

# **AUTOMATIC PRODUCT IDENTIFICATION & SHRINKAGE:**

## ***SCOPING THE POTENTIAL***

**A WHITE PAPER FOR ECR EUROPE**

**BY**

**ADRIAN BECK**

**SCARMAN CENTRE, UNIVERSITY OF LEICESTER, UK**



**AUTOMATIC PRODUCT IDENTIFICATION & SHRINKAGE:  
*SCOPING THE POTENTIAL***

All rights reserved.

ECR Europe holds copyright of this report. It may not be reproduced without the prior written permission of ECR Europe.

The comments expressed in this report are of those of the author and do not necessarily represent the views of ECR Europe. The author would like to express his thanks to the ECR Shrinkage Committee, in particular Paul Chapman from the Cranfield School of Management, Colin Peacock from Gillette, Alistair McArthur from Allied Domecq, Katrin Recke from the European Brands Association (AIM), and also Charlotte Bilby from the University of Leicester, who all gave valuable feedback on early versions of this document.

*To contact ECR:*

Efficient Consumer Response (ECR)  
AIM, 9 Avenue des Gaulois  
1040 Brussels  
Belgium

*To contact the author:*

Adrian Beck, Lecturer in Security Management,  
University of Leicester, Scarman Centre,  
154 Upper New Walk, Leicester LE1 7QR UK  
*Email: bna@le.ac.uk*

***July 2002***

Copyright © ECR Europe

# Contents

<b>Introduction</b> .....	1
<b>Developments in Product Identification and RFID</b> .....	2
<i>What is Radio Frequency Identification?</i> .....	3
The RFID Tag .....	3
The Reader .....	4
The Management System .....	4
<i>The Perceived General Benefits of RFID</i> .....	5
<i>The Auto ID Centre</i> .....	5
<i>Global Commerce Initiative</i> .....	6
GCI-ITAG .....	7
<i>GTAG</i> .....	7
<i>Defining Auto ID</i> .....	8
<b>The Problem of Shrinkage</b> .....	10
<i>Defining Shrinkage</i> .....	11
<i>Size of the Problem</i> .....	12
<i>Non-Malicious Shrinkage</i> .....	15
Process Failures .....	15
<i>Malicious Shrinkage</i> .....	17
Understanding Theft .....	17
Temptation .....	19
Motivation .....	19
Opportunity .....	20
Risks and Consequences .....	21
Professional and Opportunist Thieves .....	22
Crime Prevention in Retailing .....	23
Internal Theft .....	23
External Theft .....	26
Supplier Fraud .....	27
Responding to Malicious Shrinkage: Lessons to Date .....	28
<b>Problems of Managing Stock Loss</b> .....	29
<i>Unfortunately Necessary</i> .....	29
<i>Juggling Priorities</i> .....	30
<i>Solutions Searching for a Problem</i> .....	30
<i>Living in a 'Data Desert'</i> .....	31

---

<i>In Splendid Isolation</i> .....	32
<i>Myopic Management</i> .....	33
<b>Current Shrinkage Solutions</b> .....	34
<i>Electronic Article Surveillance</i> .....	34
<b>Meeting the Challenges – What Role for Auto ID?</b> .....	38
<i>Process Failures</i> .....	38
<i>Supplier Fraud</i> .....	40
<i>Internal Theft</i> .....	40
Theft by Staff .....	41
Collusion .....	41
Smart Management: Detering Dishonesty in the Workplace .....	42
<i>External Theft</i> .....	42
Intelligent Electronic Article Surveillance (IEAS)? .....	42
Dynamic Hot Product Lists .....	43
Sweep Thefts .....	44
Tag Visibility and Deterrence .....	44
Removing Tags .....	45
Returning Stolen Goods .....	46
<i>Developing an Information-Led Strategic Approach to Shrinkage Management</i> .....	47
A New Role for Stock Loss Managers .....	48
<i>Indirect Shrinkage</i> .....	49
<i>Prospects, Panaceas and Practicalities</i> .....	50
<b>Next Steps: Setting the Research Agenda</b> .....	52

## **Introduction**

The purpose of this paper is to explore the possibilities offered by recent developments within the sphere of product Auto Identification (Auto ID) technologies to impact upon the problem of shrinkage in the retail sector and their suppliers (both manufacturers and third-party logistics providers). Its purpose is not to provide specific strategies for its implementation, but to consider the potential to impact upon shrinkage in the short, medium and long term. In this respect, this document aims to generate discussion, debate and above all, raise questions about how this rapidly developing technology might be used, rather than to be overtly prescriptive in suggesting how it should be used.

The research was commissioned by Efficient Consumer Response Europe (ECR) and uses as its base a series of in-depth discussions with European retailers and manufacturers, technology providers and developers, standards agencies and academics. In particular, a one-day workshop was organised in February 2002, in Brussels, when invited delegates were offered the opportunity to discuss in detail the prospects, problems and potential of Auto ID. The author is extremely grateful to all those who contributed their time, expertise and knowledge to assist in this research. In particular, the staff at the Auto ID Centre in Boston (US) and Cambridge (UK), and the members of the ECR Europe Shrinkage committee.

The paper begins by looking at recent developments in radio frequency identification and tagging technologies, as well as the existing and, in some instances, well-established forms of product identification. It then goes on to chart the problems of shrinkage and the difficulties associated with tackling it. Without a clear understanding of the problems of shrinkage and shrinkage management, it is impossible to begin to identify the prospects offered by Auto ID. It continues with a review of some of the technological approaches currently adopted to tackle shrinkage, in particular the application of Electronic Article Surveillance (EAS). It then goes

on to look at specific ways in which it may be used to tackle some of the problems outlined in the previous sections. It concludes by assessing the overall issues relating to the implementation and eventual use of Auto ID in the business community.

## **Developments in Product Identification and RFID**

Putting tags on items in order to either ‘learn’ something about them or enable them to ‘interact’ in some way with other ‘things’ is nothing new<sup>1</sup>. Electronic article surveillance tags have been around for about 40 years and have been used primarily by the retail sector to try and counter the problem of shoplifting. Other systems have also been developed, most notably the Article Number and the barcode that have revolutionised the identification of products in the supply chain<sup>2</sup>. Through the Uniform Code Council (UCC) and the International Article Numbering Association (EAN International), barcodes have become a universally accepted standard and also a ubiquitous part of product packaging. The UPC enables types of products to be identified optically and for these products to be linked to databases that provide further information about them, primarily their price. UPC has had a major impact upon the commercial world through the degree of global consensus it has required and achieved. It is estimated that the bar code business is now worth between \$5 and \$10 billion a year<sup>3</sup>, with as many as 5 billion bar codes being scanned daily<sup>4</sup>

---

<sup>1</sup> The device used to identify a product has been coined a ‘taggant’ – this can be anything from an electronic chip to a printed bar code. The key aspect is that it enables the product to be linked to an identification number (which may not always be unique) and then onwards to databases providing further information on the item.

<sup>2</sup> Haberman A, (2000) (Ed) *A Life Behind Bars*. Cambridge, Massachusetts: Harvard University.

<sup>3</sup> IDTechEx Limited (2002) ‘The Structure of the RFID Industry’, *Smart Label Analyst*, Issue 15, April.

<sup>4</sup> IDTechEx Limited (2002) ‘How to Make a 5 Cent Tag’, *Smart Label Analyst*, Issue 15, April.

However, what the current barcode system does not do is identify each product uniquely – one bottle of shampoo is not distinguishable from another. It also relies upon line-of-sight to gather the information and the consequent human intervention to normally achieve this. These and other limitations have led to developments in Radio Frequency Identification and the associated technologies relating to the means of carrying data (tags).

## **What is Radio Frequency Identification?**

Like a bar code, a Radio Frequency tag is a data carrier. While a bar code carries data in a visible symbol and is read at optical or infrared wavelengths, an RFID device (or tag) carries data programmed into a chip and operates at radio frequencies, typically 125 KHz, 13.56 MHz, 2.45GHz and around 900MHz.

