the checkout process to the customer, relinquishing control at the most crucial point of the shopping experience – point of sale. Initially there was considerable scepticism, and perhaps not surprisingly, concern that huge losses would follow.

There are numerous approaches to SCO, but essentially it involves the customer taking responsibility for scanning items they wish to purchase and then paying for them using an interactive operating system. SCO presents a number of challenges in terms of controlling the shrinkage that may arise from their use, both malicious (e.g. 'customers' deliberately not scanning items or using the SCO aisle to walk out of the store with goods they haven't paid for) and non-malicious (e.g. items not scanning properly, incorrect prices being transacted).

2.6 Understanding Shrinkage

Shrinkage has been defined as:

'*Intended sales outcome that was not and cannot be realised*'.[16]

There is little current understanding on how mobile technologies could contribute towards shrinkage which was estimated to cost USD $119 billion in 2011. Australia lost 1.43% of turnover to shrinkage, amounting to just over $2 billion US dollars.[17]

It can be broken down into four main sources:

- External theft
- Internal theft
- Internal errors / Process or administrative errors, and;
- Inter-company fraud

There is little consensus on which of these accounts for the most loss.[18] The Centre for Retail Crime's Global Retail Theft Barometer (GRTB) finds external theft to be the biggest culprit (43.2%), followed by employee theft (35%), internal error (16.2%) and inter-company fraud (5.6%) (see diagram, below).

However, the National Retail Security Survey (NRSS) puts employee theft at the forefront, as does the National Retail Federation, 2011.

There has been much in the media globally about how SCO has contributed to shrinkage and particularly theft, although definitive figures and concrete evidence are elusive.[19] Some reports suggest that customer theft is up to 5 times higher with SCO than at a traditional checkout.[20] Conversely, an NCR white paper claims that according to retailers SCO has a neutral or slightly positive impact on shrink and does not contribute to shoplifting.[21] Similarly, an ECR Europe report concluded that overall the impact of SCO on rates of shrinkage was neutral.[22] The reason being that although new mechanisms of loss were occurring, they were replacing old methods of loss associated with the staffed checkout. In other words, the new POS system brought with it a raft of new problems, but these largely displaced the old cache of problems. In criminological terms, this is known as 'tactical displacement' whereby the offender employs a new method to commit the same offence.

A Case study of the impact of SCO on shrink

A 12 month study of a US supermarket chain compared rates of non-scanned items by checkout clerks compared to the number of non-scanned items by customers using SCO. Data was collected across 46 stores with 554 staffed lanes and 63 SCO lanes. The key finding was that staffed lanes were three times more likely to have a non-scanned item as compared to the self-checkout lanes.[23]

Whilst actual amounts of loss directly related to SCO are varied, it is clear that their introduction increased the number of variables in the shrinkage equation. As mobile POS further diversifies payment options, this will also diversify risks.

Views remain mixed on the impact that SCO has on the customer experience. Some commentators have lamented that self-service is indicative of a slippery slope towards less customer service,[24] whereas, some retailers have launched entirely self-checkout stores following positive customer feedback.[25]

SCO has undergone considerable evolution since its introduction over two decades ago, but it is clear that further modifications are required as survey research has revealed that some customers rate self-service checkout as one of the most irritating features of modern life.[26]

The impact of SCO on malicious and non-malicious shrinkage[27]

Non-malicious SCO problems

- problems with barcodes not scanning
- customers placing bags in the wrong area and triggering alarms that then require attention of staff and disrupt staff ability to monitor all SCOs
- age-related triggers (e.g age verification for purchase of sharps or alcohol)
- customers forgetting receipts (thus making receipts readily available for prospective thieves)
- payment problems (e.g. issues with credit card chips and pins)
- customers forgetting to take their change
- products with security products (e.g. EAS) attached

Malicious SCO problems

- not scanning items
- selecting the wrong loose item description
- misusing vouchers
- scanning but not paying
- entering the incorrect quantity/price
- 'walking'; using the self-scan area to walk through with stolen goods
- using stolen credit cards to pay for goods.
- collecting receipts to later steal or return goods.

Whilst some lessons can be taken from SCO, the uniqueness of mobile devices present some new challenges. Mobile devices are designed to have simple interfaces with a focus on ease of use. They don't therefore typically have the same level of security as would be built into a payment card. Furthermore they increasingly include multiple cellular technologies such as GPS, Bluetooth, infrared and NFC. These broader functionalities can result in more security vulnerabilities. There are two unique features of mobile payment that present new shrink issues:

1. Understanding the 'mobile' in mobile payment

- **Control:** the mobility of POS raises the issue of validating that a transaction has been completed and verified. Payment using cloud-based applications could potentially take place anywhere in the store, whereas use of NFC will in all likelihood generate the introduction of numerous POS. This can present challenges for loss prevention as the flows and movement of customers associated with traditional POS become 'disconnected', fragmented and fluid.

