University of Leicester

Developments in Retail Mobile Scanning Technologies:

Understanding the Potential Impact on Shrinkage & Loss Prevention

A Report by

Professor Adrian Beck
Dr Matt Hopkins

Department of Criminology,
University of Leicester

E·S·R·C
ECONOMIC
& SOCIAL
RESEARCH
COUNCIL

Developments in Retail Mobile Scanning Technologies:

Understanding the Potential Impact on Shrinkage & Loss Prevention

A Report by

Professor Adrian Beck
Dr Matt Hopkins

Department of Criminology,
University of Leicester

E·S·R·C
ECONOMIC
& SOCIAL
RESEARCH
COUNCIL

Disclaimer

This publication has been written exclusively by academics from the University of Leicester and not by any of the retailers that agreed to take part in this research. The document is intended for general information only and is based upon data provided by a number of retailers in Europe and the USA. Companies or individuals following any actions described herein do so entirely at their own risk and are advised to take professional advice regarding their specific needs and requirements prior to taking any actions resulting from anything contained in this publication. Companies are responsible for assuring themselves that they comply with all relevant laws and regulations including those relating to intellectual property rights, data protection and competition laws or regulations.

About the Authors

Professor Adrian Beck is currently Head of the Department of Criminology at the University of Leicester. Over the last 25 years his research work has focussed on loss within the retail sector. He is currently an academic advisor to the ECR Europe Shrinkage and On-shelf Availability Group.

Dr Matt Hopkins is a Senior Lecturer in Criminology at the Department of Criminology at the University of Leicester, UK. His research has focused on commercial victimisation, organised crime and crime prevention. He currently sits on the UK Home Office Commercial Victimisation Survey Steering Group.

The authors would like to express their gratitude to all the respondent that agreed to participate in this research – your patience and support was very much appreciated.

The Department of Criminology
University of Leicester
154 Upper New Walk, Leicester
LE1 7QH, UK
Email: Professor Adrian Beck, bna@le.ac.uk
Dr Matt Hopkins, mh330@le.ac.uk

The researchers would like to thank the ESRC for their financial support for this project (Retail KE Opps Grant 2013, ES/L005085/1) and in particular Bruce Jackson, Senior Knowledge Exchange Manager. We would also like to thank Professor Kim Cassidy and Nelson Blakely for their valuable support and advice.

E·S·R·C
ECONOMIC
& SOCIAL
RESEARCH
COUNCIL

Contents

Executive Summary

This report presents the findings of an ESRC-funded study conducted between December 2013 and February 2015. The primary focus was to identify current developments in mobile scanning technologies in the retail space; to understand how allowing customers to use their own personal mobile phones to scan and pay for items could impact upon shrinkage and also identify how crime prevention might be integrated into these systems. The methodology was based around interviews with staff involved in the development and implementation of mobile scan and pay systems across four retailers in the UK, two in the USA, one in Belgium and one in Holland. Loss prevention staff were also interviewed and analysis of shrinkage data from one retail partner was also conducted.

The key findings are:

1. Development and Perceived Benefits of Mobile Shop and Pay

- Mobile scan and payment is at an early stage of development across most retailers. At present, the focus is mainly on developing a mobile scan option only rather than one that also enables payments to be made via an App (a mobile wallet option).
- There is some evidence that customer appetite for MSP is limited. Indeed, there was a suggestion that in some locations and for some demographics the move to MSP might represent a cultural shift that could be slow to be adopted.
- The potential benefits for customers are thought to be numerous. Not only could MSP make shopping easier and quicker – through the elimination of the need to use traditional checkouts – it can also offer ways to 'personalise' the shopping experience. This can be done by offering consumers the opportunity to create shopping lists, view their purchase history, receive information on real time store offers, have access to store maps and product searching functionality, and receive and use electronic vouchers, all through an App on their mobile device.
- Respondents also identified numerous potential benefits for retailers. MSP could enable more staff to be utilised away from checkouts and on to more customer-focussed services such as in-aisle assistance. It also offers the potential for a reduction in the overall staff hours allocated to stores and the costs associated with using and maintaining traditional checkout technologies. MSP was also thought to offer greater opportunities to provide customers with forms of loyalty bonuses and exclusive product offers, and to collect valuable data on shopper behaviour to better inform future business planning.
- The research found that there are a number of technological and process challenges that need to be overcome before MSP can be rolled out across most forms of retailing. At present MSP systems are normally limited to Apple devices, Apps can run slowly and scanning barcodes with a mobile device can be difficult. The shopping process is slowed down when age restricted products, or security protected products are purchased (as a member of staff has to intervene). At present, the lack of a payment wallet option means in most retailers that0 MSP users still have to find and use a fixed payment terminal, undermining the perceived benefits of speed and ease of use.

2. The Potential of MSP to Generate Retail Losses

The research found that MSP might generate retail losses/problems in four ways – theft through malicious non-scanning of goods; non-malicious loss through non-scan/scanning errors; physical and verbal abuse against staff generated via audit checks or system errors; or transaction frauds/fraudulent use of payment wallets. In summary:

- MSP potentially promotes ease of effort for theft by removing any human contact throughout the shopping process and removing (possibly most importantly) human contact at the final payment stage of the shopping journey (when a payment wallet option is provided). In the MSP environment, the sense of risk perception or control is reduced as all elements of the customer journey can be completed without human interaction. Some respondents thought that offenders might be attracted to stores in the knowledge that they can chose to not scan certain products with relatively little risk of being caught.
- MSP gives offenders 'ready-made excuses' for non-scanning behaviour – the self-scan defence. Giving customers the freedom to self-scan gives them the opportunity to blame faulty technology, problems with the product barcodes or claim that they are not technically proficient as reasons for non-scanning.
- Proving intent is difficult where customer non-scanning is identified and deciding whether prosecutions can be made or not is potentially a legal and customer relations minefield. It is proving

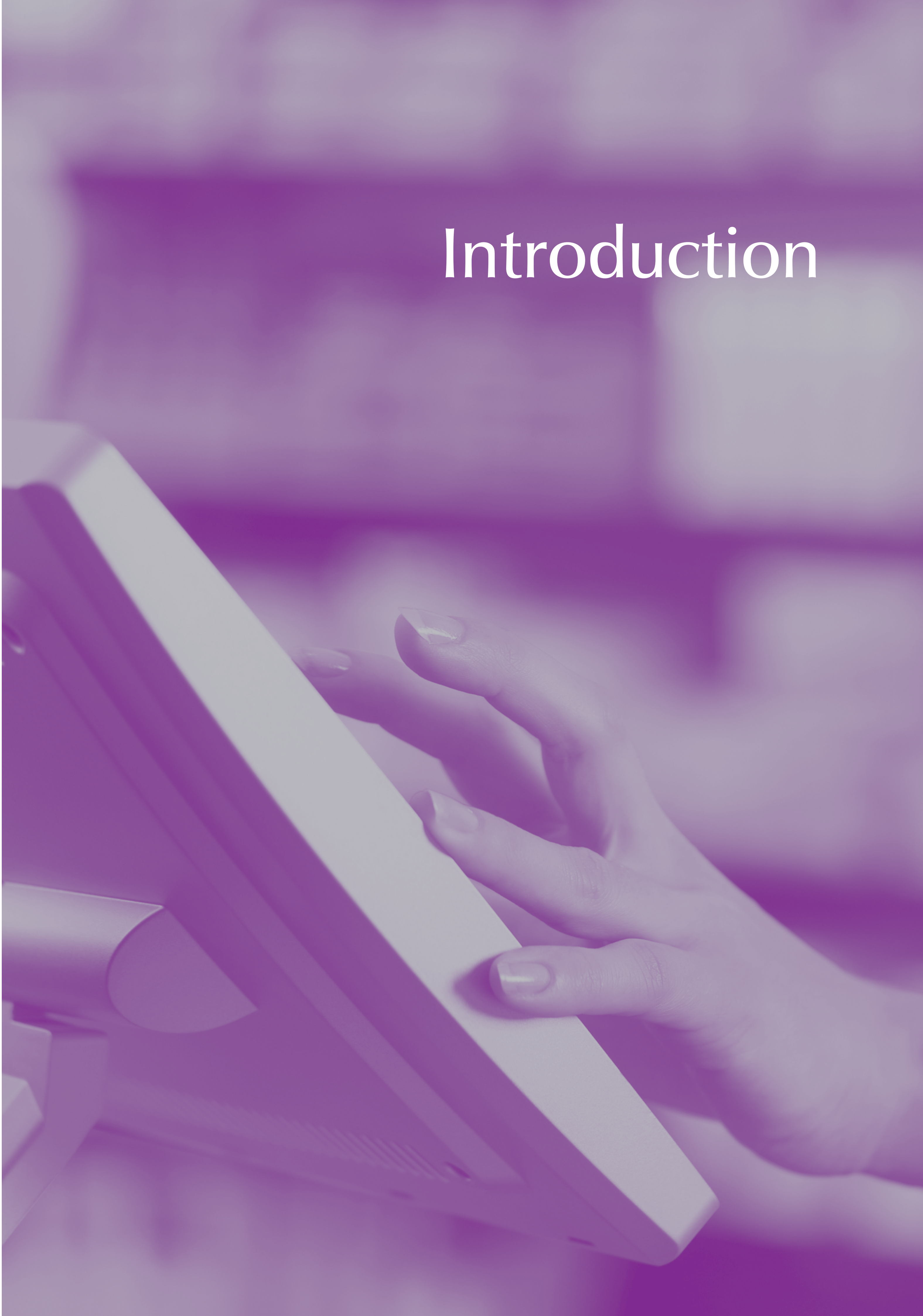
difficult for retailers to identify whether customers intended to non-scan items or if they were simply absentminded and or poor at scanning items consistently. This could be further compounded when the point of payment becomes blurred by consumers having the option to pay at any location within and potentially around the store.

- MSP could also generate provocations for aggressive behaviours. At present, there are a number of frustration points in the MSP shopper journey that could trigger disputes with staff – when products will not scan correctly, when staff have to intervene to remove EAS devices/do age verifications, when payment wallets will not work and when a check audit is requested.
- There were some concerns around the potential for fraudulent activities, including the production of self-scan labels that might be stuck on products and the potential for fraudulent payments. It was thought that the payment wallet could generate fraud such as being used with stolen credit card details or the use of fraudulent electronic vouchers or coupons via this type of technology.
- Concerns were expressed that non- and mis-scanning of items could have a detrimental 'knock on' effect in relation to inventory accuracy and on-shelf availability of stock. Thieves are notoriously unreliable when it comes to updating stock levels when they take products and customers may not readily appreciate the impact of scanning the same item multiple times when a range of similar varieties are actually being purchased.
- Available data indicates that mobile scanning technologies, including MSP, generate significantly high rates of loss (3.97% as a percentage of turnover), more than 122% higher than the average rate of shrinkage – greater than the typical profit margin (approximately 3%) of the European Grocery sector. The data suggests that if these rates of loss are typical then this type of 'service' is not likely to generate a high profit margin unless other areas of cost can be reduced to compensate for the inflated rate of loss generated, or users can be encouraged to scan a higher proportion of selected items.

3. Risk Amplification

A key aim of the study was to consider what crime prevention mechanisms were already in place to prevent MSP-generated losses and what future mechanisms might need to be considered. Our main observations were that:

- Very little developmental work had been put into fully understanding how the risks associated with MSP would be addressed beyond utilising the existing approaches. Without fully understanding what the risks might be, it was hard for retailers to consider what additional crime prevention solutions might be considered and what costs could justifiably be attributed to them.
- Current measures being used by the retailers taking part in this study focussed almost exclusively on the extremes of the shopping journey: store entry and the payment/checkout process.
- It was observed that, for the most part, the registration processes currently being used were open to easy manipulation through inputting false information, including the potential to use stolen credit card details.
- The only other risk amplifier currently available was the 'random' audit check. The process for doing this varied significantly between the retailers taking part in this study but all thought it was their most powerful weapon in generating risk in the MSP shopping journey.
- Integrating existing product protection devices into the MSP process is problematic as deactivating tagged products require staff interventions – which goes against the ethos of MSP.
- In future, risk could be amplified throughout the MSP shopping journey in a number of ways. For example, a series of retailer/customer messages (via the App) at arrival and entry to the store could reduce customer anonymity at the start of the shopping process. During the shopping trip non-scan alerts could notify shoppers and security personal if products have not been scanned. Visual recognition CCTV could be used to conduct age restricted checks. Geo secure areas could be used to monitor payment compliance.
- Current technologies can already deliver some of the requirements required to increase risk in the steps outlined in this report. CCTV systems can communicate with information databases and micro location monitoring can already be seen in some retail spaces. The challenge is developing a tag that can enable the majority of consumer products to communicate with their environment – RFID tags have been found to offer this potential but on only a relatively small range of products. No other tag technologies seem to be able to offer this type of capability at this moment in time.



Introduction

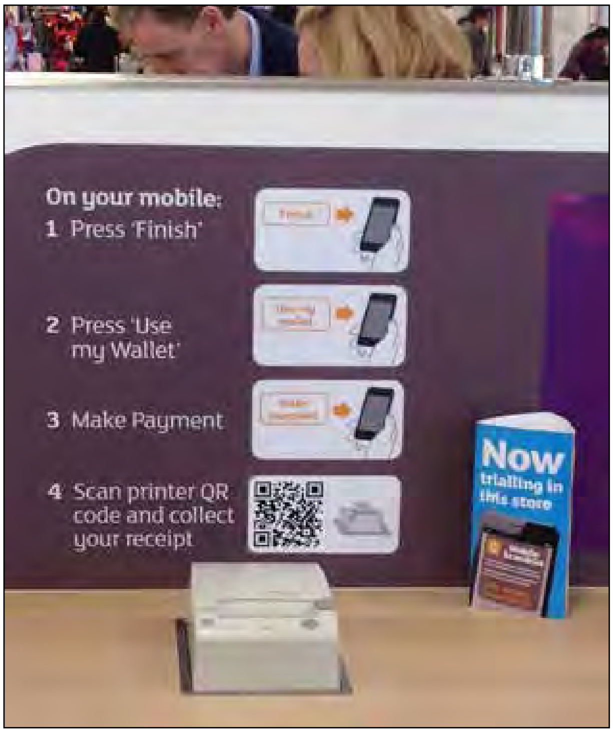
1. Introduction

This report presents the findings of an ESRC-funded study conducted between December 2013 and February 2015. The primary focus was to identify current developments in mobile scanning technologies in the retail space; to understand how allowing customers to use their own personal mobile phones to scan and pay for items could impact upon shrinkage and also identity how crime prevention might be integrated into these systems. The main aims and objectives were framed around the following research questions:

- How mobile self-scanning technologies might be used to facilitate shop theft – what new opportunities for deviant behaviour can be identified?
- How might current and future loss prevention technologies (such as CCTV, EAS and other forms of product protection) need to be adapted to minimise the risk of losses from mobile self-scanning?
- Given our current understanding of the importance of generating perceptions of risk and utilising the concept of a zone of control to achieve this, how will this be generated when customers use this technology – will there be a need to undertake random audits for instance?
- How will 'surveillance' operate within the store to ensure customer compliance? Can a 'virtual zone of control' be created either via the App or through for instance changes in store design and procedures?
- How will any existing legislative requirements on the prohibition of the sale of certain products (such as alcohol) to minors be managed?
- In what ways should retailers consider the design of current and future stores to take account of the risks this technology might generate – for instance how customers enter and leave?
- How should store and security staff be trained to recognise potentially deviant self-scan behaviour – will there be a need to create new store roles such as roving mobile scanning assistants for instance?
- Should new technologies be developed/introduced to facilitate the identification of self-scan facilitated deviant behaviour and if so how might it work?
- How robust will systems need to be in order to cope with errors/problems such as unreadable barcodes, battery failure, lack of Wi-Fi connectivity, customer-initiated voids, price reductions, voucher scams, incorrect scanning of items and the misrepresentation of goods at weighing stations?

The work focused upon developments in UK-based retailers, though the research was also mindful of international developments in this area. Thus, while the fieldwork was initially based upon detailed interviews and store visits across four UK based retailers, interviews and store visits were also conducted with two USA, one Dutch and one retailer based in Belgium.

This report is structured into the following sections. First, we outline the background to the work and the theoretical basis for the study. Second, the methodology is presented. Third, the key findings are outlined and finally, we consider the implications for crime prevention and potential areas for further research.