All RFID systems have three main components:

- *The RFID tag with its own data, functions and physical characteristics.*
- *The reader with its own functions and physical characteristics.*
- *The management system with its own hard and software.*

### ***The RFID Tag***

Broadly speaking, all tags comprise a semi-conductor chip with memory processing capability and a transmitter connected to an antenna (aerial). The amount of memory can vary with simple tags having a small amount of fixed memory (usually 64-128 bytes) and more complex tags with a capacity up to a few kilobytes. This memory can be configured to be read only (RO), write once, read many times (WORM), or read/write (RW).

RFID tags take many different shapes depending on the application and the technology. Thin tags are known as smart labels to differentiate them from the bulkier ones that are more commonly used for applications such as on animals or vehicles. Some tags have onboard batteries to increase range, and are known as active tags. These tags are more expensive and

only used for specific applications. The great majority of tags used within the retail environment are passive, taking their energy from the electromagnetic field emitted by readers.

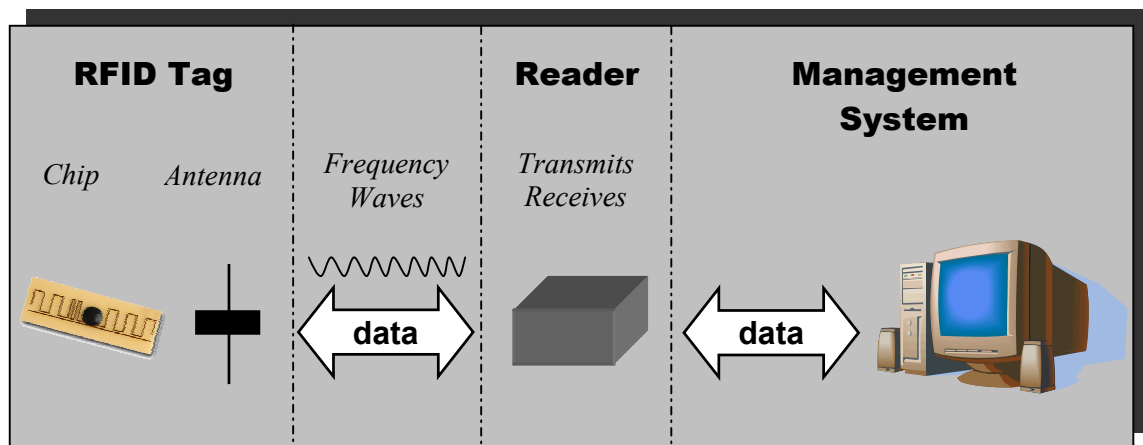
***The Reader***

The reader comprises an antenna and a controller. The controller codes, decodes, checks and stores the data, manages communications with the tags and communicates with the management system. Strictly speaking a ‘reader’ only reads data from the tags whereas an ‘interrogator’ reads data from the tags and writes data to them.

***The Management System***

The management system of RFID is the nerve centre for the application and forms part of the RFID user’s information technology system. It is responsible for using the data received from and sent to the RFID tags for logistics and commercial management. For communications to begin between a reader and a tag the reader must first recognise that tags are present in its ‘field’; it must then be able to recognise each and every relevant tag in its field. Readers are also capable of reading all or only relevant parts of the data depending on how the system is programmed.

**Figure 1 Radio Frequency Identification**





## **The Perceived General Benefits of RFID**

As RFID systems use radio waves, they can do things that optical technology cannot do, including:

*Line of sight:* you do not have to be able to see a tag to be able to read it; a tag must merely pass through the electromagnetic field emitted by the reader.

*Range:* tags can be read at very long range – many hundreds of metres in the case of very specialised tags. RFID devices used in mass logistic applications are thought to need a range of around 1 to 5 metres.

*Bulk read:* many tags can be read in a short space of time. For example the GTAG specification (see below) is designed to read 250 tags in less than three seconds.

*Selectivity:* potentially, specific data can be read from a tag, such as the temperature a product has been stored at.

*Durability:* tags can be hidden from the weather or placed in a plastic casing.

*Read/write (RW):* RFID tags can be updated after the original data has been loaded. This might be a simple change in status: ‘paid for’/‘not paid for’ in the case of a tag used in conjunction with retail electronic article surveillance (EAS). It could however, involve much more complex data such as warranty and service history in the case of, for instance, a car or microwave oven.

## **The Auto ID Centre**

The Auto-ID Centre founded at the Massachusetts Institute of Technology (MIT) in 1999 is a global, industry funded research programme tasked with developing the ‘ultimate solution’ for RFID: an ultra low cost, open standard system that can be used for any application on any physical object, including low priced consumables such as grocery items. The Auto-ID Centre mission is to ‘merge the physical world with the information world to form a single, seamless network, using the latest technology developments embracing electro-magnetic identification, computer modelling and networking’<sup>5</sup>. The Centre is working in collaboration with the global standards bodies and the auto-ID industry to help specify how items will communicate in a standard environment. The technologies currently being developed include:

---

<sup>5</sup> [http://www.autoidcenter.org/home\\_vision.asp](http://www.autoidcenter.org/home_vision.asp).

*Electronic Product Code (ePC)*: a numbering system that can provide unique identification for physical object assemblies and systems. The ePC acts simply as a number providing a pointer or address to information held in databases sitting on local networks or the Internet. The ePC has two parameters in its design. First, the number of bits necessary to provide unique identity for any product in the global supply chain. Secondly, bit partitioning to speed up the search routine.

*Product Mark-up Language (PML)*: a standard language for describing physical objects, based on the extensible Mark-up Language XML. PML is being designed to allow the distributed management of product information at central locations such as a factory warehouse or store.

*Object Naming Service (ONS)*: a service that tells computer systems where to locate information on the Internet about any object that carries an ePC<sup>6</sup>.

## **Global Commerce Initiative**

The Global Commerce Initiative (GCI) is a voluntary body created in October 1999 to improve the performance of the international supply chain for consumer goods through the collaborative development and endorsement of recommended standards and key business processes<sup>7</sup>. GCI is a global user group, but not a standards body. It sees its role as facilitating and encouraging the best possible input on business processes and standards so that existing standards bodies can work internationally with confidence. EAN International and UCC support and enable the work of GCI to better manage the development of standards around the world.

GCI operates a number of working groups to look at issues relevant to their overarching objectives. Included in this is the GCI-ITAG Working Group (Global Commerce Initiative-Intelligent Tagging Working Group).

---

<sup>6</sup> Brock, D. L. (2001) 'The Electronic Product Code – A Naming Scheme for Physical Objects', *Auto-ID White Paper*, WH-002, January; Brock, D. L. (2001) 'The Physical Markup Language – A Universal Language for Physical Objects', *Auto-ID White Paper*, WH-003, February.

<sup>7</sup> The Sponsors are: AIM - European Brands Association, CIES - Food Business Forum; EAN International; ECR - Efficient Consumer Response; FMI - Food Marketing Institute; GMA - Grocery Manufacturers of America; UCC - Uniform Code Council Inc.; VICS - Voluntary Interindustry Commerce Standards.

## **GCI-ITAG**

This working group was established to provide ‘an assessment and evaluation of the functions involved with the supply chain dynamics that would benefit from the implementation of radio based solutions’<sup>8</sup>. The group set out to consider three types of RFID application: Generic, Sectoral and Advanced. Generic referred to those applications that are common to all organisations (retailers, logistics providers and manufacturers); the bar code would be an example of this where anybody with the right IT, telecommunications and equipment can make use of it. Sectoral applications apply to those systems that are either tailored to the particular needs of a user or group of users. Examples would be closed loop applications (tracking returnable containers), road toll systems and livestock tracking. Advanced applications refer to those developments that have yet to fully emerge but may provide significant efficiency gains primarily through redundancy of the need for line of sight reading (essentially replacing the bar code). To date, the group has produced an excellent working paper on the first of these three areas (the GCI Intelligent Tagging Model: An Examination of Product and Supply Chain Opportunities) and a recent white paper on the future role of RFID<sup>9</sup>.