- **Modification:** The mobility of devices can make them susceptible to modification. A mobile device with wireless connectivity allows it to be removed from a merchant's location, which is usually assumed to be safe, and taken to a location that is convenient for the customer. This can provide benefits to the merchant but it also creates many security risks. One of the risks to the merchant is the ease for a criminal to steal such a terminal, modify it, and return it without anyone realizing. Since the mobile device has no fixed location (other than a recharging station), keeping track of it, a clear merchant responsibility, becomes more challenging.[28]

2. Electronic transactions

- Electronic payment introduces new ways for criminals to commit crime. Fraudulent activities such as card skimming and eavesdropping on transactions have become a very real concern, particularly when this can result in expensive chargebacks for retailers.

2.7 The current picture: Roll out and take up of mobile payment

Mobile payment services have principally been adopted by quick-service oriented industries such as public transportation, service stations, and fast-food and beverage vendors (e.g. McDonalds, Starbucks)[29]. Wider adoption of mobile payments, however, has not been as rapid or widespread as expected and there are many examples of discontinued mobile payment services such as the SimPay consortium.[30] However, the industry is gaining pace and many new payment instruments have emerged on the market with the objective of facilitating swift and convenient transactions that will compete with cash, cheques, credit cards, and debit cards.

At present, mobile payments represent a small proportion of sales, particularly in Australia, but things are moving rapidly and retailers need to prepare to integrate them as part of their future retail strategy. In 2012 it was estimated that in-store mobile payments in the US quadrupled, and Paypal alone processed in the region of

$14 billion in mobile payments.[31] It has been projected that mobile payments volume worldwide will mushroom from $60 billion in 2012 to $545 billion by 2015.[32]

Some retailers are taking small steps within the 'mobile acceptance' realm by replacing cash registers with mobile devices such as iPads (for example the Apple Store), or equipping sales personnel with handheld credit card scanners. Such small changes are often well received by consumers as they do not revolutionise payment methods but enable the sales personnel to move around the store to assist with customers and complete the transaction. Furthermore, from a retailer point of view they do not involve an in-store footprint that a kiosk or checkout counter would, freeing up space for more product and advertising.

Mobile payment instruments have the potential to increase both the convenience of payments and lower the transactions costs. Yet, the use of mobile payments by the retail sector has been forestalled by the uncertainty of their advantages and the success of the new technology. In particular there are a number of issues around consumer adoption and whether they can deliver on promises of convenience, versatility and most importantly, security. The question that emerges is:

How do 'brick and mortar' retailers utilise mobile payment systems to harness the benefits of mobile commerce whilst minimising the impact on shrinkage?

2.8 Mobile technologies and sources of shrinkage

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 mobile POS (such as network/Wi-Fi interruption, battery failure and inability to scan items). This category is renamed '**Internal technological and process issues**'.

In terms of **inter-company fraud**, there is little to suggest that mobile technology should increase inter-company fraud. However, the validation technologies and processes potentially implemented to enable the use of m-POS payment options might result in a diffusion of benefits that reduces the incidence of **inter-company fraud** through ease of detection.

In addition, a further category of shrinkage '**fraudulent activity**' is added.

There are also concerns around m-POS 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 report. 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.

03. THE CASE FOR MOBILE PAYMENT: BENEFITS AND OPPORTUNITY

If retailers want to stay relevant in the multichannel shopping environment, technological innovations need to be understood. Mobile payment is a key piece of the jigsaw as a means of 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.

Available information on mobile POS and multichannel retail has largely focused on the positive marketing and sales opportunities they present. In particular; 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. There have also been a number of industry publications dedicated to exploring barriers to customer adoption. However, 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.

Industry and trade publications reflect the excitement about the sales and marketing opportunities that mobile POS can offer. As an integral part of multichannel retail, mobile technologies can provide a range of touch points to connect with, tempt and retain customers. Furthermore, mobile devices offer functions not available with plastic cards, such as using geo-location technology to alert consumers of deals at nearby stores. M-scan and m-POS bring with them 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 retailers that the introduction of mobile payment technologies was customer driven, and there was a firm belief amongst the majority of the companies represented that there was a compelling case for diversifying payment options beyond traditional staffed checkouts and SCO. Some of the main benefits of mobile payment options, and the various associated functionalities are outlined below.

Margin improvement: Staff mobility & increased sales

As with SCO, there is the potential for retailers to use mobile payment as a way to leverage savings on their biggest recurrent cost – staff (although it is recognised that increased staff training might negate savings, particularly during formative implementation phases). Given the relatively high costs of staff in Australia[33] this is particularly pertinent. 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 at a SCO.[34]

The best outcome is rather than an overall reduction in staff, retailers are able to redeploy staff to perform value-added customer service that increases sales (as has been highlighted by IBM in relation to SCO).[35]

The potential to reinvest staff time into the provision of a range of services for customers was viewed as a key benefit amongst stakeholders. Mobile POS 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.