On your mobile:
1 Press 'Finish'
2 Press 'Use my Wallet'
3 Make Payment
4 Scan printer QR code and collect your receipt
Now trialling in this store

Background to the Study

2. Background to the Study

2.1 Innovation in Retailing

Although most innovation in retailing commonly aims to expand customer markets and increase shopper convenience, it can also generate loss. Within retailing, three principal phases of innovation in customer experience can be observed, with a fourth currently emerging. The first marked the move from primarily behind the counter service, with dedicated staff selecting the goods customers wished to either view or purchase, to open display where the customer could self-select items from open displays and then take them to a central point for purchase. This approach was pioneered by the Grocery sector in the early to mid-part of the 20th Century and has eventually been adopted by most parts of the industry. It was seen as a way of improving the customer experience through offering the opportunity to interact with the products available for sale and it also acted as a major catalyst for innovation in packaging design, brand management and store layout.

The second major development was the introduction of self-scanning technologies where customers not only have to find and select items themselves, but they are also expected to take responsibility for payment as well at dedicated self-scan checkouts. Initially introduced in the 1980s, again primarily in the Grocery sector, it did not see much industry role out until 2010 onwards, mainly due to the limitations of the technology and little perceived customer appetite for this type of shopping experience.

The third development marked a move towards offering mobile commerce and online shopping. Mobile commerce (m-commerce) allows customers to search and pay for products online via their own computer, tablet or mobile device and either have products delivered to an agreed address or collect them from a physical store at an agreed time. It has been noted that m-commerce is a rapidly growing market that currently represents 12% of all US e-commerce sales (Walsh, 2013). Halliwell (2013) suggests that the Smartphone is becoming a key part of the retail experience across the world and it is predicted that spending via mobile devices will double worldwide from £920 billion in 2013 to over £2 trillion by 2017 (see Clark, 2013). While some are predicting a future where the Smartphone eventually replaces the physical store[1], the 2013 Agile Customer Survey (see Halliwell, 2013) of 1,000 British shoppers identified that 54% of customers already use their mobile phone to compare prices online and 46% to research product information. Thus, for many, the mobile phone is becoming an integral part of the shopping process but not necessarily replacing entirely the traditional shopping experience of visiting actual stores – the death of the high street is much quoted but perhaps overstated at this time (Duncan, 2014; *The Independent*, 2013).

The move to mobile commerce is very much connected with the emerging fourth development (the principal focus of this report) of offering the customer the opportunity to use their own mobile device 'in-store' to not only scan items they wish to purchase, but also pay for them using the same technology, through the use of downloadable Smartphone Apps, anywhere in the store. While uptake at the moment is rather patchy and focussed primarily on the Grocery sector, some believe that this is the next major development in the ever-changing retail landscape (McKinsey & Company, 2014).

The move to develop and introduce mobile scan and pay (MSP) can be seen as part of long-term changes in the retail industry that have seen increased customer autonomy and self-service at the expense of formalised staff/customer interactions. For example, the move from counter-service to self-selection at the beginning of the 20th century allowed customers to find, select and pay for items of their choice. Curtis (1971) notes this change gave economic benefits to retailers – fewer staff needed to be employed, and the store design could be radically changed to maximise the display of goods, which led to significant increases in sales and retail profits. However, there was a price to pay – this more open and less controlled retail style made it not only significantly easier for motivated offenders to steal products, it also reduced perceptions of risk for all customers, encouraging more to think about taking advantage of the new opportunities for deviancy presented to them (Beck, 2009). The development of self-scan technologies in the 1990s and 2000s then allowed customers to not only self-select items but also expected them to take responsibility for the scanning and payment components of their shopping trip as well. Beck (2011) argues that this brought yet more opportunities for retailers to reduce costs as fewer staffed checkouts were required, but it also required a

[1] For example, in South Korea virtual shopping walls have been built where customers can purchase items via an App on their mobile phone. The shopping walls look like advertising posters and can be found in public spaces such as subways.

considerable leap of faith in the integrity and honesty of the shopper as they needed to be trusted to scan all items they wished to purchase. Although current evidence of the impact of self-checkouts on retail losses is inconclusive (see Taylor, 2013: Beck, 2011; NCR, 2012), it has been suggested that it has created significant opportunities for loss by yet further reducing the sense of risk perception for customers (and would be offenders) in store.

2.2 Mobile Scanning Technologies: Previous Research

Although several articles on MSP have appeared in retail trade magazines (see for example Halliwell, 2013), only two academic studies have considered the benefits and risk of mobile technologies in retail (see Taylor, 2013; Aloysius & Venkatesh 2013)[2]. Four key findings emerge from these studies:

1. ***There are several potential configurations of scan and pay:*** a number of potential scan and payment configurations exist including a variety of fixed and MSP options (see Table 1 for an overview). This makes any analysis of how loss/crime might be generated in the mobile shopping journey more complex than for the traditional customer journey (which was a linear process – browse, select, scan, pay) as products may now be scanned and paid for throughout the shopping process (Taylor, 2013). This also means stores may now have different types of shoppers in-store at any one point – the traditional shoppers who scan and pay at a staffed checkout; those who self-scan and pay at a fixed terminal and a new breed who want to self-scan on a mobile device and use this device as a payment wallet.

2. ***There are several technological/process issues with MSP still to be resolved:*** Aloysius & Venkatesh (2013) and Taylor (2013) highlight several process/ technological issues with MSP systems that present a risk to the shopping journey. For example, poor Wi-Fi connectivity and insufficient phone battery life may interrupt the shopping journey. Concerns have also been expressed about problems customers might face when attempting to self-scan goods (evidence from self-scan research suggests this can be problematic – see for example Beck, 2011). Indeed, Baxter-Reynolds (2013) comments on a trial of mobile scanning in a major retailer where it was found to be difficult to align product barcodes to the camera of mobile devices, the system did not recognise multi-buy offers and payment was via a normal fixed payment till, which slowed down the purchase process. Crucially, how MSP will work with existing forms of product protection – such as Electronic Article Surveillance (EAS) tagging and safer-cases – and how products that are age-restricted will be purchased via MSP (without the need for stopping customers) also still have to be resolved (Aloysius & Venkatesh, 2013; and Taylor, 2013).

[2] Taylor (2013) based her work upon a mixture of workshops with industry experts and consultation (via telephone) with ten industry professionals in Australia. Aloysius & Venkatesh (2013) conducted a store-intercept survey of 200 customers from three retailers about mobile POS; two focus groups with 53 customers; focus groups with experts and a 'tolerance for validation' survey with 1,190 customers. The findings also included some data collected by the National Association of Shoplifting Prevention (NASP) in their surveys of USA shoplifters.

Table 1: Scan and Payment Process – Current Options[3]

Scanning Options		Payment Options
MOBILE	***Mobile assisted*** – scan device is provided by retailer and member of staff scans on sales floor.	A store employee uses mobile device to take payment on the sales floor.
	Mobile self-service with retailer device – customer scans products using an infra-red scanner provided by retailer.	Customer pays at a fixed checkout terminal, which may or may not be serviced by a member of staff.
	Mobile self-service with own mobile device – customer downloads a bespoke App and uses this to scan products via the in-built camera on the device.	Customer either uses mobile device as a virtual credit card/payment wallet and pays using Wi-Fi/ phone signal, or has to go to a fixed payment point.
	Mobile automated scanning using Smartcarts – Smartcarts automatically scan items using 360 scanners.	Smartcarts automatically charge to customer account or credit card account.
FIXED	***Fixed assisted scanning*** – store employee scans products at point of sale.	Store employee accepts payment at fixed POS.
	Fixed self-service – customer scans products at a fixed terminal.	Customer pays at fixed self-service fixed terminal.
	Fixed Automated – products are automatically scanned by 360 scanner belt.	Payment automatically charged to store account or credit card by link to customer ID and product scanning software.

3. ***Customer appetite for MSP and confidence in systems is questionable:*** questions have been raised over the customer appetite for MSP and customer confidence in the systems that operate the security of payment wallets. It has been suggested that if sold to customers as a form of convenience shopping, then it is necessary to ensure that customers are confident that systems function smoothly and that security around payment is guaranteed. The evidence to date is that some customers feel current MSP systems are slow and not a particularly convenient way to shop (see Baxter-Reynolds, 2013). However, Aloysius & Venkatesh (2013) and Taylor (2013) also note concerns remain over the appetite of customers to use their own mobile phone to scan and pay. While some have concerns over liability for loss of their phone or data on their phone, Walsh (2013) suggests that persuading customers that secure payments can be made via their mobile phone will be a significant challenge.

4. ***The potential impact upon loss and shrinkage is unclear:*** shrinkage is commonly understood to include external theft, internal theft, process or administrative errors and inter-company fraud (Chapman and Templar, 2006; Beck, 2014). No studies have estimated the amount of shrinkage that MSP could generate, but it has been noted that (as with SCO) the opportunity for non-scanning of items increases: customers walking through exit barriers with goods scanned but not paid for (walking), employee-aided loss and collecting receipts to steal or return goods later (see Taylor, 2013; Aloysius & Venkatesh, 2013). There are also possible fraudulent uses of MSP, in particular in relation to payment wallets. Other malicious problems might include the intentional misuse of vouchers and selecting the wrong loose items description (carrots instead of grapes scams). Non-malicious losses might be generated through 'honest' mistakes where items did not scan because of a technical glitch. While a body of research has identified a number of opportunities that MSP might generate for loss there has been little systematic study of these risks or any attempt to ascertain if shrinkage is indeed higher in stores where MSP options are in place.

[3] Adapted from Aloysius & Venkatesh (2013).

2.3 Theoretical Basis of the Study

The previous research is useful as it identifies some of the practical process and technological problems with MSP and how opportunity for loss is generated. However, there has been little attempt to analyse the criminogenic opportunities generated by MSP through any appropriate criminological theoretical/explanatory framework or to identify how either physical or online-based crime prevention mechanisms might be built in to the shopper journey. Based upon these observations the framework for our analysis of MSP is broadly based around three well-known theoretical concepts that are outlined below.

Opportunity Theory, Techniques of Neutralisation and Risk Perception

Many academics argue that much criminality is a result of offenders taking advantage of opportunities for crime that arise in their everyday routine activities (Clarke, 1980; 1992; 1997; Clarke & Homel, 1997). Opportunity theory is thus based on the notion that offenders make rational choice decisions to offend and when exposed to a potential crime opportunity, choice structuring decisions around the effort required to commit the crime, the risks of getting caught and potential rewards on offer are made (Cornish & Clarke, 1986). This simplistic framework clearly offers a useful structure to aid our understanding of the proximal factors that might influence how MSP could generate crime and loss in the retail environment. Indeed, much criminological research has already shown that the propensity to steal is a function of the amount of effort required to commit the crime, the anticipated rewards (the goods/items available to be taken), perceived likelihood of being caught and the perceived severity of any likely subsequent punishment (Cornish & Clarke, 1986). Crucially, in relation to shoplifting, Cardone & Hayes (2012) illustrate how offenders' decision-making is closely related to the perceived effort required to successfully commit the crime (access to goods, ease of escape) and perception of the risk of getting caught (which is amplified by the presence of CCTV, number of 'place managers' or employees in store or security personnel).

The move from counter shopping to customer self-service (and latterly MSP) has, however, complicated matters in relation to proving the intent, motivation and rationale of the non-paying customer – did they actively seek to steal products or are there contributory factors which need to be understood in order to correctly frame the event? While the move to MSP *might* offer greater opportunities for theft, it also offers greater opportunities for customers to make not only genuine errors in an increasingly complicated and technologically driven process, but also generate 'excuses' for non-payment through the use of neutralising techniques (Sykes & Matza, 1957; Cromwell & Turman 2003**.** Indeed, Beck (2011: 211) notes that in relation to SCOs, proving guilt on the part of the offender is difficult as they have a series of ready-made excuses – 'I thought I had scanned that item' or 'I thought my credit card had been accepted'.

Such techniques of neutralisation might not only be developed by those not intending to pay for goods, but might also be used in circumstances where customers can feel justified in taking items if SCO systems do not operate smoothly – thus enabling customers to construct what they perceive as legitimate excuses for theft (Beck, 2011). However, Aloysius & Venkatesh, (2013: 36) also note this might not only lead to discrepancies over what losses are malicious and non-malicious, but also 'erroneous customer accusations' – can stores realistically seek criminal prosecution when a non-scanned item is found in a customer's bag when the retailer expects them to use SCO technologies?

Questions therefore remain about how MSP generates such opportunities for crime and the extent of loss that may be malicious (purposeful theft) or non-malicious (errors either due to customer or technology failings). However, further exploration is required around how opportunities for malicious or non-malicious loss might be blocked. Indeed, a wealth of crime prevention literature suggests that when new products or systems are designed efforts should be made to identify what potential crime opportunities might be generated (Felson and Clarke, 1998) and to design out such generators of crime (Ekblom, 2012). Traditionally crime prevention has aimed to reduce crime through using opportunity-reducing techniques (see Smith & Clarke, 2010) that:

1. Increase the *effort* for motivated offenders through target hardening, access control, exit screening, deflecting offenders and controlling facilitators.
2. Reduce *rewards* through target removal, property identification, benefit denial, removing inducements and disrupting markets.
3. Increase *risks* by extending guardianship, promoting natural surveillance, reducing anonymity, utilising place managers and formal surveillance.
4. Remove *excuses* through reducing frustrations and stress, avoiding disputes, reducing emotional arousal, neutralising peer pressure and discouraging intimation.

5. Removal of *provocations* through rule setting, clear signage, alerting conscience, assisting compliance and control of drugs and alcohol.

As Aloysius and Venkatesh (2013: 6) note, 'surveillance and control become more difficult in the mobile scan world'. Indeed, current crime prevention thinking is largely based around blocking opportunities using existing physical methods. For example, Taylor (2013) and Aloysius & Venkatesh (2013) make useful suggestions based upon existing solutions (such as CCTV, tagging and RFID) and processes in stores (such as validation checks)[4]. However, there is a failure to identify how these preventative measures might be integrated in to the MSP shopper journey and whether they have a realistic prospect of actually impacting upon perceptions of risk.

Thus a key challenge is to design crime prevention in to a system where existing notions of the shopping journey (browse, select, go to checkout, scan (self or by staff member), remove any product protection, pay and leave) are severely challenged, as are the traditional ways in which risk is generated and amplified. For instance, if a consumer is legitimately entitled to 'scan' items and pay anywhere in the store using their own device, without interacting at any time with a member of staff or fixed technology, how can 'risk' be injected into this type of shopping experience – what will stop the MSP shopper taking full advantage of the criminogenic opportunities presented to them – why should they scan all the items, especially those that are perceived as expensive and/ or poor value for money? This is a major challenge for introducing MSP technologies and the development of a viable and credible risk model – as the physical shopping experience begins to meld with the virtual, then crime prevention strategies will also need to be developed that take account of and utilise the same shopper environment – the MSP App may need to become the new 'guardian', generating risk and removing excuses, making it more difficult to steal, and reducing the rewards on offer through clear risk amplification.

Gagnez du temps tout en contrôlant votre budget.
self SCAN
Win tijd en hou je budget in het oog.
PROMO
ak - Tabac

[4] Indeed the current research on shoplifting generally – and understandably – focuses on physical measures of prevention such as appropriate signage, CCTV, shop design, product design, staff interaction with customers etc. (see Tilley, 2010 for an overview).

Methodology

3. Methodology

The data for the project were collected from interviews with staff involved in the development and implementation of MSP systems, visits to stores where systems were in use and through analysis of shrinkage data.

Table 2 presents a list of the participants included in the study and their respective roles. Overall, four major UK retailers were included, two USA, one from Belgium and one retailer from Holland. Two interviews were also completed with App developers/security experts. The key personnel interviewed were involved in developing or piloting MSP systems or were loss prevention personnel responsible for identifying risk and monitoring shrinkage across the company.