## **GTAG**

GTAG, which is an acronym for ‘Global Tag’, is an international standardisation initiative that is jointly sponsored by the Uniform Code Council and EAN International<sup>10</sup>. It is closely aligned with the work of the International Organisation for Standardisation (ISO) and with the initiatives being developed by the Auto ID Centre (see above). The initiative is in the process

---

<sup>8</sup> GCI Intelligent Tagging Working Group (2001) *The GCI Intelligent Tagging Model, An Examination of Product and Supply Chain Opportunities*, [http://www.globalcommerceinitiative.org/oas/gcis/gci.www\\_main.main?p\\_language=us&p\\_cornerid=10000&p\\_currcornerid=1&p\\_full=1](http://www.globalcommerceinitiative.org/oas/gcis/gci.www_main.main?p_language=us&p_cornerid=10000&p_currcornerid=1&p_full=1).

<sup>9</sup> GCI Intelligent Tagging Working Group (2001) op cit; GCI Intelligent Tagging Working Group (2002) *Intelligent Tagging – White Paper (Vision, Business Requirements, Concepts, Standards, Recommendations)*, [http://www.globalcommerceinitiative.org/oas/gcis/gci.www\\_main.main?p\\_language=us&p\\_cornerid=10000&p\\_currcornerid=1&p\\_full=1](http://www.globalcommerceinitiative.org/oas/gcis/gci.www_main.main?p_language=us&p_cornerid=10000&p_currcornerid=1&p_full=1).

<sup>10</sup> [www.ean-ucc.org/gtag.html](http://www.ean-ucc.org/gtag.html).

of creating a set of technical specifications that address a class of RFID systems whose properties are most suitable to be used in logistic applications such as asset management and returnable transport items<sup>11</sup>. It is hoped that technology providers will follow these standards when developing new systems (GTAG compliant tags for instance) therefore reducing the risk of independent technologies being unable to communicate in open environments. Recent developments have seen some of the major technology providers aligning their standards with those of GTAG on critical issues such as air interface and collision-avoidance mechanisms (the way tags communicate with readers)<sup>12</sup>.

## **Defining Auto ID**

Both the Auto ID Centre and the work of the GCI sub committee on RFID are not without their critics. Some see the vision of the ‘tagged world’ as both unrealistic and unnecessary – the technological steps necessary and the degree of collaboration required are formidable, and many of the problems it is designed to address can already be effectively tackled with existing technologies and better management systems<sup>13</sup>.

This paper does not intend to enter this debate. Its purpose is to take a vision of where all things (be they pallets, cases or items) have an RFID tag attached, and that these tags are capable of being effectively tracked along the entire supply chain<sup>14</sup> (through the use of widely distributed readers), and the resultant information is then capable of being analysed in real or near real time. The term used to describe this system in this paper will be ‘Auto ID’. It does

---

<sup>11</sup> For instance the GTAG Project Team has developed a set of minimum protocol & performance requirements (MP&PR) for technology providers to follow.

<sup>12</sup> [www.uc-council.org/news/ne\\_020702.html](http://www.uc-council.org/news/ne_020702.html).

<sup>13</sup> Some argue that the developments in symbology such as two-dimensional and linear barcodes offer significant advantages in the short and medium term and are less costly and disruptive, particularly to manufacturers. There are also many other concerns about the impact such a system may have on a range of other issues, not least the environment, recycling and the privacy of those who come into contact with tagged items.

<sup>14</sup> In this context, the supply chain is considered to be from the point of production, through transportation and warehousing, on to the retail outlet and reverse logistics (in the case of goods being returned). It also includes those items that enter the supply chain illegally (counterfeit) and leave the supply chain prematurely (for instance for sale in the ‘non-retail’ market).

recognise that there are many potential benefits to organisations from this technology<sup>15</sup> and that there may be considerable overlap between them, but the emphasis of this paper will be its impact as it relates to the problems of shrinkage only (see definition below).

---

<sup>15</sup> A whole host of potential uses have been identified, including: soft sensing of product freshness; faster product recalls; streamlined supply chains; improved compliance checking; interaction warnings; easier logistics for custom products; automatic recall; medication validation; tracking of bank notes etc.

## **The Problem of Shrinkage**

The rather euphemistic term ‘shrinkage’ is used by the business world to describe the losses that occur while they attempt to complete the deceptively simple task of producing, distributing and eventually selling goods to consumers. The term covers an enormous gamut of events, which can for the most part be broken down into two types: malicious and non-malicious. Malicious events represent those activities that are carried out to intentionally divest an organisation of goods, cash, services and ultimately profit. Non-malicious events occur within and between organisations that unintentionally cause loss, through poor processes, mistakes, bad design and so on. Like the former, this has a dramatic impact upon the profitability of an organisation.

The importance of perceiving the intentionality of a shrinkage occurrence is the impact it has upon the approach adopted to tackle it. As the word implies, intentional presumes deliberateness and a degree of forethought. It also presumes to a certain extent that existing systems have been found to be vulnerable – sometimes by accident, often by ‘probing’ – and duly ‘defeated’ by the offender. As such, remedial action to deal with some types of malicious activity will have a shelf life or period of effectiveness that deteriorates as offenders find new ways to overcome them. It could also lead to displacement – offenders target different products, locations, times or methods<sup>16</sup>. On the other hand, unintentional shrinkage is usually less dynamic and more susceptible to lasting ameliorative actions. While they may require similar levels of vigilance (for instance to make sure staff are continuing to follow

---

<sup>16</sup> Clarke, R.V. (1995) ‘Opportunity-Reducing Crime Prevention Strategies and the Role of Motivation’, in P. Wilkstrom, R.V. Clarke, and J. McCord (Eds.) *Integrating Crime Prevention Strategies: Propensity and Opportunity*, Stockholm: National Council for Crime Prevention; Clarke, R.V. (1997) *Situational Crime Prevention: Successful Case Studies*, Albany, NY: Harrow and Heston.

procedures) they are less liable to be anything like as evolutionary in nature as their malicious counterparts.

The purpose of this section is to consider in detail the topography of shrinkage and how it affects retailers, logistics providers and manufacturers. Without a very clear understanding of the threat presented by shrinkage, it is impossible to fully understand how Auto ID technologies may be used to address it.

## **Defining Shrinkage**

Opinions vary on a definition for shrinkage. Some take a very narrow perspective and limit it to the loss of stock only, choosing to exclude the loss of cash from an organisation, or consider it to relate only to the losses that cannot be explained – ‘unknown losses’ as they are usually referred to<sup>17</sup>. At the other end of the spectrum, some argue for a much more inclusive, broad ranging definition which encompasses both stock and cash, as well as the losses that result from shrinkage events – ‘indirect losses’ – such as out of stocks<sup>18</sup> caused by shop theft, the sale of stolen goods on the ‘non-retail’ market<sup>19</sup> or the production of counterfeit products. In addition, some feel that the expenditure incurred responding to stock loss should also be included in the overall cost of shrinkage.