'Endless aisle'

The introduction of mobile devices that can link directly to store inventories and catalogues has been highlighted as a key benefit. Whereas previously, stores would have to access store inventories from fixed locations, or telephone stores to check stock, customers are able to establish availability of items in other stores relatively quickly. In addition, marketing can be wrapped around products e.g. highlighting that there is also a matching pair of gloves available to the scarf that the customer has shown an interest in. In this respect, the mobile device is transformed into a virtual personal shopping assistant.

Whilst there are clearly benefits to increasing the footprint of the store via endless aisle or virtual online presence, it has been argued that this can also counter-intuitively reduce sales. It has been argued that 'putting the means for endless research in the palm of the consumer's hand reduces conversion almost as often as it lifts sales'.[36]

Also, similar to SCO, there is the potential for lost revenue in impulse buys, particularly those that take place at the traditional checkout.[37]

Overall, for retailers that are looking for new avenues of growth, bringing the online shopping experience into the brick and mortar store is an attractive proposition. Customers can take advantage of the endless aisle to search online for greater choice than what is available in store, with enhanced options for reserving items, purchasing add-ons or complimentary products and choosing to pay in situ. Furthermore, retailers can build in options around home delivery or collection.

Marketing and Loyalty programs

In addition to payment, mobile systems can also be used by retailers to collect customer behaviour and feedback-related information to enhance customer relationship management (CRM). For example, NFC-enabled smartphones contain an RFID reader which means it is able to detect products and provide customers with instant services.[38] Retailers can now signpost customers to their other branches, indicate stock levels, provide personalised offers, and respond in a predefined way to priority or frequent customers. This ensures that loyal customers are rewarded with an enhanced customer experience, tailored to their needs - potentially increasing conversion rates.

Mobile ticketing technology can be used for the distribution of vouchers, coupons, and loyalty cards. These items are represented by a virtual coupon that is sent to the mobile device. A customer presenting a mobile phone with one of these vouchers at the POS will be rewarded with the offer. An exciting development is the ability of stores to send coupons to customers using location-based services that determine when the customer is nearby.

Consumer profiles and marketing

The compilation of customer profiles and shopping habits offer huge potential for marketing and providing personalized recommendations to customers that relate to their purchase history. Not only can suggestions be made for future purposes that fit the profile, more 'softer' information can be compiled to greater understand the dynamic of the customer. For example, length spent in store and conversion rate could infer their shopping motivation; whether purely functional or seeking out a shopping 'experience'.

Real time analytics

Mobile payment can enable the use of real-time analytics data e.g. what products are selling well and what products are frequently being purchased together. In the apparel environment, this has the added dimension of being able to report this information back to customers in order to advertise what items are currently trending, thus creating added buzz around particular items. In the FMCGs sector, such as health and beauty, the purchase of a new razor could flag to the individual the need to purchase shaving foam, for example. Mobile devices can be used to provide a continuous feed of data, tracking the shopper journey through the store and measuring amounts of time spent in different categories, alerting store associates to the possibility of a profitable sale.

Simplicity and speed

There are many ways that mobile technologies are able to create efficiencies in the customer journey. For example, in the supermarket, customers can place orders at the deli via a touchscreen pad and then be sent a SMS text or other communication when it is ready to collect.

04. IDENTIFYING VULNERABILITIES, PROBLEMS AND RISKS

Retailers must be able to navigate the complexities of the payments ecosystem effectively if they are to mitigate loss. There are many ways in which mobile scanning and POS present challenges for the retail environment of the future.

Both malicious and non-malicious actions of customers and staff in-store can result in significant direct losses for retailers due to the theft of product, and/or the product not being available for purchase to legitimate customers. Malicious activities refer to deliberate mechanisms for taking product without paying, or paying a reduced price such as intentionally not scanning an item or switching the labels on products so that a lesser price is paid.

Non-malicious activities refer to system errors or software problems that can cause the customer to pay an incorrect amount. There is of course a blurring of the lines between malicious and non-malicious activities, with customers often developing justifications for their actions, such as 'the product wouldn't scan', 'I thought it had been processed', or they incorrectly identified the item on the screen etc.

This section is divided into the following potential risks:

Main Shrinkage considerations

- External theft
- M-Commerce and fraudulent activity
- Internal technological and process issues

Additional risks

- Brand protection and consumer confidence
- Privacy and data protection

4.1 External theft

There are many different techniques used by shoplifters, but most studies show that shoplifting usually occurs throughout the store, in aisles and blindspots, 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.

M-scan and M-POS increase the autonomy of the customer, relying on them to correctly scan all items selected for purchase. Furthermore, a correlating decrease in staff (as occurred with SCO) reduces the number of 'capable guardians' that can identify, and importantly intervene, when an item has been misappropriated.

Non-scanning of items

As with SCO, the use of mobile devices presents issues regarding the non-scanning of items. It has been found in previous studies on shrinkage related to SCO that some customers with deliberate intent to steal will mime the scanning action whilst shielding the barcode. To an untrained eye, the 'customer' appears to be performing the scanning process satisfactorily.