Table 2: Interview Groups in Study

Retailers	Respondents Within Retailers
UK Retailer 1: MSP pilot rolled out across several stores.	Head of Profit Protection Profit Protection Manager National Operations manager Loss Prevention Project Manager Digital Technology Programme Team Omni-Channel Coordinator
UK Retailer 2: trial phase in one store.	Director of Process and Asset Protection Retail Innovations Team Project Manager for MSP trial Investigations Team Operations Manager Head of Security Resource App Developer (in-house).
UK Retailer 3: one aborted trial.	Project Manager Loss Prevention Operations Manager Head of Marketing Team
UK Retailer 4: plans for MSP in development stage but no trial underway.	Head of Loss Prevention
USA 1: MSP rolled out across hundreds of stores and continuing to be used.	Director of Shrink Asset Protection Team Security Investigations
USA 2: MSP trialled across several stores but then ended.	Director of Asset Protection Innovations Team Self-service Team
Holland – MSP rolled out across several stores and currently in use.	Head of Corporate Security Store Development and Design Team
Belgium – MSP rolled out across several stores and currently in use.	Director of Health, Safety and Head of Risk Management
App developers/security	Product Manager, product protection company Technology Consultant

The interviews with retailers and App developers covered a number of themes. These included:

- **Current roll out of mobile scan and pay in the company:** if they have any MSP options in place across their stores, how it works, how many stores it operates in, and any problems observed with its operation.
- **Views on the development of mobile scan and pay across retailing:** what the benefits are to retailers and shoppers, what the challenges are in its development, whether mobile scan and pay is likely to become used widely throughout retailing.
- **The risk of loss in the retail environment:** the extent that MSP might increase losses, how it could increase losses, how shoplifters might exploit such systems, how such systems would work with existing legislative requirements (such as the sale of age restricted products), how it will be managed by loss prevention.
- **Product protection:** the extent that a deterrent effect can be built into existing product protection, how MSP will work with current product protection devices such as tags, how MSP and non-MSP customers will be monitored in-store, what future plans exist for product protection (whether technologies such as RFID and CCTV have a role to play), whether a credible detection component at exit gates can be created.

In addition to these formal interviews, a focus group was also conducted with a retailer who had run a trial of MSP. The principal aim was to consider issues around loss prevention and how such loss might be mitigated through the following:

- **Store design**: zones of control – how zones of control might be developed. Store layout and design – the importance of visual cues and signage to shoplifters.
- **Product-based technologies**: such as tags, RFID, and safe cases.
- **Store-based technologies:** such as CCTV, exit screening/barriers; techniques of payment validation: bag and receipt checks; product weight confirmation plates; and tolerance for validation research.
- **Consumer-based technologies:** App based preventative measures; device security, such as wipe data and replace mobile wallets instantly; use of identity verification technology (such as PIN number or fingerprint); and store data in cloud rather than on device.
- **People based approaches:** utilisation of existing security and members of staff.
- **Store processes and procedures**: training of staff.

All interviews were recorded and analysed using a themed analytical approach (Turley *et al*, 2011). This approach is common in the analysis of semi-structured or qualitative data as it allows for reoccurring themes to be identified.

In addition to the interviews, visits were made to stores (in the UK, USA, Belgium and Holland) where versions of MSP systems were in operation. In all stores (accept one) visits were overt in that they were undertaken with staff from the organisation. However, several covert visits were also made to a UK store where an MSP system was in operation. The aim of these store visits was to use the MSP systems in order to identify problems that might be experienced by users, potential opportunities for theft and opportunities for crime prevention. Extensive fieldwork notes were taken after these store visits which were then subsequently analysed.

Shrinkage data was provided by just one of the retailers where MSP systems were being trialled. As detailed in the Findings section below, getting shrinkage data from retailers is notoriously difficult – it is regarded as highly sensitive data and rarely published beyond in aggregate form covering multiple retailers as part of regular surveys. In order to protect the identity of the retailer only limited information can be provided on the data itself. The retailer is a large international grocer with many hundreds of stores and a turnover in the many ✪billions[5]. They provided data covering a 12 month period collected from hundreds of stores offering the consumer a choice of traditional means of shopping via fixed and staffed checkouts, or the option of mobile shopping via a scan gun provided by the retailer or the opportunity to use a bespoke shopping App installed on their own smart phone. For both forms of mobile shopping, payment was via dedicated fixed terminals overseen by store staff.

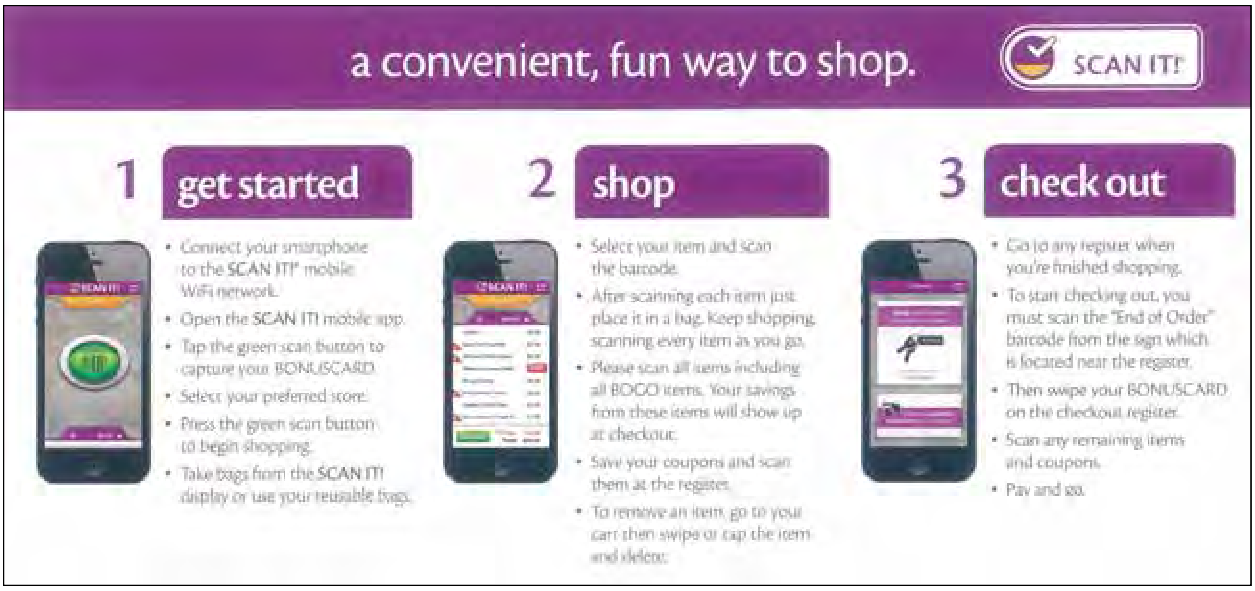
The data made available included the following variables:

- The total number of completed shopping trips.
- The number of shopping trips that used a scan gun compared with a mobile phone.
- The number of items purchased.

[5] In order to protect the anonymity of the case study retailer, This ✪ symbol will be used to represent currency.

- The value of the items purchased.
- The number of shopping trips when a check audit was undertaken.
- The average number of items audited.
- The average number of items not scanned.
- The value of items found not to have been scanned.

The data covered nearly 12 million mobile scan shopping trips with a total value of ✪21million (6 million items). Of these, 1 million trips were subject to an audit, which generated data on the number and value of items found not to have been scanned by the consumer. On average, 6 items were selected to be checked as part of an audit, from an average basket size of 30 items (20%). Unlike other retailers utilising check audits, identification of non-scanned items did not trigger a full scan of all items – only the number selected for review were checked. Unfortunately, it was not possible to disaggregate the mobile shopping data and so all data presented in this report covers both mobile scanning technologies used by the case study retailer (retailer provided scan gun and consumer owned smart phone).



1 get started

- Connect your smartphone to the SCAN IT!® mobile WiFi network.
- Open the SCAN IT! mobile app.
- Tap the green scan button to capture your BONUSCARD.
- Select your preferred store.
- Press the green scan button to begin shopping.
- Take bags from the SCAN IT! display or use your reusable bags.

2 shop

- Select your item and scan the barcode.
- After scanning each item just place it in a bag. Keep shopping, scanning every item as you go.
- Please scan all items including all BOGO items. Your savings from these items will show up at checkout.
- Save your coupons and scan them at the register.
- To remove an item, go to your cart then swipe or tap the item and delete.

3 check out

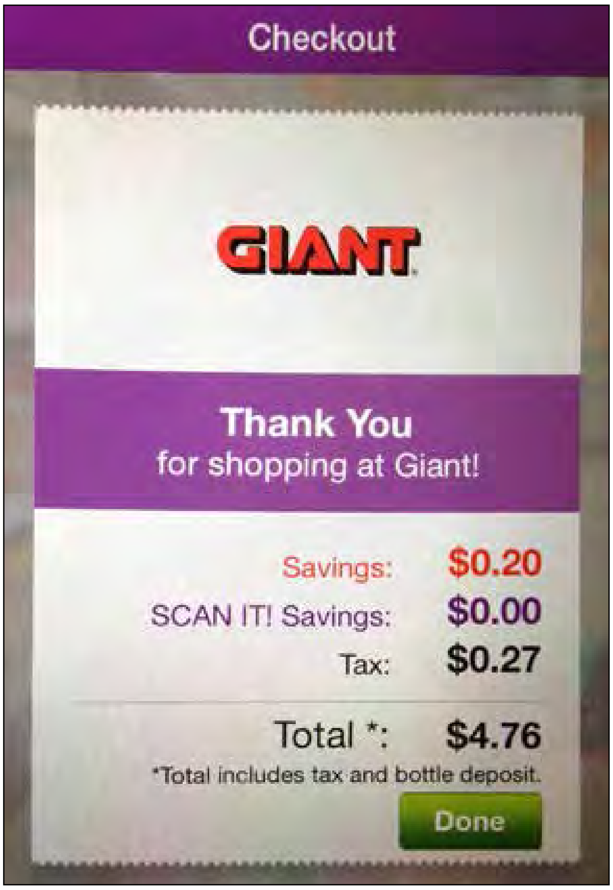
- Go to any register when you're finished shopping.
- To start checking out, you must scan the "End of Order" barcode from the sign which is located near the register.
- Then swipe your BONUSCARD on the checkout register.
- Scan any remaining items and coupons.
- Pay and go.

Key Findings

4. Key Findings

4.1 Current Developments in Mobile Scanning

All retailers in the study were at different stages in the development of MSP. In the UK, one retailer was piloting a MSP system across several stores; another was in the process of conducting a trial within one store, one had piloted a system though the company had (for the time being) shelved roll-out plans and another had not got past the planning stage of a pilot project. All of the four retailers from the international sample had rolled out MSP systems and three were currently running versions across their stores (one had withdrawn the MSP option from its stores). Across the majority of the retailers in the sample, MSP development and implementation was currently focused around only a scanning option – thus allowing customers to use their own mobile phone to scan items – rather than developing a payment wallet. Only one retailer in the study was currently trialling a scan and payment wallet with their MSP system.



Checkout

GIANT

Thank You
for shopping at Giant!

Savings:	$0.20
SCAN IT! Savings:	$0.00
Tax:	$0.27
Total *:	$4.76

*Total includes tax and bottle deposit.

4.2 The Benefits of MSP for Customers and Retailers

Although the pace at which MSP systems were being developed and implemented across the sample retailers was slow (and in many cases not without difficulties), respondents highlighted several potential benefits. Many of these echoed much of what has been published in the media (see for example, Halliwell, 2013; Walsh, 2013) and in previous research (Taylor, 2013; Aloysius and Venkatesh, 2013), though are worth recounting again here.

Respondents pointed to consumer convenience and how MSP makes the purchase process easier and quicker as key benefits. As one respondent stated, 'customers don't have to empty their trolley and reload it all again at the end… which ultimately speeds up the process' (Interview 2). It also enables customers to know exactly what they have spent at all points of the shopper journey and eventually 'convenience payment' within the aisle (rather than at a payment bank at the end of the shopping journey) should be possible. Indeed, the potential for the 'personalisation of shopping' (Interview 2) was thought beneficial as it allows the customer to keep a closer track on their purchase history and any loyalty points accrued. However, it was thought that one of the real key benefits to customers would be through utilising geo-location data and real time messaging with integrated webpage/store hubs. Geo-location data could allow stores to identify where customers are in-store, which could then be linked to store maps and directions to specific products. Integrated webpage/store hubs would allow customers to browse goods via the retailer webpage, while also being sent information about where the products are located in-store, if they are available and at what price. There is also the potential to relate items purchased to other commonly purchased items (shave gel to razors, tonic to gin, children's shoes to children's clothes etc.) and to send the customer real time push notifications about offers on other related products.

Interviewees identified several key benefits of MSP to retailers. Whilst much has been made of the potential savings that might be made on staff costs as a benefit of customer self-check-out (O'Donnell & Meehan, 2012), this was also cited as a key potential benefit of MSP. One retailer suggested that for a trial of MSP they were 'attracting away from the main banks rather than the self-check-out (SCO) so that was definitely the audience we wanted to target' (Interview 2). For some retailers the use of this technology would offer two staffing-related opportunities: to enable more staff to be utilised away from checkouts and on to more customer-focussed services such as in-aisle assistance; and a reduction in the overall staff hours allocated to stores. A knock on effect of this would also be that there would be savings on the purchase costs of physical checkout equipment (as less would be needed) as well as the associated maintenance and cash handling costs (Interview 4). In addition, less physical check-out equipment would free up more space for product displays. However as one respondent mentioned there might be a shrinkage cost involved: 'it potentially takes out a lot of labour, it might increase shrinkage, but profitability might improve [the increased cost of shrinkage would be less than the labour saving]' (Interview, 4). Indeed, it has been highlighted that as shopping patterns change (particularly with the increased usage of online/click and collect shopping), many physical stores might become less efficient to operate and retailers will need to reduce store numbers or cut costs within stores (Ramchurn, 2012). Thus MSP could offer some 'potential long-term savings in staff costs' (Interview 4). Other key benefits that MSP was thought to offer to retailers related to customer retention and the marketing of products. As eluded to above, forms of loyalty bonuses and product offers could be offered to MSP customers. Ultimately, registering customers as MSP users also allows retailers to hold even more information about them. This might allow retailers to 'sell shopping pattern data to analyse' (Interview, 4) and yet further personalise the shopping experience.

Despite these benefits there was some concern expressed over the customer up take of MSP. As one of the interviewees stated:

Everyone's telling [retailer name] they want things on their phone, they want Apps, they want to make shopping easier, but actually when it came down to it, we found that our customers prefer doing the normal shopping routine of coming in, picking up their goods and waiting to get through to the till, and even in those stores where it's very busy, people were happy just to stand and wait, rather than to use their mobile (Interview 1).

Indeed, there was some suggestion that in some locations and for some demographics the move to MSP might represent a cultural shift that might be slow to be adopted. As one retailer said 'especially in [place name], to change a 100 year shopping culture, expecting them to use their own device, go through registration, download an App to do it … they'll probably think it ain't worth it' (Interview 3).

Now
trialling in this store
10:45
Mobile Scan&Go
Take control of your shopping, use your smartphone to scan as you go
It's simple, smart & fast

4.3 Technological and Process Challenges

The in-store trials and interviews with retailers highlighted several technological and process challenges to MSP (see Table 3). Many respondents acknowledged that they were still feeling their way around the technology and that the MSP systems were far from perfect. Indeed, many were – for the time being – focusing on developing a mobile scan option (rather than a payment wallet) – either through developing existing versions of their own hand-hold scanning guns or developing new mobile Apps solutions.

At present, most MSP options are based upon supporting Apps downloaded via iTunes and operating on an Apple device – options for Android or Windows phone users are currently limited. In interview, one respondent mentioned the results of a trial in one of their stores where customers had problems in downloading the App, and said 'it was slow and cumbersome' (Interview 10). Indeed, our experience with one other retailer was that registering and downloading the App was very slow.