The recent work by the ECR Europe Shrinkage committee has developed a definition that has received relatively broad acceptance, which strikes a middle ground between the two, driven in part by the current limitations imposed upon the ability to accurately measure the impact of shrinkage upon organisations. It is based upon four categories of shrinkage encompassing both stock and cash and made up of supplier fraud, internal theft, external theft and process

---

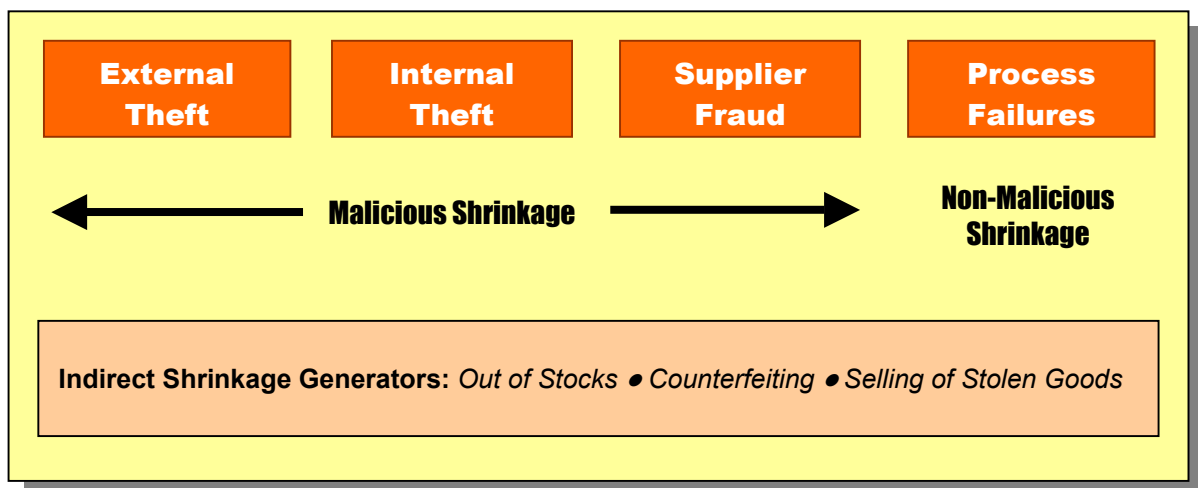
<sup>17</sup> Masuda, B. (1992) ‘Displacement vs Diffusion of Benefits and the Reduction of Inventory Losses in a Retail Environment’, *Security Journal*, Vol. 3, No. 3, pp. 131-136.

<sup>18</sup> One study has suggested that between 7 to 10 per cent of product may be out of stock at any one time, ECR Europe (2002) *Optimal Shelf Availability*, Brussels: ECR Europe, forthcoming.

<sup>19</sup> Such as car boot sales or flea markets.

failures. The first three can be regarded as malicious and intentional, while the fourth is non-malicious and an unintentional, but highly regrettable consequence of ineffective business processes, procedures and activities. This paper intends, for the most part, to use this definition, although it will argue later that one of the prospective benefits of Auto ID is to enable organisations to begin to address issues that have been seen as beyond the traditional boundaries of shrinkage management, such as some of the indirect loss events outlined above. In this respect Auto ID could have a significant impact upon the way shrinkage is defined in the future.

**Figure 2 Defining Shrinkage**



## Size of the Problem

Recent research has once again demonstrated the extent of the problem of shrinkage for retailers and their suppliers throughout the world. In 2001, research sponsored by ECR Europe on behalf the Fast Moving Consumer Goods sector (FMCG)<sup>20</sup> calculated that the

---

<sup>20</sup> The term Fast Moving Consumer Goods Sector is used here to mean those retailers and their suppliers who provide a range of goods sold primarily through supermarkets, and hypermarkets. The core of their business is providing 'essentials' such as various fresh and processed foodstuffs, but they also stock a wide selection of other goods as well including health and beauty products, tobacco, alcohol, clothing, some electrical items, baby products and more general household items. Examples of FMCG retailers include Auchen, Carrefour, Coop Italia, ICA, Interspar, Tesco and Walmart. Examples of FMCG manufacturers include Allied Domecq, Gillette, Johnson and Johnson, Procter & Gamble and Unilever. In the USA, this sector is also referred to as the Consumer Packaged Goods sector.



annual bill for shrinkage was €18 billion, based upon an annual turnover of €824.4 billion<sup>21</sup>. This equated to 2.31 per cent of turnover – 1.75 per cent for retailers and 0.56 per cent for manufacturers<sup>22</sup>. A similar study in Australasia, using the same methodology found that losses from shrinkage accounted for 1.73 per cent, and amounted to \$A942 million<sup>23</sup>. In the USA, work by Hollinger has estimated that shrinkage costs the retail sector \$30 billion a year or one-quarter of annual retail profits<sup>24</sup>. In some respects, there is nothing new about attempting to quantify the overall cost of stock loss<sup>25</sup> to the business world; the annual British Retail Consortium retail crime surveys provide a detailed breakdown on the extent and cost of the problem of crime against retailers in the UK, while similar initiatives in other European countries have tried to measure the problem as well<sup>26</sup>.

While the definition of what constitutes ‘shrinkage’ or ‘stock loss’ varies between the studies and undoubtedly has an impact upon the overall size of the loss figure, the overriding conclusion is that the extent of the problem is enormous, and that it is an issue which seems for the most part, extremely resilient to ameliorative actions. As one trading director recently put it: ‘We have had the same problem for 25 years – it doesn’t get any better, it only seems to get worse’<sup>27</sup>.

---

<sup>21</sup> M+M Euro Trade (2000) *Trade Structures and the Top Retailers in the European Food Business*, Frankfurt: M+M Euro Trade.

<sup>22</sup> Beck, A., Bilby, C. and Chapman, P. (2002) ‘Shrinkage in Europe: Stock Loss in the Fast Moving Consumer Goods Sector’, *Security Journal*, forthcoming; Beck, A., Bilby, C., Chapman, P. and Harrison, A. (2001) *Shrinkage: Introducing a Collaborative Approach to Reducing Stock Loss in the Supply Chain*, ECR Europe: Brussels.

<sup>23</sup> ECR Australasia. (2002) *A Guide to Collaborative Loss Prevention*, Australia: ECR Australasia.

<sup>24</sup> Hollinger, R. and Hayes, R. (2000) *National Retail Security Survey*, Gainesville, FL: University of Florida.

<sup>25</sup> The terms ‘shrinkage’ and ‘stock loss’ will be used interchangeably throughout this paper.

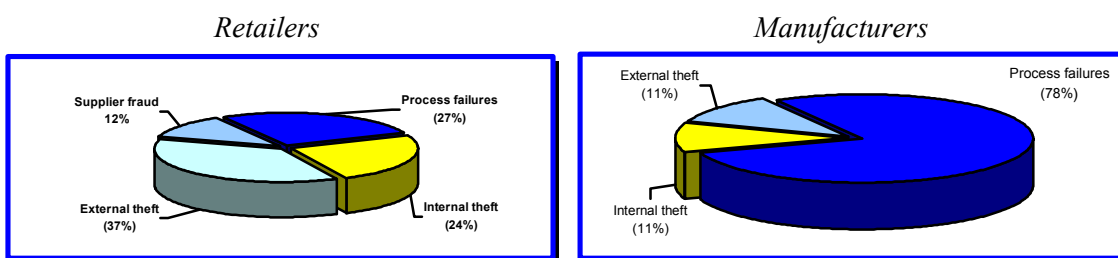
<sup>26</sup> In the UK see the annual reports by the British Retail Consortium on the costs of crime to the retail sector; and Mirrlees-Black, C. and Ross, A. (1995) *Crime Against Retail and Manufacturing Premises: Findings from the 1994 Commercial Victimization Survey*, Research Study Number 146, London: Home Office. In Germany see EuroHandelsinstitut (2000) *Inventurdifferenzen 2000: Ergebnisse einer aktuellen Erhebung*, Cologne: EuroHandelsinstitut; For data on theft only from European Retailers see Bamfield, J. (2002) *The European Retail Theft Barometer*, Nottingham: Centre for Retail Research.

<sup>27</sup> This comment was made by a senior executive (who wishes to remain anonymous) for one of the UK’s largest food retailers.

Trying to gather accurate data on the magnitude of different types of shrinkage has proved beyond current methodologies designed to measure the problem. This is because for retailers, the majority of losses remain unknown – losses are discovered after the event, usually through annual or biannual stock audits, making it impossible to answer the critical questions of what caused the loss, where did it happen and when. In the recent ECR survey, 59 per cent of retailer losses were unknown, while for manufacturers, the comparable figure was 41 per cent.