Surveillance and Control at checkout

In order to combat deliberate non-scanning, many retailers use video-analytics alongside staff that are trained to recognise common deception techniques. Furthermore, the channelling of customers into a contained area enhances the perception that there is a level of monitoring taking place which registers on the would-be thieves' risk-reward analysis (particularly opportunists).

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.

Whilst some individuals enter the store with the intent of stealing other customers might leave 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.

There is a need therefore to establish new means of verification. This is looked at further in the report under 'Techniques of payment validation'.

Can't scan, won't scan: the perpetual risk of the struggling customer

Customers-turned-thieves often develop 'techniques of neutralization' to justify leaving the store without paying for goods, or for paying a lesser price. Such excuses often include:

"The item wouldn't scan"

"The barcode was damaged"

"I couldn't find the [loose] fruit/vegetable so I selected the closest one"

New technologies invite this type of behaviour as customers who do intend to pay for items believe that they should somehow be 'compensated' for the difficulties they have encountered during the transaction.

It is unknown the degree to which once having gone undetected for a minor transgression, legitimate customers become more habitual thieves. There needs to be staff on hand to recognise struggling customers before they even realise they are struggling themselves.

'Walking'

Research has inferred that SCO increased the occurrence of 'walking'; 'customers' leaving the store with goods they have not paid for with no attempt to stop at SCO or staffed lanes. The reason for this is that SCO are designed to enable the free movement of customers through them. As such, the self-service area is often spacious and may permit thieves to exit more easily, particularly if staff are occupied with another customer.[39] Research suggests that most determined thieves find a method of secreting items upon their persons or in bags whilst in the aisles, rather than choosing to steal at the POS.

Similarly this is likely to be an issue with mobile scanning and payment. Again, 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.

'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.[40] Furthermore, a 2012 survey of 800 customers and employees found that 67% said they had participated in sweethearting in the previous two months.

The practice 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 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.

Diffusion of Responsibility

Consultation with loss prevention managers revealed concern about the fragmentation of responsibility across manufacturers of devices, developers of operating systems, application designers, network carriers, and the retailer.

In another way, it is envisaged that 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/somewhere else and not feel that it is their role to intervene should issues arise.

4.2 M-Commerce and fraudulent activity

"New smartphone POS systems represent lower hanging fruit for attackers"[41]

Mobile payments are still in their infancy and as such the true extent of fraud issues has yet to be defined. However, due to the content it is envisaged that these services will be extremely attractive to fraudsters. 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.[42] Just some of the ways that mobile payment can create avenues for fraudulent activity include:

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.

Shoulder surfing

Shoulder surfing is a security attack where information such as passwords or PINs are obtained by watching the user enter them into a device, and then stealing the card or device to use it fraudulently.

Repudiation fraud by subscribers

The uncertainty around mobile payment in its early roll out might increase the number of false claims that a transaction was not made by the customer. 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.

Fraudulent coupons

In some cases, digital coupons are easier to counterfeit, so care must be taken to ensure that coupons are redeemed as the program intends. Similarly, vouchers or discount codes transferred to the customer's device could be intercepted or duplicated.

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. This raises a bigger 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.

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 m-POS, at least in the short-term before protective security solutions have matured.

Card not present

A card not present transaction is a transaction made where the cardholder is not physically present with the card. Many networks consider mobile solutions to be card not present transactions. 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 in Australia, some major players are looking to enhance their protection policy for merchants. For example, from 11 October 2013, PayPal 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.[43]

> We have to take the same protocols we use in the card-present environment. Meaning that, if someone is using their e-wallet for the first time, they have to physically present their card and the merchant has to physically identify that consumer as an authenticated consumer. It's one of the simplest procedures to do.
>
> (Paul Tomasofsky, Secure Remote Payment Council)

4.3 Internal technological and process issues

Technology failures produce negative customer experiences, frustrate staff and impact on sales. Mobile technologies introduce a raft of new considerations that could potentially impact on the bottom line.

Wi-Fi connectivity

If retailers are to embrace mobility as an integral part of their strategies, they will need to outfit their stores with public Wi-Fi access as a cornerstone of those strategies. 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.

Charged and ready to go?

Mobile technologies introduce 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).

EAS tagging

Currently the deactivation of EAS or the removal of hard tags requires an intervention that will interrupt the fluidity of mobile payment. There is a need to move towards security devices that can be deactivated upon payment. For example, RFID can track the product in store and be deactivated once the payment has been processed.

Age-related products

As above, products that require customers to be of a minimum age for purchase 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 or Medicare card).

4.4 Brand protection and consumer confidence

The integration of m-scan and m-POS into seamless multichannel retail offers up many potential benefits, but retailers must be cognisant of the risks to ensure they maintain a positive point of differentiation from competitors. Retailers are increasingly presented with a compelling case to embrace technological innovations, such as m-POS, 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 numerous considerations for retailers with regards to the impact on their brand's culture 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.

Consumer confidence

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.[44]

There are a number of defensive measures that retailers can take to increase confidence and safeguard data should a customer's device be stolen or compromised, such as;

- **Wipe data**: Consumers are particularly eager to have the ability to wipe their device clean and replace their mobile wallets easily and instantly.