Table 3: Technological and Process Challenges: On Site Observations of MSP

Challenges	Description
Phone types	At present systems tend to support Apple devices, not those using Android or Windows operating systems even though Apple accounts for only about 20% of the smart phone market (IDC, 2014)
Slow App downloads	Registering and downloading App can be slow and frustrating.
Registration and Getting Started	In most of the trial companies getting started in store was challenging – available leaflets were often unclear, with the steps to be taken often proving to be confusing and opaque.
Wi-Fi access/passwords in store	Accessing Wi-Fi was sometimes difficult and confusing.
Problems scanning barcodes	Scanning barcodes using a mobile phone can be difficult: there was often glare from store lights depending upon angle and type of product packaging. However, persistence usually led to a successful scan although all were much slower than infrared systems. There was considerable difference in barcode identification rates between retailers – some were significantly faster than others and this had a major impact on the shopping experience.
Multi-buys	When buying the same item several times the in-App process could be laborious in some of the MSPs – no facility to enter quantity.
'Three hands syndrome'	Holding the phone, selecting items from the shelves and pushing a trolley or holding a basket is difficult to manage. It also increases the likelihood of dropping the mobile device.
Phone battery life	Some Apps required a large amount of battery power, which could be problematic on extended shopping visits.
Wi-Fi dead spots	On several visits to one retailer, the Wi-Fi connection consistently cut out in a particular part of the store.
Voiding purchases	This sometimes requires a product re-scan, but this did not always cancel the purchase. In most of the trial stores, the researchers were able to easily crash the App through multiple voiding of products.
Age restrictions	Purchase of age-restricted products always required staff intervention at the payment stage. Only some of the Apps made the consumer aware of this requirement.
Product Protection: Safer Cases/EAS Hard Tags	Purchase of items with hard product protection devices attached required staff intervention to remove the device. Only some of the Apps alerted the consumer to the need for tag removal.
Product Protection: EAS Soft/Source Tags	In the one retailer using this technology there was no facility to deactivate soft EAS tags – the exit alarm would always be activated when MPS customers left who had purchased a soft-tagged protected product.
Payment QR codes	Payment QR codes did not always work and verification bar codes proved highly unreliable. It was also found that not all commercially available QR readers would read the displayed codes – in one store the researchers had to download two QR Apps before being able to continue.
Non-country registered users	In some countries the UK-based researchers could not use the MSP systems – either the App was not made available in the country App store or the App required a local address or loyalty card number.
Payment wallets	Many systems still rely on payment at fixed payment terminals through cash or card, rather than through a payment wallet.
Paying and Security Audits	Payment process was often slow, and audit checks were sometimes frustrating.
Shopper Distraction	Easy to forget to scan items before placing in bag/basket/trolley, particularly when searching for other items/chatting to friends and family.
Ineligibility for Vouchers	In the company with a payment wallet option those consumers making use of this facility could not receive the voucher options available to non-MSP customers.
Non-Scannable Barcodes	Whilst overall scan accuracy was high, on two occasions products would not scan which meant the shopping trip could not be completed – one was a faulty barcode while the other was a system product setup issue. A single point of failure can add significantly to customer inconvenience – MSP shop had to be abandoned and conventional shopping journey taken instead.

As detailed above the research team uncovered and experienced a wide range of challenges associated with using current MSP systems. Indeed, access to good quality free store Wi-Fi was found to be key to the successful operation of MSP systems – one operator made this especially difficult by having two separate Wi-Fi networks in the same store, only one of which would allow MSP to work! However, a more significant and common problem highlighted in the interviews and with our in-store trials related to the relative ease with which products could be scanned. Sometimes it was difficult to align product barcodes to the phone camera and it could be difficult to carry a phone, a basket and scan a product all at the same time (the three hands syndrome). Such scanning problems are not only a potential source of customer frustration, but also create problems for retailers in identifying when customers make genuine scan errors or when they claim items would not scan (as a technique of neutralisation in relation to theft). While some retailers were thinking about how to deal with the 'three hands syndrome' such as offering consumers a wrist or neck lanyard or some form of device docking bay on trolleys or baskets, none had taken this very far. Concerns were raised about lanyards in terms of store liability should the lanyard break and the device be damaged, while the latter raised concerns about designing a docking station that would fit all available mobile devices and not raise the risk of theft when consumers moved away from their trolley/basket.

What was particularly revealing from the researcher's in-store use of MSP was the relative ease with which products could be put into a bag, basket or trolley without first being scanned due to genuine distraction. The grocery store where most of the trials were undertaken is a large 87,000 square metre store – locating products on an extensive shopping list can be challenging, especially when under time pressure. By the time a product had been located and thought had turned to the next item on the shopping list, it was relatively easy to miss out the scan step. In addition, when two people were shopping together it was again easy for the scan step to be missed by the non-MSP user putting products into the bag, basket or trolley. At the end of one shopping trip the researcher found that 10% of items in a basket had not been scanned through genuine error caused by distraction (the items were then scanned before payment was made). This raises an interesting challenge for MSP systems – retail stores are complex, often busy spaces crammed with messaging aimed at tempting the shopper into making impulse purchases. Retailers may find that an increase in non-malicious 'thefts' due to non-scans are simply an inevitable by-product of overlaying the requirement to accurately scan all items onto an already 'noisy' and immersive shopping experience – the shopper is being asked to do too many things at once. Previous research has highlighted that having too much stimulus or too many activities going on in one environment can result in 'directed attention fatigue' (Berman & Kaplan, 2010) where humans are distracted and fail to concentrate on one task at a time. Indeed, when one considers the more traditional staffed checkout or indeed the SCO environment, activity at this stage is primarily one-dimensional – scanning all the items in the basket or trolley as quickly and (retailers would hope) accurately as possible. Few distractions, beyond some nearby impulse purchase options, exist – the consumer or the member of staff is largely focussed upon the task in hand.

Some respondents stated that results from their trials had revealed that phone battery life had been an issue for customers. Indeed, on longer shops (50+ items) this was found to be a problem although as consumers become more familiar with the system the length of the shopping journey may be reduced, saving on battery life. However, a more frustrating issue was around Wi-Fi dead spots in store that could lead to the App failing to register a product at all. Further to this, cancelling a purchase normally required a re-scan of the product, which further slowed down the shopping trip.

In most MSP systems the final part of the shopping trip mirrors the experience of SCO customers. At present age restriction checks have to be carried out by staff, with some of the trial Apps making the consumer aware of this when they scan the item while others would only flag up the need for validation at the point of payment. Similarly, some of the MSP systems would alert the consumer when a product was protected with an anti-theft device that would need to be removed by a member of staff at the point of payment or at a customer service desk. The payment process was a challenge for all the companies taking part in the research – only one had integrated a payment wallet into their App; the others relied upon the consumer taking their device to either a regular checkout or a bespoke payment area or an area where SCO and MSP customers could be processed together. The experience of using the payment wallet was mixed – a quirky in-store process, which required a time limited barcode to be found in the store before a payment could be processed, meant that it was seldom quick and often frustrating, leading to little if any time saving compared with SCO systems. The company operating this recognised the problem and claimed that Version 2 of the App planned to resolve this issue.

The reluctance to offer an in-App payment option by most of the companies was partly a technical issue of ensuring adequate security for the consumer, but was mainly driven by concerns around ensuring customer compliance – they were very nervous about allowing a user to pay anywhere in the store because of the total absence of available control. Even in the one company using a mobile wallet option, they instructed users to go to a designated area where a member of staff with responsibility for SCO was nearby to monitor activity and undertake any required check audits.

4.4 The Potential Impact on Shrinkage

It was clear that retailers had given some thought to the potential crime problems that might be generated through MSP (though this was speculative rather than proven through any analysis of shrinkage or loss). Indeed, it was thought there would be an impact upon shrinkage, but the question for many was whether increases in shrinkage could be balanced with reductions in labour costs: 'if we do see an increase in shrinkage in five years' time, there's a pay off between that and the wage numbers' (Interview 2).

Primarily, it was identified that MSP might generate crime or loss in four ways:

- Theft through malicious non-scanning of goods.
- Non-malicious loss through non-scan/scanning errors.
- Physical and verbal abuse against staff generated via audit checks.
- Transaction frauds or fraudulent use of payment wallets.

Importantly, a distinction was made between the types of 'offender' who might exploit MSP. There was a suggestion that MSP would not be used by shoplifters who chose to conceal goods or even overtly walk out ['walking'] (see Bamfield, 2012). As one respondent said 'it could provide the camouflage for theft' (Interview 9), though another stated 'if you wanted to nick a pack of razor blades, why go through the whole signup up process with goods?' (Interview 4). Indeed, Aloysius and Venkatesh (2013:51) suggest shoplifters see potential opportunities to use MSP systems, but at present do not see MSP as likely to 'make these activities [shoplifting] either easier or more difficult'. However, in the same research it was reported that one shoplifter suggested 'it was only a matter of time… that they would figure out new ways to exploit the system' (Aloysius & Venkatesh, 2013: 51). Respondents in this study suggested that moving towards the 'ultimate in self-service' (Interview 10) might not only send out the wrong physical cues to potential offenders (Cardone & Hayes, 2012), but those shoppers who might not necessarily plan to steal could take the opportunity to exploit weaknesses in systems if possible. Similar to research conducted on SCO (Beck, 2011), it was thought retailers might actually encourage shoppers who fully intend to scan and pay for products to engage in criminal activity. As one respondent said: 'what you might see is people who traditionally don't intend to steal but realise… when I buy 20, I can get five for free… maybe I'll continue to do that' (Interview 4).

Using the language of opportunity theory several possibilities emerge in relation to the crime generating properties of MSP**.**

Ease of Effort/Access to Products

Whereas traditional counter shopping limited access to goods, the rationale for customer self-service, SCO and MSP is that customers have open access to products and within the SCO and MSP model, the customer takes responsibility for payment with limited or no staff involvement at all. As one respondent commented 'it's the ultimate in trust' (Interview 6) or as another said 'they call it 'Scan and Rob'' (Interview 8). Thus, MSP potentially promotes ease of effort for theft by removing any human contact throughout the shopping process and removing (possibly most importantly) human contact at the final payment stage of the shopping journey. As succinctly put by one interviewee; 'you scan it and you walk … you've got no controls in place' (Interview 5). Of course the self-service culture has meant retailers have implemented a range of product protection devices – hard tags, soft tags, spider tags, safer boxes/cases – to promote risk throughout the shopping journey. However, one respondent suggested an unintended effect of MSP might be a sort of 'displacement effect… where due to the ease… we [might] see a greater number of non-protected items going missing' (Interview 4). Indeed, another respondent suggested in mystery shopping trials of one MSP system, even where product protection alarms were activated there was little response from retail staff: 'he didn't pay for half… set the alarms off, they ignored him, walked back in, set the alarms off, they ignored him' (Interview 5). Indeed, in one store trial conducted for this research, it was identified that when a validation check was not conducted at the point of payment it would have been easy to steal non-protected items. In another store visit completed for this study, the main reason for the ease at which goods could have been stolen was because validation staff were more concerned with processing customers quickly through the payment process (as staff were getting frustrated over the continual technical glitches with the payment wallet option) rather than conducting re-scan/audit checks.

Increased Rewards for Offenders/Non-scanners

The MSP environment might generate long-term rewards for offenders/non-scanners. Indeed, several respondents suggested that non-scanning behaviour could become part of the routine behaviours of some shoppers. At present, there is some evidence that non-scan is a part of the behaviours of some SCO customers; 'people will always take advantage of opportunities. You see the self-service figures, one in five admit to stealing on self-service' (Interview 1). Therefore, there is a possibility that some shoppers might begin to perceive certain stores as easy targets and thus increase the frequency at which they use/target them. Indeed, studies of repeat victimisation illustrate that offenders select targets based upon *risk heterogeneity* factors – where a target is so attractive they will select it to commit crime (regardless of whether it has been a successful target for them previously) and as a result of successfully committing a crime then return on another occasion to the same target – known as 'event dependent repeat victimisation' (Farrell & Pease, 1993; Farrell, 2005). Indeed, several interviewees suggested that – as with SCO – MSP could act as a risk heterogeneity factor – where people are attracted to stores in the knowledge that they can chose to not scan certain products with relatively little risk of being caught. As one respondent suggested, 'you get away with it once and then you can just repeat it again and again…' (Interview 7).

Reduction in Risk Perception

Several studies have shown that surveillance or various forms of capable guardianship are important in the prevention of shop theft (Tilley, 2010; Butler, 1994; Cardone & Hayes, 2012; Beck, 2011). For example, the number of 'place managers' (store employees) throughout the store, using customer meet and great practices (Tilley, 2010), increasing staff vigilance (Butler, 1994) and formal surveillance (such as security guards) can all impact upon risk perception (Butler, 1994; Cardone & Hayes, 2012). Thus, increased anonymity reduces the perception of risk (Aloysius and Venkatesh, 2013). Within the MSP environment, the sense of risk perception or control is reduced as all elements of the customer journey can be completed without human interaction. Indeed, a further likely long-term consequence of MSP is that the number of place managers will be reduced, as one respondent said 'there are benefits [from MSP] in labour savings, but there could be other problems with that' (Interview 4).

Likely Excuses

Previous research has highlighted that SCO allows consumers to use 'ready-made excuses' (Beck, 2011: 210) for offending (the self-scan defence). Therefore, giving customers the freedom to self-scan gives them the opportunity to blame faulty technology, problems with the product barcodes or claim that they are not technically proficient as reasons for non-scan (Aloysius & Venkatesh, 2013). Indeed, issues around the 'self-scan error' and 'self-scan defence' regularly came up in the interviews. Of course, scanning error is not only common amongst self-scan users, but checkout operators also frequently non-scan items. This led one respondent to suggest that some of their stores had actually seen improvements in shrinkage because 'the customers were more accurate [at scanning] than the cashiers' (Interview 7) or are more likely to 'double scan' to make sure something was included in their shopping basket – in effect pay more than once for the same item.

However, one of the key problems where customer non-scan is observed is in proving intent to steal items and whether prosecutions can be made or not. As one respondent said 'I scan 20 items and I don't scan five, am I a thief or am I someone who's not very competent?' (Interview 4). Another noted, 'I don't think we could ever prosecute anybody as things exist today, because they could always fall back on the argument 'well, I pressed the button, I thought I'd scanned it'' (Interview 2). Indeed, observations conducted in MSP stores for this research were that validation staff were always more than willing to accept this as a form of defence (even when we had knowingly not scanned items). Deciding when multiple non-scanning events constitute a pattern was something that all of the retailers were keen to understand and it was certainly a key component of the main risk generator currently available in the MSP shopping journey – the 'random' audit capability (see below).

Efforts have been made within MSP systems at the point of payment to ensure that customers are sure they have scanned all of their items. Most systems have an on-screen prompt, either in the App or on the payment screen, that asks the customer 'are you sure you have scanned all of your items'. If a customer then proceeds to press 'yes' knowing they have not scanned some items this can be proof of intent. One respondent said:

> …but where I'd feel comfortable convicting [on SCO]… this guy scans three items, pays for those three items, punches in his card details, which is great for us because we can track him… but there's five items that haven't been scanned, and soon as he's got his receipt, he bags those up. That to me would be strong enough to put in front of the police and say this is absolutely premeditated, he's decided he's going to steal them, you can see by his behaviour he's made no attempt to pay for them and he's left without paying for them (Interview 4).

Across some jurisdictions retailers have been concerned about potential reputational damage that might be caused by prosecuting customers for not scanning a small number of items. One retailer suggested that its self-checkout option was abandoned as 'too many of our desired customers made little mistakes' and as 'theft is strictly regulated here in [name of country], you need to prosecute' (Interview, 6). Indeed, issues in relation to intent are further confused by where the last point of sale (POS) will be in future MSP systems. At present it is clear where the last POS is in most retailers, though as MSP payment systems develop, potentially payments could be made in the shopping aisle or (Wi-Fi permitting) in the car park of the store. This creates problems in understanding where in the shopper journey the final payment point is. As one respondent said in relation to MSP, 'there is no longer a last point of payment and by law we would normally stop people after that' (Interview 2).

Likely Provocations

At present, there are a number of points in the MSP shopper journey that could trigger disputes with staff. Our store visits identified frustration points when products would not scan, when staff had to intervene to remove EAS devices/do age verifications and when payment wallets would not work. For example, on one shopping trip the researcher was given a cash discount because of unacceptably long delays in processing a MSP payment. Indeed, Aloysius and Venkatesh (2013) noted that continual intervention from staff at the POS in relation to age-restricted items and exit validation audits (or re-scans) can generate customer frustration. As one respondent suggested in relation to validation audits, 'customers hate it and we know it's a crap experience and we accept that' (Interview 8). However, most respondents suggested customers are generally fairly relaxed about having their shopping subject to exit/validation audits as long as checks are conducted in a non-confrontational and educational way. It was noted that validation audits normally 'only lead to aggressive behaviour when customers have not-scanned items correctly' (Interview 6). Indeed, Aloysius and Venkatesh (2013) suggest customers find validation audits before payment to be less intrusive than checks after the transaction has been completed. Interviews also revealed that UK based customers might have a greater tolerance to validation audits than their European or American counterparts. However, further research is required to ascertain how tolerant customers are of such processes.