Given the lack of information linking losses to particular causes, most shrinkage measurement methodologies rely upon respondents ‘using their knowledge and experience to estimate what the breakdown between each type of loss might be’<sup>28</sup>. Clearly this moves any estimates of the causes of stock loss from the realms of hard data, usually provable and based upon evidence, to ‘soft’ data, something that is not based entirely upon fact but reliant upon impressions, opinions and personal bias. This is an issue that this paper will return to below when managing shrinkage is considered. However, given this significant problem in determining the causes of stock loss, the 2001 ECR study found that retailers and manufacturers allotted significantly different weight to the different categories of loss (Figure 3).

**Figure 3 Perceived Causes of Stock Loss in the European FMCG Sector**



For retail respondents, external theft was perceived as the main cause of stock loss (37%), followed by process failures (27%), internal theft (24%) and finally supplier fraud, which was

---

<sup>28</sup> This example is taken from the ECR Europe shrinkage questionnaire that was distributed to retailers and manufacturers in 2000.

thought to make up 12 per cent of all shrinkage losses. Taken together, theft was considered to account for nearly two thirds of all losses (61%) or €8 billion. In contrast, manufacturers identified process failures as the biggest culprit – 78 per cent of all losses. Both internal and external theft were thought to equally account for the remaining 22 per cent (11% each), although this still equates to €1 billion of losses due to malicious activities.

The differences between the two are very stark – retailers do not see any one cause as dominating their thinking – all four factors receive between 12 and 37 per cent of the total, while manufacturers believe that process failures dominate their stock loss problem.

## **Non-Malicious Shrinkage**

### *Process Failures*

It is difficult not to underestimate the complexity of modern retailing and the globalisation of product manufacture and distribution. Consumers have become accustomed to having ready and almost continual access to products that originated many thousands of miles away from the eventual point of sale. In food retailing, seasonality now has little impact on availability as sophisticated and complex supply chains source products from around the globe. In addition, consumers have become more demanding in the quality and range of products they expect in their retail environment. Hence supermarkets regularly stock in excess of 20,000 SKUs<sup>29</sup> while clothes retailers will regularly change most of their stock to meet the vagaries of rapidly changing popular fashion. Arguably, all of this has made companies more profitable and given consumers an unprecedented shopping experience<sup>30</sup>. But this complex global production, distribution and retailing web comes at a price – that of organisational inefficiency in managing the myriad of processes required to make the system work.

---

<sup>29</sup> There are some companies that stock far more, such as Walmart that has an estimated 120,000 SKUs.

<sup>30</sup> Some may argue that the globalisation of manufacturing and retailing has had a detrimental effect upon local economies and helped to fuel a growing 'wealth gap' between the developing and developed worlds.

Getting the right products to the right place, in the right condition at the right time and price, and linked to the right information, is the goal of modern retailing, but when this fails, it generates losses, which are defined as process failures or ‘Paper Shrink’<sup>31</sup>.

The 2001 ECR survey found that for retailers, process failures accounted for 27 per cent of all losses or €3.6 billion a year. For their suppliers, the percentage was much higher – 78 per cent, but accounted for the same amount – €3.6 billion. Taken together, in Europe’s Fast Moving Consumer Goods sector, process failures cost €7.2 billion a year, or €19 million a day. In the US, it has been estimated that for every \$100 of shrinkage, \$17.50 could be due to process failures<sup>32</sup>. This is a significant price to pay for organisations not getting it right.

The recent workshop on RFID and shrinkage and other research has identified the key elements that contribute to process failures (paper shrink). They are:

*Stock going out of date:* product not being sold in time because too much was ordered; it was not discounted in time; or stock was not rotated properly.

*Price reductions:* stock being sold below the price originally envisaged; too much was ordered; stock had not been rotated properly; or expected sales targets had been overly ambitious.

*Damage to stock:* caused by the methods used to store and distribute products. This can include temperature sensitive produce such as foods.

*Delivery errors:* a combination of the wrong products being delivered to the wrong places at the wrong times. This can include the failure to record products transferred between stores.

*Pricing errors:* the incorrect pricing of product, either below the planned price or incorrectly discounted in connection with product promotions.

*Scanning errors:* store staff incorrectly scanning products on the shelves causing errors in the inventory; checkout staff forgetting to scan products; or incorrectly entering the product identification code.

---

<sup>31</sup> See Sullivan, M and Vince, C. (2001) ‘How Much are you Losing to Paper Shrink?’ *Retail Insights*, Vol. 10, No. 5.

<sup>32</sup> Ibid.

*Incorrect inventory checks:* staff mis-counting product in the warehouse, in the storeroom or on the shelves, causing errors in the expected and actual levels of stock.

*Product promotion errors:* products being sold at promotional prices when they should not be; associated products being sold at discounted prices when they should not be; or incorrect multi-buy discounts being applied.

*Master file errors:* incorrect entry of product type or quantities on the master inventory file. This can lead to companies thinking that they have more or less of a particular product than is currently in the supply chain.

*Returns:* products that have been legitimately returned by customers not re-entering the supply chain correctly.

*Intra-company transfers:* products being misplaced as they move between different parts of the organisation, such as between different retail stores.

Common to most process failures is that they are a consequence of two related types of failure: a failure to *collect* and a failure to *communicate* information accurately and timely about the products currently within the supply chain. They are a failure to answer two simple questions: ‘what products do we have?’ ‘and where are they?’ Answers to these questions then enable the key questions of ‘what products do we need?’, ‘where do we need them to be?’ and ‘what price should we be charging for them?’ to be answered.

## **Malicious Shrinkage**

### ***Understanding Theft***

Organisations can be the victims of theft carried out by both the staff they employ (internal theft) and from outsiders targeting their assets (external theft). The extent to which internal and external theft accounts for shrinkage is very much open to speculation, but in order to assess the potential role of Auto ID to tackle this problem, it is important to first of all understand the context of theft from organisations. Criminological research suggests that three

key elements need to be present in order for an offence to be committed: a likely or motivated offender, a suitable target and the absence of a capable guardian<sup>33</sup>.

**Figure 4 Factors Required For an Offence to Take Place**

$$\text{Offence} = \text{Motivated Offender} + \text{Suitable Target} + \text{Absence of Guardian}$$

For example, within a retail environment, the motivated offender could be a shoplifter, the suitable target could be a 'hot product' such as alcohol or tobacco, and the absence of a guardian could be the lack of a store guard, or indeed various forms of technology such as closed circuit television or electronic article surveillance equipment. The key to reducing offending is to remove one or more of these factors from the 'offending equation'.

In addition, there are a number of factors that act upon the offenders decision-making thought processes, which can be broken down into five areas: temptation; motivation; opportunity; risks and consequences (Figure 5).

**Figure 5 Factors Likely to Influence Decision to Offend**



<sup>33</sup> Felson, M. (1996) 'Preventing Retail Theft: An Application of Environmental Criminology', *Security Journal*, Vol. 7, pp. 71-75.

Each of these factors can have a negative, neutral or positive effect on the risk of offending. They can also work in isolation or in combination depending upon the circumstances surrounding the offender.

### *Temptation*

In retailing, staff and customers are in an environment whereby they are constantly surrounded by valuable and desirable products and where staff often have to deal with relatively large amounts of cash. This inevitably leads to staff and customers being tempted. Two components of temptation that may trigger theft are greed and need (or perceived need).

### *Motivation*

Motivation is an important factor in affecting the likelihood to offend. There are three parts which need to be considered: acceptability, neutralisation (or excuses) and marginalisation. Acceptability is associated with whether the dishonest act is perceived by the offender to be wrong. For instance, if staff do not consider particular practices to be dishonest, or they see managers or supervisors behaving in a dishonest manner, such as eating stock on display, then this can legitimise the act. Offenders may utilise a form of neutralisation whereby the theft of goods or money is considered to be victimless and hence nobody really suffers. Thieves who commit crimes because of this often excuse their act by using explanations such as ‘well the company can afford it’.