- **Identity verification technology**: high-tech protection measures, such as requiring fingerprint identification technology in order to gain access to the mobile wallet, or simply a PIN or signature movement.

- **Data storage**: data stored remotely in the cloud, rather than on the device.

Not only will such preventative security measures offer customers peace of mind, but many report that they'd be far more willing to use all the capabilities of a mobile wallet.

A recent comScore study found the largest share of consumers (44%) preferred a mobile wallet that had a PIN or password protecting access. PayPal has adopted this model in its trials with retailers including Home Depot, Foot Locker and JCPenney.[45]

Privacy and data protection

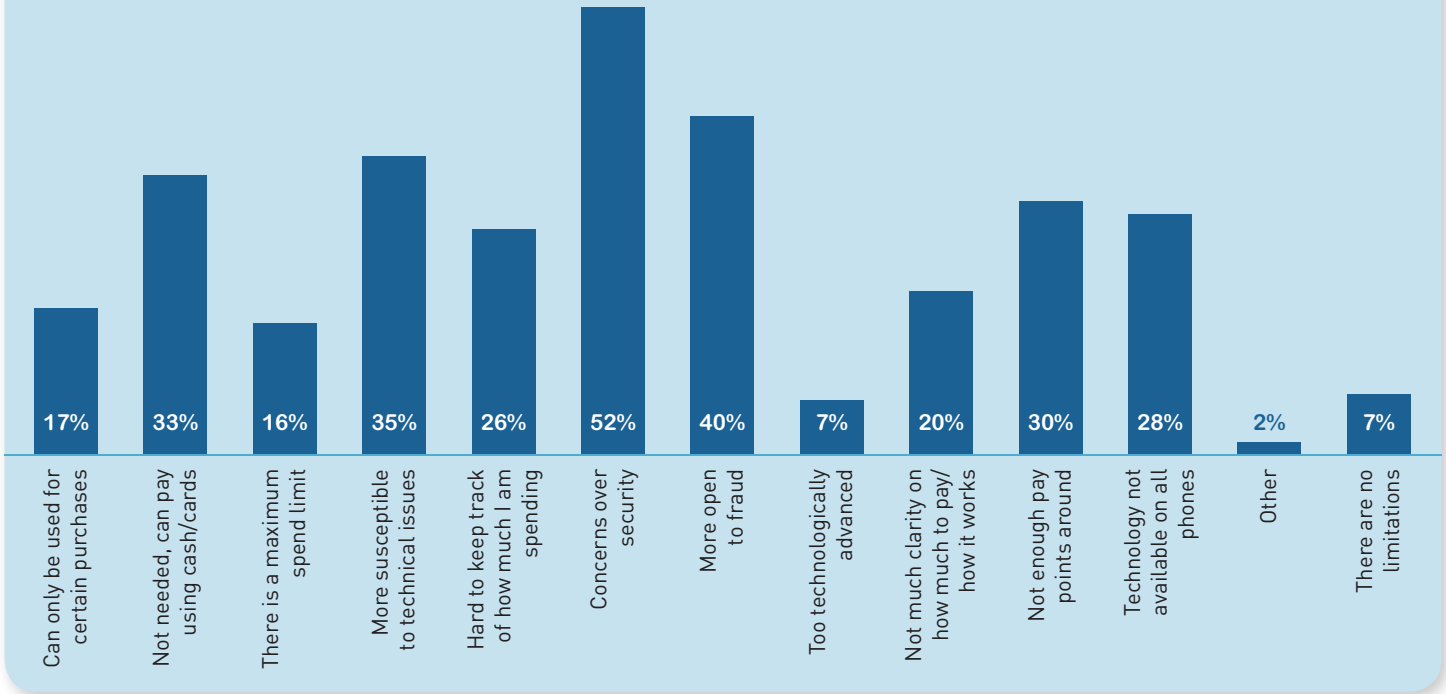
All of a sudden the mobile phone is about to be transformed beyond a spy in your pocket to your bank, your mortgage lender and your landlord.

(Jeffrey Chester, Executive Director, Centre for Digital Democracy)

There are clearly concerns about the data protection and privacy assurances provided to consumers using their mobile devices for retail purposes. It is reported that many individuals are holding back on utilising technological innovations because of security and privacy concerns, despite the appeal of quick and simple transactions.

Just some of the barriers to consumer adoption are outlined in the table below.

What do you see as the limitations of using Contactless Mobile Payments to make purchases?[46]



Security solutions are going to play an integral part in product protection in the multichannel retail environment of the future, particularly as customers and POS become more mobile.

From a loss prevention perspective, the technologies (such as RFID) that enable mobile POS systems can also be deployed as powerful tools for shrinkage management. One industry white paper suggests that use of smartphones as payment devices may actually decrease the risk of customer theft from retailers, since authentication and authorization processes may be more sophisticated than those of existing payment methods.[47]

The providers of product protection equipment need to work closely with manufacturers of mobile payment technologies to ensure that problems that continue to be experienced with devices such as EAS tags can be addressed.