Previous research has also suggested that MSP might aid those wanting to engage in transaction frauds (Bamfield, 2012) – using false barcodes, bogus receipts, card fraud and colluding with staff ['sweethearting']. Our respondents seemed less concerned about fraudulent activity than non-scanning. However, three did highlight concerns around fraudulent activities. One noted that a concern in the business was around the production of self-scan labels that might be stuck on products. While any shopper can label switch, it was suggested it might be easier for MSP customers to do so without being detected as it might not look so unusual for them to be carefully looking at product barcodes in the aisle – which might offer an opportunity to change labels. Other concerns were expressed over fraudulent payments with one respondent giving an example:

> …in the early days of the [electronic payment] wallet, we had some attempted fraud and we recognised that because an account was created, a number of small shops [trips] were done through a card and then a big shop was attempted, on the same day. So what someone was trying to do was validate that the process worked (Interview 8).

While it was thought that the payment wallet 'could open up a new world for fraud if customers payment details could be stolen and used via the App' (Interview 8) it was also suggested that not only might electronic payment wallets facilitate the ease at which stolen credit card details can be used, there was also the potential for the use of fraudulent electronic vouchers or coupons. Although not mentioned in the interviews, Taylor (2013) also notes that possibility of ease of repudiation fraud – where customers may claim that they had not purchased certain items or goods that they appear to have paid for. Overall, it was apparent greater consideration needed to be given around possible fraudulent uses of MSP systems. As one respondent stated:

> What we would need to understand, is the vulnerability around card fraud and how fraudsters use it either through getting other people's details from a mobile wallet perspective, or payment method. Because that's where it

> becomes quite interesting. If I steal your phone, how do we protect the App to make sure that you have to put in your password every time to check out. Or some unique identifier that says I can't just steal your phone, do all the shopping I want, pay for it and I'm out the door with a one touch payment (Interview 4).

Finally, one of the biggest concerns raised about MSP was in relation to the potential impact on inventory accuracy. Both the non-scanning of items and theft have a 'knock on' effect in relation inventory accuracy and on-shelf availability of stock. As one respondent noted, certain product groups create problems. For example, 'when someone buys five different varieties of the same dog food, do they just scan one five times, where does that leave our inventory accuracy?' (Interview 4). Also it has been observed that customers often attempt to, but wrongly, scan loose products such as fruit/vegetables and multi-buy offers – when there is a buy one get one free, do you scan the 'free' item? Indeed, one respondent noted 'the inventory drift could have quite a significant impact on the store in terms of availability sales' (Interview 4). This in turn can significantly affect other aspects of the business such as home delivery where poor availability can lead to retailers having to compensate customers for missing items.

4.5 Analysis of Shrinkage

The Difficulties of Measuring Retail Losses

While a number of retailers have been operating versions of MSP for the last few years, no data has been published to date analysing the impact these systems have on rates of store 'shrinkage' – the term used by the retail industry to describe a basket of losses ranging from shop theft to products going beyond their sell by date. While this is a widely accepted global term to describe 'retail losses', there is in fact no standardised definition as to what it actually means. For some it refers to all the losses that are 'unknown' within their business, in other words those losses that are found when store audits are undertaken and a comparison is made between what the retailer thinks should be in a store (received stock minus sold stock) and what is actually present (the difference between expected and actual stock holding). For other retailers shrinkage refers to only those incidents which are criminal in nature – internal and external theft, while others prefer a more inclusive definition that also takes account of losses such as the value of those products which have gone beyond their sell by date, or have been discarded because they have been damaged (often described as process or administrative losses). This high degree of ambiguity makes efforts at benchmarking within the industry notoriously difficult and subsequent results highly unreliable.

It is further complicated by the fact that retailers also vary in the way in which these losses are measured, with some preferring to calculate loss based upon the cost price of the items lost (the actual price paid by the retailer for the product) while others prefer to use retail prices (what the retailer would have received had the product been sold at the price offered to consumers), arguing that there are a whole host of consequential costs associated with lost products, such as transportation, staff costs etc. that are not reflected in the cost price. Depending upon the margin imposed by the retailer this could inflate or deflate the shrinkage figure considerably, perhaps by around about 60-70%.

On top of these significant definitional issues, retailers also face an enormous problem actually identifying the causes of their shrinkage losses. This is because a large proportion of losses (depending upon how they are defined) will only ever be uncovered when a physical audit of stock in a retail stores is undertaken (as described above) and this, while varying between retailers, will normally be an annual event. This means that losses may remain unknown for up to 12 months, making identification of when incidents happened, where they occurred and by whom almost impossible to identify. This has led to the development of a 'guessing game' within the industry where efforts are made to try and estimate what might be the likely causes of these losses, which unfortunately generates data more useful in gauging how the industry perceives the problem rather than measuring the actual problem itself.

To add a final further complication, retailers rarely if ever publish their rates of shrinkage – they are not typically included in annual reports and few will share their losses with external organisations. Understanding this reticence is difficult to explain beyond organisational concerns about reputation (high losses viewed as a sign of poor management) or increasing the risk of being viewed as an easy target by criminals (high losses means poor security). Either way, retailers do not readily make this type of information available to researchers and when they do they frequently insist upon anonymity and strictly enforced Non Disclosure Agreements (NDAs).

The reason for this preamble on what the term 'shrinkage' means and why data on its prevalence is difficult to find is to put the ensuing data into a context. Of the 6 retailers that agreed to help with this research only one was prepared to share any data on the impact mobile technologies might have on rates of shrinkage. In order to protect the identity of this retailer we have to be cautious in the way in which we describe and present the results, including to a certain extent how they were generated. This is less than ideal but the researchers have taken the view that given nothing is currently available in the public domain on this issue then a partial data set is a move in the right direction.

Measuring Loss in a Mobile Shopping Environment: A Case Study

As detailed in the Methodology Chapter, the retailer that agreed to share data with the research team is a ✪multi-billion turnover grocer with many hundreds of outlets providing a wide range of products and services. It is important to reiterate the way in which the audit data was generated and the opportunities and limitations of this information. Like many of the other retailers installing this technology, the key defence against abuse was seen to be the threat of an end of shop audit (see below) when a customer is stopped and some or all of the items in their bag, basket or shopping trolley are checked for accuracy and where a discrepancy is found it is either added to the customer's bill or removed and replaced back on the shelf. This method arguably generates the most accurate 'shrinkage' data ever available to a retailer – the type and value of a product that is either being attempted to be stolen, or has been 'forgotten' by a consumer, is precisely measured over a relatively large sample of shoppers and over a relatively long period of time. For the majority of unrecorded shrinkage losses retailers typically have almost no idea of where, when and how losses have occurred, and so this level of granularity on specific forms of shrinkage losses is very rare indeed.

As detailed above, the causes of most shrinkage losses are unknown and are only usually uncovered at annual stock audits when the location, time and perpetrator are all unknown. With this type of audit data, all of these factors are known except for the motivation of the offender, which remains in doubt – was it an attempted theft (malicious) or simply human error (non-malicious)? So this is a potentially rich vein of information to understand the extent to which consumers using this technology are not scanning items they have put in their bag, basket or trolley. Where this data is more problematic is that the case study retailer tasked a member of staff undertaking an audit to only check a relatively small number of items – on average 6 – out of a typical basket size of 30 items. If one or more non-scanned items were found amongst the 6 items selected for audit, then they would be either added to the customer's bill or removed and replaced back on the shelf, **but** the remaining items would not be checked for accuracy. So, in effect, the 6 items were used as a 'sample' of the total contents of the shopping basket.

Some caution has to be expressed with this method of data collection as there are two principal flaws. First, while retail staff undertaking an audit were told to try and choose the selected items randomly from a bag, basket or trolley, inevitably items from the top are much more likely to be checked. This could allow malicious thieves to 'bury' non-scanned items at the bottom of the bag, basket or trolley to avoid selection and hence reduce the number of non-scanned items recorded. Second, if one or more non-scanned items were found amongst the few items chosen for audit then this is highly likely to suggest that other non-scanned items are present in the bag, basket or trolley, but these would not be found (for other retailers taking part in this research the identification of one or more non-scanned items would automatically trigger a full scan of all items in the bag, basket or trolley). This decision to limit the scale of the audit parameters inevitably reduces the overall number and value of items found to have not been scanned.

Unfortunately the data provided by the retailer did not separate audit data relating to shopping trips using scan guns provided by the retailer and those shopping trips which used a customers' mobile phone – the data was only available in aggregate form. While this limits our ability to talk specifically about the risks associated with MSP devices, the processes employed by the case study retailer were almost identical in terms of the way in which payment and audit were carried out for both types of mobile shopping.

The Case Study Data

As detailed above it is only possible to offer generalised data in order to protect the identity of the retailer. The data presented is based upon nearly 12 million shopping trips with a value of just over ✪ one billion in sales, over a 12 month period of time. Of those trips only 2% or about 250,000 were shopping trips where a mobile phone was used. Of those trips, the vast majority (80%) utilised an iPhone compared with an Android device (20%). At the present moment, the data suggests a very low take up rate for this technology, with consumers much preferring either the traditional form of shopping (self selection and scanning at a staff checkout) or the use of a handheld device provided by the retailer (a scan gun).

Of the nearly 12 million completed shopping trips some 1 million were subject to an audit, equating to just over 6 million items that were checked for scan accuracy. The total value of the audited items was over ✪21million with nearly ✪850,000 being found not to have been scanned. This equates to a shrinkage rate (calculated as a percentage of retail turnover) of 3.97%.

So how does this figure compare with other known shrinkage numbers? There are a number of international surveys undertaken to measure the rate of shrinkage in the retail sector. For purposes of comparison, four measures have been selected:

1. The agreed comparable shrinkage rate for the case study retailer taking part in this study.
2. The Global Retail Theft Barometer, which is the survey with the broadest global reach (the 2011 edition has been selected because it is considered as the most recent reliable version of the survey) (Bamfield, 2011).
3. The latest available rate from the National Retail Security Survey (2012), which is the longest running shrinkage survey, though it only covers the USA (Hollinger and Adams, 2012).
4. A survey carried out by the UK's British Retail Consortium (2012).

These comparisons are presented in Table 4.

Table 4 Comparisons of Mobile Scan Shrinkage Data With a Basket of Shrinkage Measures

Comparable Shrinkage Rates	Shrinkage Rate	Difference	
Mobile Scan Shrinkage Rate	3.97%	Point Difference	Percentage Increase
Case Study Company 2014[6]	1.47%	2.50	+170%
Global Retail Theft Barometer 2011[7]	1.29%	2.68	+208%
National Retail Security Survey 2012[8]	2.60%	1.37	+53%
The British Retail Crime Survey, 2012[9]	1.21%	2.76	+228%
Overall Average[10]	**1.79%**	**2.18**	**+122%**

What can be seen is that the rate of shrinkage generated by Mobile Scanning is considerably higher than the rate recorded by all the other studies – the highest difference being found with the British Retail Consortium where it was 228 per cent higher. Overall, when the average rate for the grocery sector data is compared, then the rate of shrinkage in Mobile Scanning is found to be 122% higher. This is a profound difference in the rate of loss and given that one estimate suggests the overall margin of profit in the European Grocery Sector is just 3% (Beck, Chapman and Peacock, 2003), then taken at face value, this rate of loss generated by Mobile Scanning could be seen as at best a not-for-profit retail venture.

There are two further points worth making. First, the case study company has not provided data on potential savings generated by the introduction of self scan technologies (as detailed earlier) that could mitigate against the significantly higher rates of loss found such as reductions in staffing and traditional check out technologies for instance. It may be that in the future this higher rate of loss may be sustainable if other store costs can be reduced to compensate for the elevated shrinkage risks associated with this type of retailing. Secondly, the data does not shed any light on the motivation of the shoppers found to have non-scanned items in their bag, basket or trolley – were they deliberately not scanning items because they were trying to steal them or had they genuinely forgotten to scan the items due to difficulties with the technology, distraction or absentmindedness? This is a critically important question in determining how to generate risk amplification with this form shopping – if it is predominantly the former, then this points to the importance of risk amplification through approaches such as audits to act as a credible deterrent, while if it is largely the latter, then it points towards the need to improve consumer communication, perhaps with products via some form of tag (see below), and or the overall design of the system. Either way, more research is needed to unpick this very high rate of non-scanning by consumers using mobile forms of scan technology.

[6] This is calculated based upon the Company's agreed rate of unknown shrinkage loss, which they regard as the most reliable comparator for this data.

[7] This is the comparable rate for the global grocery sector rather than the overall rate, which was 1.45%.

[8] This is the comparable rate for the US grocery sector rather than the overall rate, which was 1.47%.

[9] This survey does not provide a breakdown by type of retailer.

[10] This is based upon the average of the studies excluding the British Retail Consortium data, which is not a strictly comparable number as it reflects all the retail sector whereas as the others represent only Grocery, which is regarded as more comparable with the mobile scan shrinkage data.

4.6 Physical Crime Prevention, Virtual Guardianship and Risk Amplification

A key aim of the study was to consider what crime prevention mechanisms were already in place to prevent MSP-generated losses and what future mechanisms might need to be considered. It was apparent from the interviews that the key priority for retailers at the moment appeared to be around 'proof of concept' – to understand if an MSP system could be implemented in store and what the technological challenges were rather than what crime prevention solutions were required. The following quote characterises the approach taken:

> Retail is a funny game, get the technology out there, understand that it works in a number of stores and then we will, if the business case is good enough figure the rest out (Interview 4).

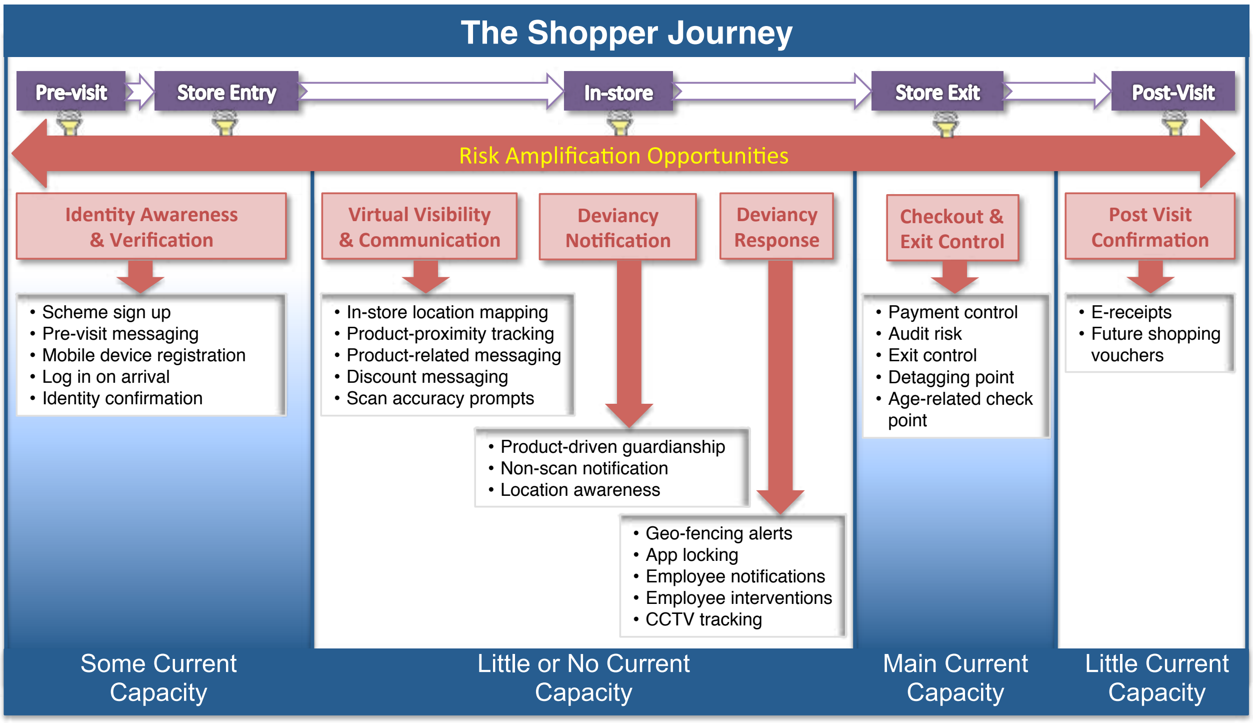
What was apparent from all of the retailers taking part in MSP trials was that very little developmental work had been put into fully understanding how the risks associated with it would be addressed beyond utilising the existing approaches used in other aspects of the retail business. This was aptly illustrated by one of the retailers who when asked how they were dealing with the problem of non-activation of soft EAS tags, that caused the constant activation of the exit alarm: 'currently we have no idea how we are going to fix this problem' (Interview 8).