Finally, marginalisation within the company may have a role to play in explaining why some staff become dishonest. Staff who are on short-term or part-time contracts, or see no obvious path of promotion may consider themselves ‘temporary’ employees within the work environment and hence perceive themselves to have less to lose if they are caught committing dishonest acts. Those most frequently caught for staff theft include young, part-time employees who have been with the company for a relatively short time and do not see

themselves staying with the organisation for very long<sup>34</sup>. It may be the case that it is how they perceive their position within the company that is the critical variable in explaining their likelihood to become dishonest.

### *Opportunity*

Opportunity is of critical importance and is based upon three significant factors: space, time and position. Space is associated with opportunities provided by particular parts of the store – a survey of retail staff found that a majority identified ‘backroom’ areas as offering an ideal opportunity to steal goods, primarily because staff were often on their own<sup>35</sup>. Similarly, managers legitimately enter all parts of the store without necessarily raising suspicion. For external thieves, ‘blind spots’ within stores, such as behind pillars or areas that are not readily observable by staff or CCTV can provide opportunities for theft<sup>36</sup>. Time is also an important factor of opportunity. If particular members of staff work at times when either there are lower levels of supervision or there are very few or no other staff present (such as night shifts), then their opportunity to steal is higher. In addition, shoplifters may choose times when they know a retail store has very few staff working, or when the store is particularly busy (other shoppers providing ‘cover’ for their offending). Finally, position or role in the company can provide staff with the opportunity to commit crime. Positions of responsibility and or specialisation can offer staff the opportunity to be dishonest (for instance buyers or IT staff).

---

<sup>34</sup> See Beck, A. and Willis, A. (1991) *Security in Woolworths: A Profile of Staff Dishonesty*, Leicester: CSPO, University of Leicester; Beck, A. and Willis, A. (1993) ‘Employee Theft: A Profile of Staff Dishonesty in the Retail Sector’, *Journal of Asset Protection & Financial Crime*, Vol. 1, May, pp. 45-57; Beck, A. and Willis, A. (1995) ‘Enemy Within’, *Security Management Today*, Vol 4, No. 9, pp. 16-17.

<sup>35</sup> Ibid.

<sup>36</sup> Beck, A. and Willis, A. (1992) *Store Design & Security: An Analysis of Shoplifting by Product Type and Location*, Leicester: CSPO, University of Leicester; Beck, A. and Willis, A. (1998) ‘Sales and Security: Striking the Balance’, Gill, M. (Ed.) *Crime at Work: Increasing the Risk for Offenders*, Vol 2, Leicester: Perpetuity Press, pp. 95-107.



### *Risks and Consequences*

Sanctions or disincentives to commit crime can influence the likelihood to offend. These are the perceived chances of being caught and the consequences of any subsequent punishment. If offenders consider the risk of being caught as low, then this may act positively to encourage dishonesty. Similarly, if the punishment is relatively lenient, then again this may act positively on encouraging theft. Alternatively, if potential offenders consider themselves at significant risk of being caught and appreciate that the punishment will be severe (loss of job for instance or a criminal record) then this can act as a powerful disincentive. In addition, offenders then need to decide whether the rewards are sufficient and the prospects of being caught low enough to proceed with the offence.

Taken together these variables go some way in explaining the factors that may encourage theft by customers and staff. It is important to remember that these processes can work in isolation and in combination depending on the particular offender and the circumstances surrounding the incident. Indeed, for some offenders there may be powerful factors that act positively to encourage dishonesty while at the same time other factors may act in the opposite direction and in effect cancel each other out.

For example, an organisation could take this model and apply it to their particular context to analyse the likelihood of internal and external theft taking place: what motivation do staff have to steal? Do they have access to discounted stock, is there a staff shop, are they made aware of the impact stock loss has upon an organisation? Similarly, what opportunities are present for offenders? Do certain grades of staff work shifts when levels of supervision are low, is vulnerable stock displayed in areas of low visibility near to readily accessible means of escape, would stock loss be noticed quickly? Finally, are the risks and consequences of offending made clear to staff and customers? Are staff and customers regularly informed of company policies relating to theft, what is the likelihood of dismissed staff finding other work in the area, are frequent shoplifters issued with banning orders?

*Professional and Opportunist Thieves*<sup>37</sup>

Much research has been done on trying to categorise different types of offender and the methods they adopt, with two main types tending to be identified: the ‘professional’ and the ‘opportunist’. Professional thieves are seen as offenders who steal in order to convert stolen products into cash or other items (such as drugs). They generally have good knowledge of the security systems employed by retail companies (they will often visit stores prior to offending to audit the security measures used, such as CCTV, EAS systems, security staff etc<sup>38</sup>), and will seek to identify weaknesses that can be exploited (such as blind spots in the store layout). Research has shown that professional thieves have a high degree of scepticism concerning technology-driven approaches to product protection and often see human intervention as the key factor in deterring them from offending<sup>39</sup>. They are likely to target items that meet the ‘hot products’ criteria of: concealable, removable, available, valuable, enjoyable and disposable<sup>40</sup>, and are more likely to perform multiple item thefts (sweep thefts)<sup>41</sup>. Finally, they are likely to try and overcome current loss protection approaches<sup>42</sup> (such as removing tags or carrying electrical items to ‘explain’ why they have triggered the EAS system, such as garage door opening devices or beepers), work as part of a team, and evolve their methods to meet changes in stock loss protection methods.

---

<sup>37</sup> See Klemke, L. (1992) *The Sociology of Shoplifting: Boosters and Snitches Today*, New York: Praeger.

<sup>38</sup> Weaver, F. and Carroll, J. (1985) ‘Crime Perceptions in a Natural Setting by Expert and Novice Shoplifters’, *Social Psychology Quarterly*, Vol. 48, No. 4, pp. 139-359; Kallis, M. and Vanier, D. (1985) ‘Consumer Shoplifting: Orientations and Deterrents’, *Journal of Criminal Justice*, Vol. 13, pp. 459-473.

<sup>39</sup> Kallis and Vanier (1985) op cit, Hayes, R. (1997) ‘Shop Theft: An Analysis of Apprehended Shoplifters’, *Security Journal*, Vol. 7, pp. 11-14.

<sup>40</sup> Clarke, R.V. (1999) *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods*, Police Research Series Paper, No. 112, London: Home Office.

<sup>41</sup> These are thefts where multiples of the same items are stolen at once, hence the term ‘sweeping product off the shelves or racks’.

<sup>42</sup> Klemke (1992) op cit.; Shapland, J. (1995) ‘Preventing Retail Sector Crimes’, in M. Tonry and D. Farrington (Eds.) *Building a Safer Society: Strategic Approaches to Crime Prevention*, Chicago: The University of Chicago Press.

Unlike their professional counterparts, opportunist shoplifters tend to steal items for their own use or consumption. They are much more impulsive in their decision-making<sup>43</sup> and spend virtually no time planning the offence. They generally have little knowledge of the methods employed by the retailer to counter theft and will target a wide range of merchandise, including those perceived to be hot products. More importantly, they are perceived to be much more likely to be deterred by the overt presence of security measures such as tagging systems, CCTV and security guards.

### *Crime Prevention in Retailing*

The guiding philosophy in dealing with theft from organisations is one of crime prevention – deterring the offender from committing the crime in the first place. Crime prevention works in a number of different ways but for the retailer the key principle is trying to increase the offender perception that the risk of being caught (and subsequently sanctioned) is sufficiently high through the presence of a ‘capable guardian’ to deter them from committing the crime in the first place<sup>44</sup> (see the earlier model on understanding theft, page 18). In other words, the offender’s sense of personal risk of detection, punishment, and humiliation should be compelling enough to overcome their desire and ability to steal<sup>45</sup>. Within the store environment, a capable guardian could be human (guards and store staff) or technological (EAS tags, CCTV).