To catch a (rational) thief

The rational thief weighs up the benefits and risks of a crime before committing the act, and chooses the course of action that maximises gain whilst minimising risk and the potential for loss. Increase the risks – reduce the losses.

While just 0.37% of Australian retail sales is spent on installing more robust security solutions, such as electronic article surveillance (EAS) and secure merchandising products, there is an ongoing need to continue to evolve more sophisticated and creative security solutions in an increasingly mobile environment.

Zones of control

It has been suggested in relation to SCO, that retailers need to create 'zones of control' around the POS. Zones of control 'maximise modes of surveillance and the design of the SCO space, to impact upon perceived risk and likelihood of apprehension'.[48]

Recommendations for creation of zones of control around SCOs stipulated that:

- Stores create a separate self-checkout space which feels 'enclosed', and that controls customer movement and limits entrance and exit; this could include moving the SCOs away from the entrance/exit area.
- The space is carefully monitored (staff surveillance; CCTV and public view monitors; technological monitoring through till-based alerts and alarms).
- Self-scan supervisors are appropriately trained and responsible for a maximum of 4 self-scan kiosks at a time.[49]

In the multichannel retail environment of the future it becomes harder to create zones of control. As the 'customer journey' illustrates, there is considerable disconnect in the predictability of location for potentially high risk activities such as checkout. As customers get mobile, so the safeguards and protections must do so too.

5.1 Techniques of payment validation

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

- **Bag and receipt checks**

  Whilst relatively common in the Australian sector, 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, or they might feel embarrassed if buying items of a personal nature and 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. Staff can also become complacent about looking for suspicious activity via any other means.

- **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.

- **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.[50] RFID embedded in a counter/platform at the POS kiosk can register all items in the shopper's bag or basket virtually instantaneously[51] and deactivate tags of registered items. When used at exit points, RFID-enabled security antennae detect tagged items that pass through the store without having been scanned.

Nespresso (Sydney) RFID scales

Customers receive a branded Nespresso bag on arrival in the store. After selecting the desired items, customers place their bag on a scale to automatically calculate how many items have been chosen. RFID tags on the individual packs allow the POS to determine which items are being purchased, and this information is displayed on the screen. At the point of purchase, the customer is assisted by staff. The RFID tags act as theft prevention, as they activate the alarm sensors at the exit if the tags have not been deactivated.[52]

Studies of the application of RFID for loss prevention have also demonstrated its value in controlling shrinkage via eliminating return merchandise fraud, improving supply chain security and reducing theft.[53] A recent publication detailed a new system for preventing 'ticket-switching' in apparel stores – where the customer pays less than an item's price because of a deliberate or inadvertently switched label. The solution utilised item-level RFID-tagging items in combination with authentication protocols.[54]

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.[55]

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.[56] However, within the apparel industry (e.g., American Apparel; Zara) there has been an increase in retailers placing item-level RFID tags throughout the store to enable complete real-time visibility of all items.[57] 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.

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.[58] The research found that 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.

Training

Training was regarded as one of the key defences against shrinkage in consultation with retailers. The introduction of new functionalities in the retail environment can be considered to be an arms race against those with malicious intent. Importantly, training should ensure that all employees feel equally responsible for identifying, targeting and preventing retail crime.

In relation to SCO, it has been found that clerks and cashiers manning 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.[59] This new emphasis on security and the loopholes of new technologies must be reflected in training.

A research Agenda

- Customer confidence in new mobile solutions is imperative. Focus groups and interviews across different demographic groups will provide useful indicators to inform roll out strategies. Consultation should include perceptions of security, data protection, impact on privacy and tolerance for different techniques of payment validation.

- Devising a 'red team' to find security vulnerabilities will help retailers find weaknesses in their systems and processes before the criminals do. New infrastructure presents an arms race for security, and retailers need to stay ahead of the game.

- As POS diversifies, pen-testing should be conducted to develop a databank of likely theft and manipulation scenarios.

- Fraud is a very real vulnerability as fraudsters migrate to what they see as a soft target, at least in the early days of implementation. Being alert to fraudulent activity and building resilience in to systems is essential.

Technology and software

- Retailers need to align mobile solutions with customer demographics and business need. There are no clear market leaders in mobile retail solutions which presents some risk for early-adopters.

- Trialling new modes of tag removal and age verification that doesn't undermine the flow of the mobile customer is important to maintain a positive point of differentiation from competitors.

Training

- As with SCO, investing in quality and frequent training for staff will be a key tenet of any loss mitigation strategy. All staff should have a remit for loss prevention, thus avoiding a diffusion of responsibility as the customer journey undergoes disconnect.

- Refresher training is particularly important in the fast-moving technological solutions domain.

Store layout and design

- Store layout can have a demonstrable impact on its perceived vulnerability. The store will need to be reconfigured to accommodate increasingly mobile customers whilst building in sophisticated security, particularly at the point of exit to provide robust payment validation.