It was clear that without fully understanding what the risks might be, it was hard for retailers to consider what crime prevention solutions might be considered and the costs that could justifiably be attributed to them. Overall the general approach to the development of any integration of crime prevention was based upon existing solutions (see below) and it is clear that in the near term developments will be largely reactive rather than proactive. As one interviewee noted, this was a result of the need for a strong business case in order to implement new crime prevention solutions:

> It's always harder to justify having mitigation if the problem hasn't already happened. So when the problem has arisen, you can then say "well this is what we've seen, if you bring in a solution, this is what we can say", so until that problem actually is in your face, then you're kind of almost chasing shadows in a way, because we have to then pay money for that solution, and if we haven't seen a loss as yet, then the business could turn around and say "we've not lost anything, why would I want to pay x amount of money for this type of solution? (Interview 1).

Sortie sans achat
Uitgang zonder aankoop
selfSCAN
Gagnez du temps tout en contrôlant votre budget
selfSCAN
Win tijd en hou je budget in het oog

Figure 1: Behaviour Control through Risk Amplification



Our analysis so far has suggested that MSP might generate shrinkage in a number of ways. We now consider how that risk might be reduced. By considering the shopper journey (see Figure 1) we identify (a) what crime prevention measures are currently integrated into MSP systems and (b) how physical and virtual preventative measures might be designed-in to MSP in the future. There are three key preventative properties that the model incorporates. First, there is a suggestion that there needs to be greater integration of the *physical* and *virtual* than currently exists. Second, it aims to develop ways in which to *amplify a sense of risk perception* and *reinforce risk* throughout the shopper journey. Third, the model identifies where *excuses* and *provocations* can be designed out of MSP.

There are five main points in the shopper journey – pre-visit, store entry, in-store, store exit and post visit. The model outlines the risk amplification opportunities at each point of the journey and whether these measures are either (1) currently available/being used by retailers and (2) how risk might be amplified in the future. We also consider how current product protection might be integrated into MSP systems.

Risk Amplification: Measures Currently Being Used

Current measures being used by the retailers taking part in this study focussed almost exclusively on the extremes of the shopping journey: store entry and the payment/checkout process, with the latter being regarded as the most important through some form of 'randomised' audit/checking.

With regards to generating risk at the start of the shopping journey, it was felt that minimising a sense of anonymity offered one feasible way of amplifying some form of risk for the would-be MSP shopper. Indeed, research on shoplifters has found that the greatest deterrent tends to be members of staff approaching and offering help – thieves are keen to remain anonymous and any contact with attentive staff is highly likely to put them off (see Cardone & Hayes, 2012). While the process of registration varied considerably between the case-study companies, all required the MSP shopper to 'register' their presence in the store. Indeed, some registration systems were more likely to promote a sense of risk than others. For example, in some stores you could pick up a loyalty card at customer service and immediately 'register' on the system and begin shopping, while others were more robust – requiring a valid email address/

mobile telephone number. In the one system where payment could be made via the App, then a further step of registering a credit card was required.

Research by Aloysius & Venkatesh (2013) found that shoplifters would not consider using a system where any personal details had to be revealed to a store, further suggesting that anonymity is preferred. However, for the most part the registration processes currently being used were open to easy manipulation through inputting false information, including the potential to use stolen credit card details. For instance, our trials showed that in one of the companies on entry to the store, there was no verification process or way of identifying that the person using the mobile device is who they claim to be – 'check-in' is via scanning a QR code at the front of the store. Once the code has been scanned the user is then presented with a welcome message: 'Welcome to Company A, are you at Location Y Store?' The shopper then verifies yes and is allowed to start scanning – it implies that the system doesn't really know where you are. This geo-specific question is a potentially good risk amplifier, but this form of log on and identify confirmation step is problematic. This type of log in recognition is device specific (anybody could use my device, with my details to scan and pay). Thus, more person-specific forms of log in and verification could be explored. Secure options that are currently available include a biometric solution where fingerprint ID could be used. Once logged in a pop up screen could then alert the customer with a real time message [i.e. Hello Mr Smith, Welcome to Company A at Rise Park. How are you? It is x time on this date]. This would not only alert the customer to the fact the system knows who they are and where they are, but also that it is working in real time.

In the current development life cycle of MSP systems, it is perhaps not surprising that there is currently little appetite for excessive rigour at this stage – sign up is currently low, the steps for registration, as detailed earlier are already rather complicated, and encouragement of usage is considered a higher priority than designing a potent risk amplifier through anonymity denial. But, future developments should certainly consider how this part of the process could be made more robust by ensuring transparency of identity of the would-be MSP user – knowing that somebody knows you are in the store reduces anonymity and could act as an important risk generator.

Once the MSP user has successfully registered their presence in the store at the start of their shopping journey, they are then very much left alone until they reach the end of the shopping journey – no other means of risk amplification are currently used. Once the customer has selected and (hopefully) scanned all the items they wish to purchase, they then encounter the only other risk amplifier currently available – the 'random' audit check. The process for doing this varied significantly between the retailers taking part in this study but all thought it was their most powerful weapon in generating risk in the MSP shopping journey. In risk generation terms, the process is relatively straightforward – the user is made aware that on a randomised basis they will be subject to a check on what they claim to have scanned and what is actually in their bag, basket or trolley. Because the audit is 'advertised' as random, this is supposed to generate a degree of risk within the user that is likely to deter them from purposefully non scanning items. In order for this to work, however, the risk has to be credible – the audits do need to happen, and the consequence needs to be sufficiently robust (i.e. the customer needs to know that there will be consequences for their miscreant behaviour). As discussed earlier, in a self-scan environment adhering to the first principle is significantly easier than the second – all the retailers had degrees of sophistication within their audit generation algorithms that could make audits happen based upon some form of risk factor associated with the user.

However, dealing with the outcome of a mismatch between claimed and actual basket content is much more difficult for retailers to achieve: some ignored it completely by not matching up the manual scan of all items with what was supposedly listed on the App (the difference was recorded but not made apparent to the member of staff undertaking the audit); others used it as a trigger to undertake a full scan of all items (where a partial scan had been requested by the audit algorithm); while some used the event to recalibrate the audit algorithm so that the user would be liable for much more frequent audit checks in the future (a form of punishment through audit-driven irritation). As detailed earlier none of the retailers had much appetite for prosecuting those who were found to have a mismatch in claimed and actual 'scanned' items. Thus, the level of confidence in claiming malicious intent was simply lacking for most cases to be taken to the criminal justice system.

As a risk amplifier, the end of shop audit process offers a rather ambiguous and complex message for the MSP user. On the one hand the awareness of the likelihood of being audited is a strong and unambiguous message, especially when it is backed up by a process which is perceived to be 'random', credible and thorough (some concerns were raised about when the system requested a small sample of items to be checked and the member of staff just picked up items on the top of the basket or bag when a motivated non scanner is likely to bury non scanned items at the bottom). However, on the other hand, the consequence of being found not to have scanned some items could be perceived as at best 'modest' and at worse 'non-existent' beyond having to pay for all the items in the bag, basket or trolley.

The 'non-scan defence' of 'I thought I had scanned them' is difficult to refute unless a visible and auditable trail of persistent behaviour is apparent (Beck, 2011). Perhaps what is more realistic and evident from some of the case study retailers is the imposition of informal punishment through inconvenience and irritation. As one retailer described their reaction to a known shoplifter who was trying to use the system to steal large quantities of goods: 'we've got this guy in and he definitely needs a full audit because he's one of the regulars. [We] Let him go through the whole system, made his life a pain by giving him a full re-scan' (Interview 10). In this case the offender quickly gave up using the system and probably reverted to other more traditional means of stealing from the store. Certainly the option of tailoring the audit frequency to the circumstances of the environment (is it a store with a known shrinkage problem?) and the profile of the user (have they mis-scanned before?) would seem to be a viable and important part of amplifying risk in the MSP shopping environment. Indeed, most of the retailers described a variety of shopper behaviours that could be used as triggers to increase the likelihood of an audit occurring. These included:

- Number of previous trips without an audit (audit cycles such as 1 in 10 shopping trips).
- Previous non-scanning events.
- Length of time since last non-scanning event (customers build up a confidence score).
- Evidence of product voiding within the shopping trip.
- Unusual shopping behaviour (e.g. typical purchases not evident in latest shopping basket).
- Unusually long shopping trip compared with number of purchases.
- Special offer purchases in basket (increased risk of BGOF non scanning).
- Well-known multi-purchase mis-scans in basket (for instance varieties of dog food all scanned via one variety).

To finish your transaction touch 'Scan & go shop' or scan your Nectar Card.

This list is in no way exhaustive and retailers were not keen to share them all for obvious reasons. In building audit trigger algorithms retailers clearly have to strike a delicate balance between generating a sufficiently credible risk-amplifying profile to encourage as many customers as possible not to abuse the system, while at the same time minimising user inconvenience and increasing staff costs through carrying out a large number of audits (in the retailer case study detailed earlier, a million audits had been performed in one year). All retailers taking part in the research recognised that the system had to be dynamic, adaptive and 'intelligent' – learning from previous consumer behaviour. Whilst not present in all the systems it was deemed important by some that the 'random' element should be controllable by local store staff, so that local knowledge of known offenders could be used to trigger audits. It was also considered very important that the communication with users about audits had to stress that they were triggered by the 'system' and not store staff – this was viewed as a key way of limiting any potential for violent and physical abuse of staff. For example, in the US, one of the retailers described a situation where the system rather than local staff was accused of being 'racist', programmed to only stop black people (Interview 9).

In the trials undertaken by the researchers the audit experience was rather mixed – policies varied on whether the first use of MSP should always trigger a full audit or not. Those in favour claimed it was an ideal opportunity to educate the user and reinforce the credibility of the audit; those against claimed it was important to ensure the user had as hassle free as possible shopping experience the first time around. The danger with the latter of course is that if such a policy became widely known then the inaugural shop for the new user could be seen as a licence to steal as much as possible knowing that they would definitely not be checked. In addition, on-going technical issues tended to undermine the efficacy of the

audit process – staff often had to apologise for glitches in the system and the need to de tag some items also acted as a distraction. However, as the systems improve then this is likely to become less of an issue.

Finally, one of the retailers combined the 'checkout' process with a form of exit control – the process of payment generated a bar code that had to be used to open the exit gate in the store. It did not of course have the capacity to know whether all the items had been scanned and paid for, but it was another form of risk amplification around the end of shopping journey experience.

Of the two risk amplifiers currently used by the retailers taking part in the study – registration when entering the store and the threat of audit at the end of the shopping journey, the latter was perceived to be the most important, but for some it was also incompatible with the spirit of how MSP was likely to transform future developments in retailing: 'Re-scan is labour intensive and potentially negates the business labour saving model' (Interview 4). In addition, the vision for some, where the shopper is given the ultimate freedom to shop when and how they want, was seriously undermined by what could be viewed as a rather draconian, untrusting and intrusive audit process at the end of the shopping experience. While perfectly true, the challenge is developing alternative and perhaps more subtle ways of generating and amplifying risk in the MSP experience that will offer the same if not better ways than audits do of enforcing customer compliance.

MSP and Current Product Protection Devices: Incompatible Retail Technologies?

One of the real challenges to those retailers investing in MSP systems is how to take account of any existing product protection devices currently employed in their retail stores. There are three main types of common product protection devices in use in retailing across the world:

- *Hard Electronic Article Surveillance (EAS) Tags* – these are normally highly visible tags firmly attached to products (such as clothing and alcohol), or in the form of spider of loop alarms, which can be wrapped around or through products (such as jackets and boxed electrical items), requiring a special tool to remove them.

- *Soft EAS Tags* – these are small flexible tags that can be attached either at the point of manufacture or when products arrive at distribution centres or retail stores. They can be either covert (hidden in packaging out of sight of the consumer) or overt (placed on the outside of packaging where it can be plainly seen). They are normally deactivated at the checkout via forms of scanning and close field technologies.
- *Safer Cases* – these are transparent lockable plastic cases that products can be placed inside. They may or may not have an EAS tag incorporated into them as well. The idea is that it makes the product more bulky and so less easy to steal, especially in large quantities (sweep thefts).

The use of these three technologies varies widely across retailing and there are a number of different standards within tagging technologies[11]. They are designed to act as a deterrent by increasing the risk of apprehension through activating alarms at exits if they are not removed or deactivated. Research suggests effectiveness may vary, not least because of the many ways in which the tags can be removed or shielded to prevent activating the alarms, and there are difficulties in getting retail staff to provide a credible and consistent response to alarm activations, especially when deactivation processes are patchy and inconsistent (Hayes and Blackwood, 2006; Beck, 2007). However, their use is very widespread and often a key component in the loss prevention strategy of many retailers.

Of the retailers taking part in this research who had active MSP systems in operation, only two used soft and hard tags on a regular basis – the others did not rely upon any form of product-based protection.

The challenge presented by MSP systems is how these types of protection devices can be removed or deactivated in a way that does not comprise security or generate too much inconvenience for the consumer. For instance, it would not make good security sense to provide the MSP user with a place in the store where they could take the tags off themselves or deactivate them. This creates problems in knowing what products had been paid for and it could also allow shoplifters to de-tag items in order to steal products. At a SCO or staffed checkout, a member of staff is on hand to remove hard tags and safer cases, while some SCO checkout machines are designed to deactivate tags when the barcode is scanned. At the same time, developing a deactivation process that significantly inconveniences the MSP shopper is equally undesirable – it would not be very acceptable if the MSP shopper had to, for instance, go to the customer service desk and unpack all their goods so that those with a tag attached could be removed or deactivated.

One of the retailers using MSP and product protection freely admitted that they had not found a solution to the problem – soft tags were not being deactivated and a consumer exiting the store having purchased any products with this type of protection attached would activate the alarm: 'we can't guarantee that people aren't going to walk out and set the alarms off because they haven't been de-tagged … ' (Interview 9). The view was that the guard at the exit somehow knew that the customer was an MSP user and simply allowed them to leave. This is highly problematic for a number of reasons. First, it yet further reinforces already high levels of staff scepticism about the validity of exit alarms – indeed that 'tag pollution' perpetuates the 'crying wolf' syndrome. Secondly, it undermines the ability of the store guard to respond to the exit alarm when there are a significant number of alarms being activated by legitimate MSP users – how do they know whom to stop? Thirdly, it can cause shopper embarrassment when they trigger the alarm – particularly if a security guard in front of other shoppers stops them.

The other retailer using product protection had developed their App to alert the consumer to when a product they had scanned was protected and required a tag to be removed (hard tags or safer cases). The App

[11] See Hayes and Blackwood (2006) for a complete overview of the various types of EAS tags used by the retail industry.

would also flag this up and prevent the payment step being completed until a member of staff had been called and they removed the tag. This seemed to work reasonably well but was clearly dependent upon the user having to pay at a specific point in the store (they had not developed a mobile wallet option) and the member of staff removing all the tags.

The interviews shed little light on how the industry was proposing to deal with this issue. As one retailer stated, 'you need retailers and manufacturers to come together (and I guess and tech guys) to say, "This is what we want to do in the future" and at the moment we're just too early on that evolutionary route with self-scanning to have that' (Interview 8). Although the product protection provider suggested that new technologies are being developed it was not clear how advanced these are: 'we have a number of technology products [being developed], how far down the road is another question' (Interview 9). At present, most current efforts seemed to be focussed on the SCO environment and how deactivation technologies could be better incorporated into fixed scan technologies. The only possible options currently available were focussed on RFID tags. As the product protection provider stated 'there is an RFID solution in there… if you can come up with a really good RFID solution, then it will help implement RFID in retail and you'll get all sorts of benefits' (Interview 9). The challenge is developing an RFID solution that could be used in an intelligent way to deactivate when the consumer had purchased the products – in effect the tag communicates with the store inventory and when the payment is authorised the tags switch status from 'not sold' to 'sold' and consequently will not activate the exit alarms. But as discussed in detail above, current RFID technologies are only capable of operating effectively on largely non-metal and products containing relatively small quantities of fluid, or the cost of the tags makes it prohibitively expensive to put on small value items, which rules out in excess of 70-80% of products in most grocery retailers (which are the group mainly developing MSP systems).