### *Internal Theft*

The ECR survey estimated that for retailers 24 per cent, and for manufacturers 11 per cent of all losses were due to internal theft, which accounts for just over €3.7 billion of loss each year. Despite this, companies, stock loss practitioners and indeed researchers have continued

---

<sup>43</sup> Ibid.

<sup>44</sup> Baumer, T. and Rosenbaum, D. (1984) *Combating Retail Theft: Programs and Strategies*, Stoneham, MA: Butterworth.

<sup>45</sup> Bamfield, J. (1994) ‘Electronic Article Surveillance: Management Learning in Curbing Theft’, in M. Gill (Ed.) *Crime at Work: Studies in Security and Crime Prevention*, Leicester: Perpetuity Press.

to largely ignore it as an area of concern<sup>46</sup>, choosing to focus more on the other problems affecting the sector, particularly external theft. Why has this tended to happen? There are four key reasons.

First, a lack of reliable, timely and detailed data on stock loss means that incidents of staff theft are rarely recorded compared with other forms of theft. For instance, recorded data on shoplifting is usually dependent on the perpetrator being caught in the act either by security staff or surveillance equipment. Such incidents are far more likely to generate 'known' incidents and hence appear on company crime databases. This then causes 'data reinforcement' whereby only those problems that are recorded are seen as a problem and hence little effort is then made to investigate and subsequently record other data. Therefore an apparent lack of data can lead stock loss managers to perceive that staff theft is not a priority in comparison with other 'better recorded' crimes.

Secondly, there has been a tendency for unknown losses to be apportioned to offenders outside the company. It is often more palatable to blame losses on those who are not part of the store or company 'team'. For instance, unaccounted for losses can be attributed to shoplifters, after all, research has shown that perhaps as few as 1 per cent of all shoplifters are ever caught<sup>47</sup>. It could also be the case that the degree of collusion between staff and shop thieves is underestimated, with the role of the shoplifter being prioritised over the involvement of store staff.

---

<sup>46</sup> See Mars, G. (1982) *Cheats at Work: Anthropology of Workplace Crime*, London: Unwin; Hollinger, R., Greenberg, J. and Scott, K. (1996) 'Why Do Workers Bite the Hands That Feed Them? Employee Theft as a Social Exchange Process', *Research into Organisational Behaviour*, Vol. 1, pp. 111-156; Beck, A. and Willis, A. (1993) op cit; Beck, A. and Willis, A. (1995) op cit; Bamfield, J. (1998) 'A Breach of Trust: Employee Collusion and Theft from Major Retailers', in M. Gill (Ed.) *Crime at Work: Increasing the Risk for Offenders*, Leicester: Perpetuity Press, pp. 123-142.

<sup>47</sup> See Arboleda-Florez, J., Durie, H. and Costello, J. (1977) 'Shoplifting: An Ordinary Crime?' *International Journal of Offender Therapy and Comparative Criminology*, Vol. 21, No. 3, pp. 201-7; Murphy, D. (1986) *Customers and Thieves*, Aldershot: Gower.

Thirdly, by its very nature, staff theft can be a difficult crime to detect and investigate. Staff have to handle cash and products in order that sales can be made. They are put in a position where the company has to give them considerable amounts of autonomy and must trust them to perform their functions honestly. Very often incidents of staff theft only come to light when a member of staff has stolen relatively large amounts of cash or produce, or when other members of staff or security equipment has detected or witnessed the incident. The difficulty in detecting and investigating staff crime leads to security managers opting to focus on other more accessible crimes such as shoplifting, burglaries, credit-card fraud and vandalism. In addition, the potential solutions to these crimes are often more identifiable and easier to target and so it could be that stock loss practitioners target those incidents that are perceived as easiest to solve.

Fourthly, it often been stated that security initiatives designed to target staff theft are often bad for morale, that pointing the finger at staff can lead to a workforce that is poorly motivated and inefficient. It is also argued that investigations into staff theft can be seen as reflecting badly on the image of the company and its managers. After all, it was the managers who recruited and trained the staff who are now stealing from the company, which may reflect badly on the manager's judgement and competence. It can also portray the image of management not being in control of the staff and hence the company. High levels of staff theft may be interpreted by the Board and the shareholders as signs of incompetence. Managers at all levels may perceive it as 'shooting themselves in the foot' if they begin to expose and then try and counter high levels of loss through dishonest staff. It may be better to point the finger at those who work outside the company and hence can be seen as less under the direct control of company management. It could also be the case that a company may prefer to sustain high losses through staff theft than face the consequences of adverse publicity.

Taken together, a lack of data, a tendency for unattributable loss to be apportioned to those outside the store or company team, a realisation that it is often easier to target more

identifiable security problems, a perception that focusing on staff dishonesty may be bad for staff morale and a belief that if high levels of staff dishonesty are uncovered, it may reflect badly on the image of the company and its managers, can all lead to theft from within the company being side-stepped as a major area of concern.

Looking at the specific threats presented by staff, four areas of concern are highlighted below:

*Theft of Stock*: members of staff removing goods from the premises, either by hiding it in their personal belongings, placing them outside the building ready for collection at a later date, or using the internal mail to post it to their home or some other location. This also includes theft by delivery staff, who remove stock from their vehicles.

*'Grazing'*: staff consuming stock while at work.

*Collusion or 'Sweethearting'*: members of staff, often operating the till, colluding with customers to steal products. This is usually done either by staff not scanning items at the check out or mis-scanning (using a code for an item that is cheaper than the one being purchased). It can also include collusion when goods are being returned to the store (possibly stolen in the first place) and with delivery workers, suppliers and contractors.

*Theft of Cash*: members of staff stealing cash from the till or cash office, or short changing customers and pocketing the proceeds.

### ***External Theft***

In stark contrast to internal theft, external theft has for the most part dominated the stock loss agenda. Despite numerous studies showing that it is not the single most significant threat to organisations<sup>48</sup>, it continues to receive the lion's share of stock loss expenditure. Partly this is because of some of the factors outlined in the previous section (in particular the volume of external thieves caught compared to internal thieves), but also because the industry itself is responsible for perpetuating the 'myth', enthusiastically assisted by security service providers

---

<sup>48</sup> Buckle, A. and Farrington, D. (1984) 'An Observational Study of Shoplifting', *British Journal of Criminology*, Vol. 24, No. 1, pp. 63-73.

who play a significant part in setting the agenda and promising quick fix technological panaceas.

There are five main threats from external theft:

*Shoplifting:* offenders entering a retail store and removing goods without paying for them. The goods can be concealed in many different ways (in bags, under clothing or secreted in push chairs and prams). This includes so called 'sweep thefts' when offenders take a large number of the same item at the same time, and tag switches when shop thieves replace a bar code or sales ticket with one representing a lesser value.

*Returning stolen goods:* shoplifters returning previously stolen items in order to obtain a cash refund. There are many variants of this, including: the purchase of the same product as the one stolen and then using the genuine receipt to refund the stolen item; using a stolen or invalid cheque book/credit card to purchase items and then returning the goods and getting a cash refund; or simply intimidating store staff, claiming that receipt-less items were genuinely purchased.

*Grazing:* customers consuming stock while they are in the store.

*Till snatches:* offenders targeting till operators, demanding or grabbing cash and usually carried out in a threatening or violent manner.

*Burglary:* offenders entering a building (usually by force) when it is closed, and removing goods and or cash.

### ***Supplier Fraud***

The 2001 ECR Europe study on stock loss identified that for retailers 12 per cent of all losses were thought to be due to supplier fraud, which equates to €1.6 billion a year. Supplier fraud is defined as the losses due to suppliers, or their agents, deliberately delivering fewer goods than companies are eventually charged for. This includes vendor and contractor fraud and the losses due to discrepancies in the goods supplied by third parties and not from companies' own distribution centres. The recent workshop on RFID and shrinkage identified the key ways in which this form of malicious shrinkage took place. They were:

*Under/Over Delivery:* suppliers delivering less goods than the retailer ordered, but charging them for the full amount, or deliberately sending them more goods than they ordered and billing them for the new amount.