- Store layout will need to encourage customers to move in predictable flows and channel them through a validation point.

07. CONCLUSION

The introduction of any new technology, service or process will generate a host of new problems, risks, vulnerabilities, security concerns and training needs.

The onset of the mobile customer will similarly bring with it a new cache of shrinkage problems.

Retailers will need to pre-empt these issues if they are to respond to the customer-driven changes whilst protecting the bottom line.

It is clear that there are many benefits to mobile payment systems, particularly in terms of the wrap-around services and rewards that can be built into them. However, a key point is that they signal the convergence of financial services with telecommunications and the risk this presents should not be understated.

The manufacturers of devices, developers of operating systems, application designers, network carriers, and the retailer all need to ensure that they work together to recognise the risks and embed resilience in system designs. This requires particular attention as the impact of payment fraud and risks can be far reaching. Customer confidence in these systems in hinged on ensuring that they are secure from the outset.

Despite conflicting evidence regarding the benefits and limitations of SCO, it is widely recognised that consumer-oriented payment systems represent an enduring feature of the retail environment, and the onset of mobile payment is testimony to this.

APPENDIX: METHODOLOGY

The methodology consisted of several activities:

(i) Workshop

The focus of the report builds upon the findings from a one day workshop held at the University of Technology Sydney in May 2013 (see report for further details).

(ii) Literature review and scoping exercise

A literature review of academic research papers, industry documentation and reports was completed. Reflecting the relatively new adoption of mobile payment in the retail sector, there was a lack of academic literature that specifically addressed loss prevention. The relationship between shrinkage and new mobile payment technologies was featured in a number of industry/trade publications. It was found that academic literature on mobile payment systems in the retail context focuses mainly on the technical aspects of the technology and implementation models; sales and marketing opportunities; and analysis/projections of customer acceptance.

(iii) Consultation

Consultation took place with industry professionals working within loss prevention, asset protection, and business development. Ten individuals were consulted with via telephone interview, representing seven different companies. The interviews took place between mid-August and end of September 2013. In addition, academic experts in the area of loss prevention were consulted with to scope the current knowledge and understanding around new technologies and their relation to shrinkage.

REFERENCES

[1] Dahlberg, T. et al (2008) 'Past, present and future of mobile payments research: A literature review', *Electronic Commerce Research and Applications* 7 (2008) 165–181.

[2] The term 'shrinkage' is used to denote 'losses suffered by retailers due to internal and external theft, process failures and inter-company fraud, including both known and unknown losses'. Beck, A. (2011) *The Impact and Control of Shrinkage at Self-Scan Checkouts*; An ECR Europe White Paper.

[3] 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), p.43.

[4] 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).

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

[6] *Mobile Payment Acceptance Solutions; Visa Security Best Practices*. Available at: http://usa.visa.com/download/merchants/bulletin-mobile-best-practices.pdf (accessed: 21.10.13)

[7] Burghardt, B. et al (2010) *Near field Communication: Organising Everyday Life Intuitively*. BMW Forschung und Technik GmbH. Available at: http://www.future-store.org (accessed: 21.10.13).

[8] Google Wallet recently released an updated version of the app for all Android phones version 2.3 and higher, and to AT&T, T-Mobile and Verizon subscribers, which will not have an NFC component. However, there are still several banks and card companies signed up with Isis, the telecom companies, and NFC payments programs continue to be announced.

[9] Yarbrough, S. and Taylor, S. (2012) *The Future of Payments: Is it in the Cloud or NFC? Regardless of Your Conclusion, It's About Consumer Choice and Control*. Available at: www.tsys.com (accessed: 16.10.13).

[10] The Metro Group Future Store Initiative is a cooperation between companies from the retail, consumer goods, IT and service sectors. The aim of the group is to drive the modernization process in the retail sector. More than 75 partners develop and test innovative technologies and real-world concepts. See www.future-store.org.

[11] The Fresh & Easy Neighborhood Market has been trialling a mobile scanning solution in stores in California. The 'Scan As You Shop' handheld device allows shoppers to scan products as they shop, keeping track of what they spend. Fresh & Easy also has a mobile app integrated with their loyalty programs.

[12] For more information see: 'eTile: 19" InStore Tablet + Intel i7', *Channel News Australia*. Available at: http://www.channelnews.com.au/business/YRPIYTHY.aspx (accessed: 20.10.13).

[13] Nordstrom has embraced mobile technologies as part of its multichannel strategy. It has introduced shopping apps, on-the-spot item location and register-free transactions. As it states on the Nordstrom website, they have 'put the entire Nordstrom experience squarely in the hands of customers, where they're finding countless ways to share it, Tweet it, Pin it and make it their own' (www.nordstrom.com).

[14] http://www.qthru.com

[15] Walmart's 'scan and go' mobile app lets users scan items with their iPhones while shopping and then pay at a self-checkout kiosk. Walmart rolled out the pilot to 200 stores in March 2013. The app doesn't allow customers to use mobile devices to complete purchases yet, but Walmart is part of a consortium of retailers (including Best Buy, Target, and Lowe's), that is working on a new mobile-payment service called Merchant Customer Exchange (MCX).