This is a significant and yet to be resolved challenge for the retail industry and their security suppliers. Retailers themselves recognised the problem but had no current solution, particularly when they used soft EAS tags. A short term fix for another was to add a process step within the App and the payment process to ensure a member of staff was alerted to remove any hard tags, but this hardly sits well with the overall ethos of MSP shopping. Within the security industry there was little appetite to discuss how future developments in MSP might compromise existing product protection approaches – it seemed the development did not sit well with current business plans and product developments.

In the longer term, as detailed above, the development of a smarter tag that can be applied to all products and have the capacity to communicate with its environment, would seem to be the answer to the problem. Not only would it increase deterrence by communicating directly with the would-be miscreant, but it would also give credible and timely information to local guardians who in turn would be more willing to take the threat seriously and respond accordingly. Until then, retailers who intend to make use of current product protection technologies and introduce MSP systems are likely to face a range of compromises as the two clash and compete in the retail environment, with both undermining the other.

Amplifying Risk in the MSP Shopping Experience: What Might the Future Bring?

As detailed above, retailers are currently focussed upon just to two stages of the MSP shopping journey to amplify risk – when the consumer enters the store, through a process of anonymity reduction, and when the consumer decides to pay, through the threat of audit-induced awareness of miscreant behaviour. In reality the latter is by far the most important weapon in the retailer's current risk amplification armoury. This is less than ideal, leaving the majority of the shopping experience free from any form of risk amplification whatsoever. The audit check is also a rather blunt and potentially disruptive strategy – likely to irritate customers, bring staff into possible conflict situations and impact upon potential staff savings and consumer convenience.

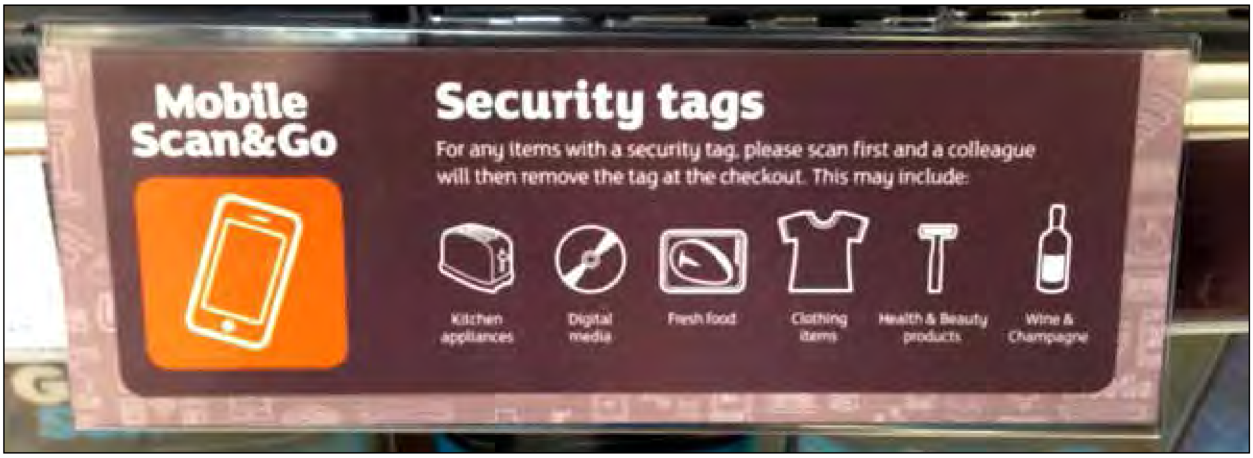
What follows is how, through a mixture of existing and as yet close to development technologies, together with changes in business processes, the MSP shopping experience could be made less likely to generate unacceptable levels of risk and losses for retailers who decide to embark upon its use, while at the same time offering the shopper a potentially seamless journey. As illustrated in Table 5, it is done through describing how a future shopping trip might unfold, how the various elements might act to amplify risk and whether the technologies currently exist to achieve this outcome. We have, wherever possible, tried to create a scenario which relies upon technologies that are either currently available in some form or near to development – it would be very easy to create a scenario which relied upon sci-fi style technologies which are unlikely to be seen on the high street in the foreseeable future.

Table 5: The Mobile Scan and Pay Shopping Trip of the Future

Steps in the MSP Shopping Journey	Risk Amplification	Feasibility
Registration to use MSP: In order to use the MSP service the shopper of the future has to provide a verifiable email address and register a credit/debit card as well as register the device upon which the MSP App will be used. Only those devices that employ biometric verification to operate are allowed to be registered to ensure customer security and convenience.	By requesting that MSP users establish a number of identity checks prior to using the system, it minimises the opportunity for the user to perceive themselves as anonymous. The process is marketed as a highly secure and convenient way to shop.	Retailers could introduce this with current technologies
Pre-shopping trip: Prior to arriving at the store the shopper has received a series of in-App alerts from the retailer about a number of special offers currently available at their local store together with some e-vouchers only they can use. The alerts are sent to coincide with the usual time when the shopper typically visits the store to reduce customer irritation.	Once again, establishing retailer awareness of the consumer and reducing anonymity – 'they know when I am coming to the store'.	Retailers could introduce this with current technologies – would require analysis of previous shopping history.
Arrival at the store site: As the shopper pulls into the car park the App gives advice, via mapping functionality, about the nearest free parking spaces, recognising whether they are entitled to use any special parking bays such as those reserved for disabled customers or parents with children.	Yet more consumer identification and anonymity reduction.	Retailers could introduce this with current technologies – would require consumers providing additional information about themselves.
Store entry: As the shopper enters the store the App automatically activates the shopping trip functionality, including an integrated shopping list and a proposed route around the store to optimise the shopping journey (including possible diversions for products on offer they might be interested in).	Yet more consumer identification and anonymity reduction.	Possible with current technologies – product locations would need to be geo-located in the store and the location of the consumer's device monitored via store Wi-Fi.
The shopping trip: The shopper begins their shopping trip and starts to remove items from the shelves and scan the barcodes using their mobile device. As the products leave the shelf this is recognised by the store system and the product, via a smart tag that knows whether it has been scanned or not.	No risk amplification at this stage.	Some of this technology currently exists, such as iBeacons, which can recognise micro movements of objects and some RFID technologies will notify the store system of the status of a product. Unfortunately, most current RFID tags only work on some types of products (they do not work well on metal and products containing fluids).
Non-scan alert 1: Our shopper is in a hurry and unfortunately forgets to scan one of the items and puts it into the trolley. The product senses that it has moved from the shelf and is now in close proximity to other items that have been scanned. As the trolley moves to more than 2 metres away from the product's shelf location it sends a message to the App saying that it has not been scanned and asks the shopper if they would like to do this.	This will alert the consumer that the system is fully aware of what has and has not been scanned. The risk of not scanning the product becomes elevated.	While some current tags could achieve this level of functionality, they are relatively expensive, bulky and would require some form of power source.
Non-scan alert 2: The shopper ignores the message and continues to move down the aisle. As they reach the end of the aisle, the App flags up an alert telling the shopper that if they do not scan the item before leaving the aisle then the App will be suspended and the shopping trip will end.	This further reinforces the risk of apprehension and introduces a level of punishment – the shopping journey will be terminated	Current RFID tags can identify when tagged products have moved from one area to another.
Place manager notification 1: As the non-scanned product reaches the edge of the geo-fenced area it sends a message to the automatic CCTV system that then begins track the shopper. It also sends a message and a picture of the shopper (from the CCTV system) to the nearest member of staff.	None at this stage	Digital CCTV systems can now automatically track objects. Through existing technologies, information about a particular product and a picture of a person could be sent to a member of staff using a hand held device.

Steps in the MSP Shopping Journey	Risk Amplification	Feasibility
Place manager response 1: The member of staff then approaches the consumer and offers them help relating to the particular product that has not been scanned, perhaps reassuring them that the barcode on this product is always a little tricky to scan.	This is a major risk amplifier – detailed knowledge of a particular non-scanned product by a member of staff would significantly heighten the shoppers concerns about the risk of being caught and store visibility of their actions. It would be a strong reinforcing moment of the capability of the surveillance network in the store.	Currently possible with existing technologies.
Place manager surveillance: Once the product is correctly scanned the shopper leaves the aisle but continues to be tracked by the CCTV system until the system is satisfied they have correctly scanned the next 5 items taken from the shelves.	None at this stage	Current Digital CCTV systems can provide this capability.
Visual recognition: On the shopping list is a bottle of alcohol and as the consumer selects and scans the item, the CCTV system, via facial recognition, confirms the shopper holding the mobile device that scanned the item is the person registered with the company, who has been confirmed as above the statutory age to buy alcohol. The App shows a message to this effect.	Once again, the system is reinforcing its awareness of the shopper's behaviour and their personal information.	New developments in facial recognition have improved reliability, especially if the camera could achieve a low level front on picture of the face of the consumer.
Place manager notification 2: The consumer reaches the end of their shopping list and begins to head towards the exit, forgetting to pay for the items that are in their trolley. As they reach a geo-secure area near the exit the scanned items alert the store that they are not connected with a payment transaction and once again trigger the CCTV system to send a message to the store guard with a picture of the shopper.	None at this stage	Current RFID technologies can do this.
Place manager response 2: The guard approaches the customer and offers them assistance to help use the App to make payment for the list of items he is viewing on his mobile device. The customer then makes payment and leaves the store. The incident is logged against their customer profile.	Final confirmation of the system's awareness of the movement and behaviour of the shopper, which is reinforced through human intervention.	Current technologies can do this.
Store exit: The consumer is then guided back to their car via mapping technology that logged the location of the vehicle.	Consumer further aware of the store being aware of their location	Current technologies can do this.
E-receipt issued: An electronic copy of their receipt is sent to their email address.	Final confirmation of the identity of the shopper with the recent shopping event	Current technologies can do this.

For some the above scenario will paint a nightmare picture of surveillance and dystopian control imposed by a ruthless retail organisation, manipulating their customers by constantly monitoring their location, shopping habits and lifestyle choices (Albrecht & McIntyre, 2005; O'Hara & Shadbolt, 2008). For others it is a vision of how the shopper of the future will be given a more flexible, smarter shopping experience tailored precisely to their individual needs, desires and expectations. Regardless of the desirability (most of the tracking capability described above currently exists and is used by smart device users on a regular basis) what is interesting to this research is the way in which the MSP shopping environment could be better controlled through a more nuanced and embedded form of risk amplification. It offers a way to move from the current rather blunt and one dimensional approach, principally based upon consumers being worried that they might be stopped for an audit at the end of their shopping journey, which may expose their malicious or non-malicious product scanning activities, to one which is integrated into the actual shopping experience based upon virtual


Mobile Scan&Go
Security tags
For any items with a security tag, please scan first and a colleague will then remove the tag at the checkout. This may include:
Kitchen appliances
Digital media
Fresh food
Clothing items
Health & Beauty products
Wine & Champagne

visibility and communication, deviancy notification and deviancy response. In effect the production of risk becomes the responsibility of the products themselves – they become the guardians of control through virtual communication with the shopper and other parts of the retail environment. Through these links products are capable of amplifying risk to the consumer – in effect saying: 'not only can I tell you [the shopper] that you haven't scanned and paid for me, but I can also tell other capable guardians [typically humans] you haven't and they will ensure that you do'.

In addition to dealing with the core issue of making the consumer aware of the system's capacity to identify when they have and have not scanned and paid for items, it also relies upon significantly limiting the opportunity for the would-be MSP user to do so anonymously. The registration to use the system needs to be sufficiently robust to not only satisfy the retailer about the identity of the user but also in the case where age-restricted products are on sale, the courts and legislators. As previous research has shown, would-be shoplifters are less likely to steal when their presence and identity is known to the retailer (see Cardone & Haynes, 2012). As mobile phones become ever more ubiquitous, and the link between the owner and the location of the device becomes even more embedded in case law (see McGowen, 2002)[12], then issues of false representation will be minimised. In addition, the greater use and acceptance of biometric technologies will further limit the opportunities to use MSP technologies anonymously.

For most of the steps outlined above, current technologies can already deliver some of the requirements to make it a reality, certainly in terms of data sharing and technological convergence – getting digital CCTV systems to talk to information databases is not overly difficult. Equally, micro location monitoring and the transmission of hyper-contextual information through technologies such as Apple's iBeacon and Bluesense Networks' Bluebar[13] using Bluetooth Low Energy wireless protocols can already be seen in some retail spaces (Tech Crunch, 2013). The real challenge is developing some form of tag that can enable the majority of consumer products to communicate with their environment – RFID tags have been found to offer this potential but on only a relatively small range of products, primarily those that have little metal or fluid content (van Eeden, 2004). No other tag technologies seem to be able to offer this type of capability at this moment in time. Even if one could be developed, and a staged approach to its application in the retail environment was established (perhaps putting them first on items of high value or more prone to theft), the reality is that retailers and their suppliers would need to invest heavily in a significant amount of technological infrastructure to achieve this outcome. This is not without precedent – the retailer Decathlon is attaching over 500 million RFID tags per year to more than 80% of all products in 840 stores across 22 countries, creating an almost fully integrated RFID architecture (ECR, 2015), but the benefits to the retailer and the consumer need to be very carefully articulated before such an investment is made. In this respect, the history of the development of RFID is instructive – it has been continually promising to revolutionise the retail world since it was first launched back in the late 1990s (Beck, 2006), but has been dogged by poor technological performance and an inability to develop a Return on Investment (ROI) model that is palatable to the retail and manufacturer community.

[12] For example in the Damilola Taylor murder case two suspects claimed to have an alibi at the time of the attack: a mobile phone belonging to one them was used miles away from the scene of crime, and this was considered sufficiently robust evidence to be accepted by the Judge.

[13] See: http://beekn.net/guide-to-ibeacons/.

Summary and Future Research

Volg de instructies op de betaalautomaat
Uw bon kan worden gecontroleerd

5. Summary and Future Research

The move to develop and introduce mobile scan and pay (MSP) can be seen as part of long-term changes in the retail industry that have seen increased customer autonomy and self-service at the expense of formalised staff/customer interactions. What seems clear from this research is that retailers will need to continually look at a range of mobile technologies, including those focussed on scan and pay, to better understand how they might bring benefits to their businesses, through improved customer convenience and satisfaction, and potentially organisational efficiencies. This is a rapidly developing field with few signposts other than ensure continuous innovation or risk stagnation. As has been documented in this report, there are a number of retailers around the world who are actively trialling MSP technologies with varying degrees of success. Some have begun to develop a gradual roll out as the numerous technological and organisational hurdles have been overcome, while others have gone back to the drawing board to reimagine how it might fit (or not) with the broader priorities of the business.

The main focus of this research has been on whether and how MSP might generate increased levels of loss and what if any crime prevention solutions could be developed to try and minimise the risk. The research has found that MSP systems have the real potential to create elevated levels of risk for retailers – it removes (in theory at least) the need for any form of human contact throughout the entire shopping journey, including probably the most important element, the point of payment. This could lead to increased levels of non-scanning either due to malicious intent (stealing) or non-malicious practices (absentmindedness, distraction or faulty technologies) that could lead to unacceptably high levels of loss. As was found from the data provided by one of the retailers, rates of loss were over 122% higher in relation to mobile scanning and this brought the overall rate above the typical average profit margin for the European Grocery sector – making it a largely unprofitable exercise.

A concern is that 'non-scanning' could become part of the routine behaviours of some shoppers and people might be attracted to stores in the knowledge that they can chose to not scan certain products with relatively little risk of being prosecuted. In addition, allowing customers the freedom to self-scan gives them the opportunity to develop 'neutralisation techniques' that 'blame' faulty technologies, or problems with barcodes or even absentmindedness as the reasons for non-scanned items being present in their bag, basket or trolley. For some retailers this 'self-scan defence' could be come a recurring and highly problematic scenario for store staff to deal with, making prosecution of shop thieves highly unlikely. Observations of MSP systems found that staff were always more than willing to accept this as a form of defence and across some jurisdictions retailers have been concerned about potential reputational damage that might be caused by prosecuting customers for non-scanning some of the items in their bag, basket or trolley.

Other concerns were also raised by respondents interviewed in this research, not least worries about potential fraudulent activities, including the production of self-scan labels that might be stuck on products and the potential for fraudulent payments. It was thought that the payment wallet could generate fraud as it could facilitate the use of stolen credit card details and the fraudulent use of electronic vouchers or coupons. In addition, in future MSP systems there might be increased ambiguity over where the last payment point is within a store – potentially payments could be made in the shopping aisle or (Wi-Fi permitting) in the car park of the store. This will create problems in understanding where in the shopper journey the final payment point is and thus where retailers can legally challenge suspected shop thieves.

More broadly, concerns were expressed that non- and mis-scanning of items could have a detrimental 'knock on' effect in relation to inventory accuracy and on-shelf availability of stock. Thieves are notoriously unreliable when it comes to updating stock reports when they take products and customers may not readily appreciate the impact of scanning the same item multiple times when a range of similar varieties are actually being purchased.

In order to minimise crime-related losses retailers have developed a wide range of ways of amplifying risk so that would-be offenders perceive it to be not worthwhile committing crime in this environment because of an enhanced concern about being caught. For the traditional shopper/thief this is done in a number of ways including signage, tags on products, visible CCTV, staff checkouts and so on. For the thief, the typical way of stealing is to try and conceal items on their person and hope that staff either in person or on CCTV do not see them. While certainly not wholly effective, this range of risk amplification methods have worked reasonably well at keeping levels of loss within tolerable boundaries. With the introduction of MPS systems, most of these existing systems are, if not made redundant, then certainly seriously compromised. MSP users can 'scan' items on the go and place them directly in their bags, they can then use their mobile phone to make 'payment' without interacting with a member of staff and then leave the store – it is a fluid and potentially uncontrolled shopper journey with few of the traditional mechanisms of risk amplification playing a role in invoking concern about the risk of apprehension in the mind of the user should they not stick to the 'rules'.

In order to meet this challenge retailers taking part in this study have focussed upon just two points in the shopper journey to amplify risk in the mind of the MSP user – at the start of the trip and at the end when payment is required. The former is typically done through some form of registration either with a store card or other form of identification, while the latter is delivered via check audits carried out according to some form of algorithm. No other means of risk amplification are currently available beyond these two points in the shopper journey. It was concerning that very little developmental work had been put into fully understanding how the risks associated with MSP would be addressed beyond utilising these two approaches. Some respondents did infer that without fully understanding what the risks might be, it was hard for retailers to consider what additional crime prevention solutions might be considered and what costs could justifiably be attributed to them.

In the short term it seems that having a credible and reliable audit check process in place is the only available mechanism to inject any real sense of risk into an MSP programme. The process for doing this varied significantly between the retailers taking part in this study but all thought it was their most powerful weapon in generating risk in the MSP shopping journey. In the medium term this may be supplemented by more nuanced methods of user identification and verification – ensuring that prospective users register enough information to minimise their sense of anonymity as they enter and use the system. It was observed that, for the most part, the registration processes currently being used were open to easy manipulation through inputting false information, including the potential to use stolen credit card details.

A key challenge is developing longer-term solutions that are designed or integrated into MSP systems. At present there are difficulties in integrating tagging/product identification in the MSP shopper journey. However, in the longer term developments in tagging/product identification technologies should enable the risk amplification process to be more firmly embedded in the shopping journey, offering would-be users regular cues and prompts, both virtual and physical, about the risks they are taking should they attempt to subvert the system. For example, a series of retailer/customer messages (via the App) at arrival and entry to the store could reduce customer anonymity at the start of the shopping process. During the shopping trip non-scan alerts could notify shoppers and security personal if products have not been scanned. Visual recognition CCTV could be used to conduct age restricted checks. Geo secure areas could be used to make payment. While some technologies can already deliver some of the requirements required to increase risk in the steps outlined above, the challenge is developing a tag that can enable the majority of consumer products to communicate with their environment – RFID tags have been found to offer this potential but on only a relatively small range of products. No other tag technologies seem to be able to offer this type of capability at this moment in time.

Summary of Findings and Future Research

1. As yet the consumer appetite for MSP systems is unproven – current systems have not seen a high degree of take up thus far, with shoppers presently preferring either fixed self scan checkouts, self scan guns provided by the retailer or traditional staffed checkouts.
2. Numerous technological and user issues continue to limit retailer confidence in using such systems, such as consistent store Wi-Fi, reliable scanning systems and the 'third hand' syndrome.
3. Developing a secure and reliable payment wallet is proving challenging for some of the early pioneers of MSP – largely unsupervised and seemingly non-controlled payment is generating much anxiety amongst some loss prevention executives.
4. Most retailers and technology providers have not resolved how to incorporate existing product protection technologies with MSP. For the foreseeable future technologies such as EAS tagging systems are likely to clash with, rather than complement MSP systems, causing staff and customer irritation.

5. Existing risk amplification approaches do not fit well with MSP systems – there is a need to create new ways to increase the perceived risk of being caught through product initiated guardianship and consumer communication. In addition, reducing consumer anonymity when using MSP systems will further amplify risk.
6. Check audits generated by consumer behaviour driven algorithms are the only realistic current way of amplifying some form of risk in the MSP environment. Future algorithmic models will make increasing use of a broader range of consumer-based data to create more nuanced approaches to performing these checks, including consumer shopping patterns, store tracking and other socio economic factors.
7. Available data indicates that mobile scanning technologies, including MSP, generate significantly high rates of loss (3.97% as a percentage of turnover), more than 122% higher than the average rate of shrinkage and higher than the typical profit margin (approximately 3%) of the European Grocery sector. The data suggests that this type of 'service' is not likely to generate a high profit margin unless other areas of cost can be reduced to compensate for the inflated rate of loss generated, or users can be encouraged to non-scan less.
8. The various mobile self scan technologies generate uncertainties around whether evidence of non-scanning is a result of malicious or non-malicious behaviour – does it create a new low risk way of stealing for the opportunistic shoplifter or highlight essentially honest, loyal but absentminded shoppers who are not very good at scanning goods consistently? This potentially places retailers in a difficult position both in terms of how to develop ways of legally prosecuting miscreant behaviour and at the same time reassuring the non-malicious customer.
9. If customers do begin to steal at a higher rate because of a perceived reduction in risk, such as through the use of the 'self scan defence' of presumed error, retailers might be seen as ultimately creating a crime-generating environment. In this situation claims by retailers of high rates of victimisation and a perceived poor response from the criminal justice system to their problems, might be seriously undermined by counter claims of promoting profit above social responsibility by 'allowing' thieves to help themselves without sufficient controls in place.

Undoubtedly, the study of the potential impact of MSP on retail losses is in its infancy – relatively few retailers are actively testing these technologies at the moment although many are reviewing their strategic business plans to better take account of how the 'mobile world' is changing the retail environment. Like any research in a newly evolving field, it has inevitably generated a series of new questions requiring exploration, including:

- Will the consumer of the future adopt MSP as their preferred mode of in-store shopping?
- Can a more robust Return on Investment model be developed which takes full account of all the costs and benefits of MSP systems?
- How might the applicability of MSP systems be affected by store type and socio-economic factors, such as local crime rates?
- Can a more reliable picture be developed of whether non-scan events are malicious or non-malicious – can the motivation of the non-scanner be better understood?
- Are there particular types of products that are more likely to be non-scanned either maliciously (highly desirable or easily resold items) or non maliciously (such as poor product and bar code design)?
- How tolerant will customers be of various types of crime prevention mechanisms focussed on MSP and will this vary depending upon the prevailing consumer culture?
- How can existing product protection technologies be adapted to make them more compliant with MSP systems?
- What evidence is there of consumer concern about retailer tracking and surveillance generated by MSP systems?
- How can end of shop audit algorithms be developed to create the right 'amount' of risk amplification for any given consumer?
- How might new tagging technologies be developed to create risk amplification throughout the MSP shopping journey?

This is in no way an exhaustive list of future research questions relating to MSP but it does highlight a number of key questions that will help retailers to better understand how their future mobile shopping offer might either give them a powerful and profitable competitive edge or alternatively, generate excessive losses that could prove highly detrimental to the overall health of their business.

6. References

Albrecht, K. & McIntyre, L. (2005) *Spy Chips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nashville: Nelson Current.

Aloysius, J. & Venkatesh, V. (2013) *Mobile Point-Of-Sale and Loss Prevention: An Assessment of Risk*, The Sam M. Walton College of Business: University of Arkansas.

Bamfield, J. (2011) *The Global Retail Theft Barometer 2011*, Nottingham: Centre for Retail Research.

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

Baxter- Reynolds, M. (2013) 'Consumer mobile app casebook – Sainsbury's Mobile Scan-and-go'. www.theplatform.io, 12 September [accessed 26th August, 2014].

Beck, A, Chapman, P. and Peacock, C. (2003) *Shrinkage: A Collaborative Approach to Reducing Stock Loss in the Supply Chain*, Brussels: ECR Europe.

Beck, A. (2006) 'Shrinkage and Radio Frequency Identification (RFID): Prospects, Problems and Practicalities'. In M. Gill (ed) *The Handbook of Security* (First Edition), Basingstoke: Palgrave MacMillan: 462-482.

Beck, A. (2007) 'The Emperor Has No Clothes: What Future Role for Technology in Reducing Retail Shrinkage?', *Security Journal*, 20 (2): 57-61.

Beck, A. (2011) 'Self-scan checkouts and retail loss: Understanding the risk and minimising the threat', *Security Journal,* 24 (3): 199-217.

Beck, A. (2014) 'Understanding Loss in the Retail Sector'. In M. Gill (ed) *The Handbook of Security* (Second Edition), Basingstoke: Palgrave MacMillan: 361-382.

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

Berman, M. & Kaplan, S. (2010) 'Directed Attention as a Common Resource for Executive Functioning and Self-Regulation.' *Perspectives on Psychological Science,* 5 (1): 43-57.

British Retail Consortium (2012) *Retail Crime Survey 2012*, London: British Retail Consortium.

Butler, G. (1994) 'Shoplifters Views on Security: Lessons for Crime Prevention'. In M. Gill, *Crime at Work: Studies in Security and Crime Prevention*, Leicester: Perpetuity Press: 56-72.

Cardone, C. & Hayes, R. (2012) 'Shoplifter Perceptions of Store Environments: An Analysis of how Physical Cues in the Retail Interior Shape Shoplifter Behaviour', *Journal of Applied Security Research*, 7 (1): 22-58.

Chapman, P. & Templar, S. (2006) 'Scoping the contextual issues that influence shrinkage measurement'. *International Journal of Retail and Distribution Management,* 34 (11): 860-972.

Clark, L. (2013) 'A big app-ortunity for indies too'. *The Grocer*, 12th October: 40-42.

Clarke, R. V. (ed) (1992) *Situational Crime Prevention: Successful Case Studies*. Guilderland, NY: Harrow and Heston.

Clarke, R. V. (ed) (1997) *Situational Crime Prevention: Successful Case Studies* (Second Edition). Guilderland, NY: Harrow and Heston.

Clarke, R. V. (1980) 'Situational Crime Prevention: Theory and Practice', *British Journal of Criminology*, 20: 136-147.

Clarke, R. V. & Homel, (1997) 'A Revised Classification of Situational Crime Prevention Techniques'. In, S. Lab (ed) *Crime Prevention at a Crossroads*. Highland Heights, KY and Cincinnati: 17-27.

Cornish, D. B. & Clarke, R. V. (1986) *The Reasoning Criminal: Rational Choice Perspectives on Offending*, New York: Springer-Verlag.

Cromwell, P. & Turman, Q. (2003) 'The devil made me do it: Use of neutralizations by shoplifters'. *Deviant Behaviour,* 24 (6): 535-550.

Curtis, B. (1971) *Security Control: External Theft*, New York: Chain Store Age Books.

Duncan, E. (2014) 'Death of the High Street? Hurrah…', *The Guardian*, 27th April, http://www.theguardian.com/commentisfree/2014/apr/27/dont-mourn-loss-of-high-street-turn-shops-into-houses [accessed 2nd March 2015].

ECR Europe Shrinkage and OSA Group (2015) *Presentation by Decathlon*, Barcelona, 28th January, access to presentation slides restricted for commercial reasons.

Ekblom, P. (2010) 'The Private Sector and Designing Products Against Crime'. In, C. Welsh and D. Farrington (eds) *The Oxford Handbook of Crime Prevention*. Oxford: Oxford University Press: 384-403.

Farrell, G. (2005) 'Progress and Prospects in the prevention of Repeat Victimisation'. In, N. Tilley (ed) *Handbook of Crime Prevention and Community Safety*, Cullumpton: Willan: 143-170.

Farrell, G. & Pease, K. (1993). *Once Bitten, Twice Bitten: Repeat Victimization and its Implications for Crime Prevention*. Crime Prevention Unit Paper 46, London: Home Office.

Felson, M. & Clarke, R. V. (1998) *Opportunity Makes the Thief: Practical theory for crime prevention*. Police Research Series Paper 98, London: Home Office.

Halliwell, J. (2013) 'Retailers need to get smarter about phones', *The Grocer*, 12th October, 2013: 36-38.

Hayes, R. & Blackwood, R. (2006) 'Evaluating the Effects of EAS on Product Sales and Loss: Results of a Large-scale Field Experiment', *Security Journal*, 19 (4): 262-76.

Hollinger, R. & Adams, A. (2014) *National Retail Security Survey 2012*, Florida: University of Florida.

IDC (2014) *Smartphone Vendor Market Share 2014*, http://www.idc.com/prodserv/smartphone-market-share.jsp [accessed 6th March 2015].

McGowen, P. (2002) 'Damilola Boys Have Phone Alibi'. *London Evening Standard*, 14th February, http://www.standard.co.uk/news/damilola-boys-have-phone-alibi-6330448.html [accessed 6th March, 2015].

McKinsey & Company (2014) *The Future of Retail: How to make Your Bricks Click*, http://mckinseyonmarketingandsales.com/the-future-of-retail-how-to-make-your-bricks-click [accessed 2nd March 2015].

NCR (2012) *How Self-Checkout Can Impact Retail Shrinkage: An NCR White Paper*, Georgia: NCR Corporation.

O'Donnell. J. & Meehan, S. (2012) 'Self-checkout lanes boost convenience, theft risk', *USA Today*, 4th September, http://usatoday30.usatoday.com/money/industries/retail/story/2012-04-06/self-scanning-checkout/54117384/1 [accessed 29th August, 2014].

O'Hara, K. & Shadbolt, N. (2008) *The Spy in the Coffee Machine: The End of Privacy as we Know it*, Oxford: Oneworld Publishing.

Ramchurn, R. (2012) Retailers must 'downsize to survive', *Architects Journal*, 4th April, http://www.architectsjournal.co.uk/news/daily-news/-retailers-must-downsize-to-survive/8628854.article# [accessed 29th August, 2014].

Smith, M. & Clarke, R. V. (2010) 'Situational Crime Prevention: Classifying Techniques Using "Good Enough" theory. In, C. Welsh and D. Farrington *(eds) The Oxford Handbook of Crime Prevention*. Oxford: Oxford University Press: 291-315.

Sykes, G. & Matza, D. (1957) 'Techniques of Neutralisation: A theory of delinquency', *American Sociological Review,* 22 (6): 664-670.

Taylor, E. (2013) *Mobile Technologies in retail: A review of benefits and risk*, Kingston, Australia: Efficient Customer Response Australasia.

Tech Crunch (2013) *Apple Turns on iBeacons in all 254 US Stores for in-store Notifications and More*, http://techcrunch.com/2013/12/06/apple-ibeacons-u-s-retail-apple-store/ [accessed 6th March 2015].

The Independent (2013) 'High Street Blues: The Slow Death of Retail Britain', *The Independent*, 20th January, http://www.independent.co.uk/news/business/analysis-and-features/high-street-blues-the-slow-death-of-retail-britain-8458766.html [accessed 2nd March 2015].

Tilley, N. (2010) 'Shoplifting', in F. Brookman; M. Maguire; H. Pierpoint and T. Bennett (eds) *Handbook on Crime,* Willan, Collumpton: 48-67.

Turley, C., Ludford, H., Callanan, M. and Barnard, M. (2011) *Delivering the NOMS Offender management Model: Practitioner Views from the Offender Management Community Cohort Study*, London: Ministry of Justice Report 7/11.

van Eeden, H. (2004) 'Why UHF RFID Systems Won't Scale', *RFID Journal*: http://www.rfidjournal.com/article/articleview/1056/1/82/ [accessed 6th March, 2015].

Walsh, M. (2013) 'Mobile Payments Still Lack a Clear Winner', www.mediapost.com/publications/article196184/mobile-payments-still-lack-clear-winner [accessed 26th August, 2014].

University *of* Leicester

The Department of Criminology
University of Leicester
154 Upper New Walk, Leicester
LE1 7QH, UK