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

[17] Beck, A. and Peacock, C. (2009), *opp cite.*

[18] Chapman, P. and Templar, S. (2006), *opp cite.*

[19] 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)

[20] Davis, S. (2012, June 18). Thefts from self-service checkouts a concern warns expert. *Australian Broadcasting Corporation. abc.net.au.* Available at: www.abc.net.au/local/stories/2012/06/18/3527801.htm (accessed: 28.10.13).

[21] NCR (2012) *How Self Checkout can Impact Retail Shrink; An NCR White paper*. NCR Corporation.

[22] For example, see; Beck, A. (2011) 'Self-scan checkouts and retail loss: Understanding the risk and minimising the threat', *Security Journal. 24*(3), 199–215.

[23] Beck, A. (2011) The Impact and Control of Shrinkage at Self-Scan Checkouts; An ECR Europe White Paper.

[24] For example, see Evans , J . and Dayle , E . (2009) Self scanning: Profit or loss? RILA Auditing and Safety Conference. Orlando: RILA.

[25] In June 2010, Tesco Express in Kingsley, Northampton, became Britain's first self-service only store. It had a total of five self-service checkouts overseen by a single member of staff but no staffed checkouts. Tesco described it as an 'assisted service store' designed to increase efficiency and speed up the shopping process.

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

[27] Adapted from Beck /ECR Europe (2011), *opp cite*.

[28] PCI Mobile Payment Acceptance Security Guidelines (2013).

[29] Au & Kaufman (2006) 'The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application', *Electronic Commerce Research and Applications* Volume 7, Issue 2, Summer 2008, 141–164.

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

[31] Business Insider (2013) *Why mobile payments are set to explode*. Available at: www.businessinsider.com.au/why-mobile-payments-are-set-to-explode-2013-5 (accessed: 21.10.13).

[32] Walsh, M. (2013), *opp cite.*

[33] Currently the full-time adult minimum wage is $16.37 per hour or $622.20 per week in Australia, compared to £6.31 per hour ($10.65 AUD) in the UK for example.

[34] 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).

[35] IBM (2008), *opp cite.*

[36] Interbrand (2013) 'Untapped Potential in Digital'. Available at: www.interbrand.com

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

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

[39] 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, J. (2012). *Shopping and Crime* (p. 325). Palgrave Macmillan.

[40] Brady, Voorhees, & Brusco (2012) 'Service Sweethearting: Its Antecedents and Customer Consequences', *Journal of Marketing*, 76: 2.

[41] 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).

[42] Hayes, F. (2013) 'Mobile Retailers Hit Hardest By Payment-Card Fraud—And Many Have Given Up', *FierceMobileRetail*. Available at: www.fierceretail.com/mobileretail/story/mobile-retailers-hit-hardest-payment-card-fraud-and-many-have-given/2013-09-25 (accessed: 21.10.13).

[43] 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)

[44] Russell & Sapienza (2013) 'Opening the Mobile Wallet: Consumer Sentiment Around Mobile Payments', *Huffington Post*. Available at: www.huffingtonpost.com/russell-j-sapienza-jr/mobile-wallet_b_3989997.html?utm_hp_ref=business (accessed: 04.10.2013).

[45] Walsh, M. (2013), *opp cite.*

[46]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).

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

[48] Beck, A. (2011). Self-scan checkouts and retail loss: Understanding the risk and minimising the threat. *Security Journal*, 24(3), 199–215.

[49] Ibid.

[50.] Gozycki, M., Johnson, M. E., & Lee, H. (2004). *Woolworths "Chips" Away at Inventory Shrinkage through RFID Initiative*.

[51] A recent RFID self-payment kiosk technology permits an RFID reader to identify the contents of a shopper's basket in approximately one second. See: Swedberg, C. (2013, May 10). IER's Expedited Self Payment Kiosk Speeds Up Checkouts - RFID Journal. *RFID Journal*. Available at: http://www.rfidjournal.com/articles/view?10667/2 (accessed: 21.10.13).

[52] Avenell, P. (2013). Nespresso launches self service POS terminals, flags same day delivery. *www.current.com.au.* Available at: www.current.com.au/2013/07/08/article/Nespresso-launches-self-service-POS-terminals-flags-same-day-delivery/DMZEDYKAID.

[53] 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* (JABR), 21(2).

[54] Zhou, W., & Piramuthu, S. (2013). Preventing ticket-switching of RFID-tagged items in apparel retail stores. *Decision Support Systems*, 55(3), 802–810.

[55] Burnside, W. D., & Ryan, J. M. (2013, May 10). Shelf-monitoring system. United States of America. Available at: www.google.com/patents/WO2013032697A3?cl=en.

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

[57] Zhou, W., & Piramuthu, S. (2013), *opp cite.*

[58] Cardone, C., & 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*, 7(1), 22–58.

[59] Andrews (2009), *opp cite*.

The Australian National University

December 2013