*Phantom Delivery:* suppliers claiming to have delivered orders when they have not.

*Invoice Error:* suppliers charging for more goods than delivered.

*Returns:* suppliers not crediting retailers for the full value of goods returned by them.

*Promotions:* suppliers using promotions to mask under or over deliveries or invoice errors.

*Quality/Weight of Items:* suppliers sending sub-quality products (compared to those stated on the original order) or delivering products that are below the original weight stated or expected (for instance in the delivery of fresh food).

The critical aspect of many of the approaches adopted by suppliers to defraud retailers at the point of delivery, is that they exploit two key factors: the inability of most retailers to accurately check the delivery of items to a distribution centre or store and the ‘distance’ between the point of delivery and the administrative/ordering function of the retail organisation. The sheer scale of deliveries to retail organisations means that it is almost impossible to check, certainly at item level, that what a supplier claims they have delivered has actually arrived. In addition, suppliers can exploit any disjunction between point of order and invoicing, and place of delivery. For example, when the buyer does not know that the products they originally ordered have actually been delivered to the original specification, or those responsible for billing are not fully informed about what was actually delivered.

### ***Responding to Malicious Shrinkage: Lessons to Date***

As detailed earlier, the three types of malicious shrinkage outlined above, and the specific threats associated with each of them, present a significant challenge to stock loss practitioners. In particular, and of direct relevance to the use of Auto ID, is the evolutionary nature of the approaches adopted by offenders – for some a new crime prevention strategy is perceived as less of a problem and more of a challenge! In addition, internal thieves are often in an ideal position to ‘probe’ new and existing processes and procedures to find loopholes that will enable them to increase their opportunities and reduce their risks. Recognising the organic nature of the approaches adopted to carry out malicious shrinkage is important in developing reduction strategies that are both realistic and responsive to this constantly changing offending environment. The use of Auto ID to tackle this type of shrinkage needs to be fully aware of this.



## **Problems of Managing Stock Loss**

Responding to shrinkage has suffered from a number of inter-related problems that have combined to limit its effectiveness in dealing with an issue that is costing businesses billions of Euro a year both in terms of losses and expenditure on so called ‘solutions’. Indeed, recent research has shown that if stock loss could be eliminated then profits of a typical European retailer would be 58 per cent higher<sup>49</sup>. The factors undermining effective stock loss management are: its perceived periphery within organisations; not being able to prioritise it compared to other duties; a tendency to be uni-dimensional, reactionary and solution driven; decision-making within an information vacuum; a lack of cross functional organisational co-operation; and a poor appreciation of the threats posed throughout the entire supply chain.

### **Unfortunately Necessary**

Shrinkage management suffers from an image problem within organisations. Too often it is not seen as actively contributing to bottom line profitability. It is seen as a regrettable consequence of doing business or a function that can be called upon when things have gone badly wrong, such as a break-in, when products have been contaminated or a member of staff has been attacked (often reinforced by finance officers). To this end, it is often seen as the task that requires the skills of those formally employed in public policing – detaining offenders and employing guards. Therefore, its poorly perceived profile inevitably leads to its relative marginalisation within the business.

---

<sup>49</sup> This is based upon research conducted by Cranfield School of Management.

## **Juggling Priorities**

The roles and responsibilities of security/loss prevention departments are often many and varied, ranging from issues of health and safety, through monitoring contract guarding companies, to responding to kidnap attempts on senior members of the organisation. This myriad of often competing duties, some of which may be a statutory requirement and could incur significant liability if non-compliance or negligence is proved, means that prioritising stock loss and shrinkage can be difficult for those tasked with its management.

## **Solutions Searching for a Problem**

Many of the methods and approaches currently adopted by shrinkage managers can be characterised by a prioritisation of one particular problem: shoplifting, coupled with an almost obsessive belief that the answer can be found in a quick fix technological panacea (usually electronic article surveillance). As the data presented above has shown, retail shrinkage managers themselves suggest that only about one-third of loss is caused by external theft, and yet as one senior manager put it: ‘tackling shoplifting accounts for about 95 per cent of our security budget’<sup>50</sup>.

In addition, security providers have to a considerable extent driven the stock loss agenda, in particular those offering technology-based products. This has caused shrinkage management to be led by a ‘we have a solution, can we now find a problem’ approach to stock loss. The danger with this is that companies can become locked into relationships with suppliers whereby more and more (expensive) technology is seen (with ‘evidence’ often provided by the suppliers) as the answer to the shrinkage problem.

---

<sup>50</sup> This comment was made by a senior executive (who wishes to remain anonymous) for one of the UK’s largest food retailers.

As detailed in the ECR report on shrinkage, which put forward a ‘road map’ on responding to the problem, there are a number of critical steps that need to be completed before a solution is selected, not least the collection of context-specific data on the nature of problem, and careful analysis of the underlying causes. Only after these steps have been completed can suitable solutions be selected. And even then, they need to be rigorously evaluated to measure the true impact they are having. Unfortunately, current stock loss practitioners tend to skip the preparatory steps and base their solution selection on gut instinct and security providers’ often extravagant claims.

**Figure 6 The ECR Europe Shrinkage Road Map<sup>51</sup>**



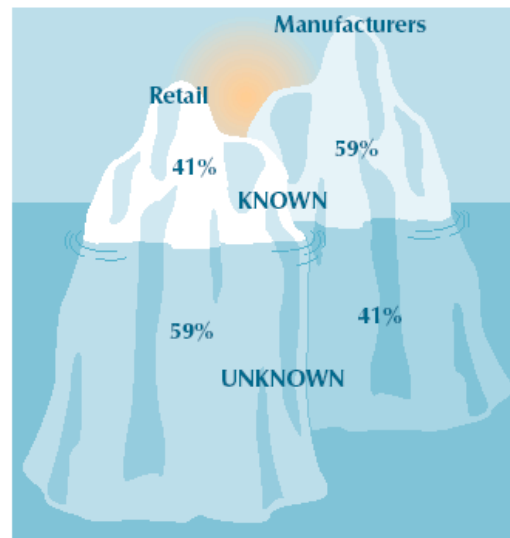
### **Living in a ‘Data Desert’**

One of the most fundamental problems currently facing security managers is a lack of relevant, timely and accurate data on stock loss. As detailed earlier, retailers in the European FMCG sector cannot account for 59 per cent of their losses, while their suppliers are unaware of 41 per cent of their shrinkage. Put another way, €10 billion of loss in this sector is simply unaccounted for (Figure 7).

---

<sup>51</sup> Beck et al (2001) op cit.

Figure 7 The ‘Shrinkage Iceberg’<sup>52</sup>



Without doubt, a paucity of data plays a pivotal part in producing poor product protection. Not knowing means not understanding, which means that any response will inevitably be piecemeal, partial and poorly defined. As the ECR report on shrinkage highlighted:

‘In theory, the concept of stock loss reduction is simple. It can be described in terms of the three following steps: make stock highly visible so that loss is immediately noticed; quickly identify the causes of the loss; and implement preventative solutions to resolve the cause of the loss and prevent reoccurrence’.<sup>53</sup>

What is almost totally absent is the data required to make the first step possible. Good decisions and effective threat assessments rely upon having high quality, reliable information<sup>54</sup>. Those currently tasked to tackle the problem of shrinkage are virtually operating behind a blindfold, dramatically inhibiting their decision-making capabilities.

### In Splendid Isolation

If security managers can be defined as working in a ‘data desert’, then they can also be considered to be there very much alone. The ECR survey found very low levels of both inter and intra company co-operation on resolving the problem of stock loss. Very few organisations have recognised the value of co-operating across company functions to develop more integrated and strategic approaches. Functions such as buying and marketing, IT and human resources were found to be rarely involved in security management issues and yet they

<sup>52</sup> Ibid.

<sup>53</sup> Beck et al (2001) op cit.

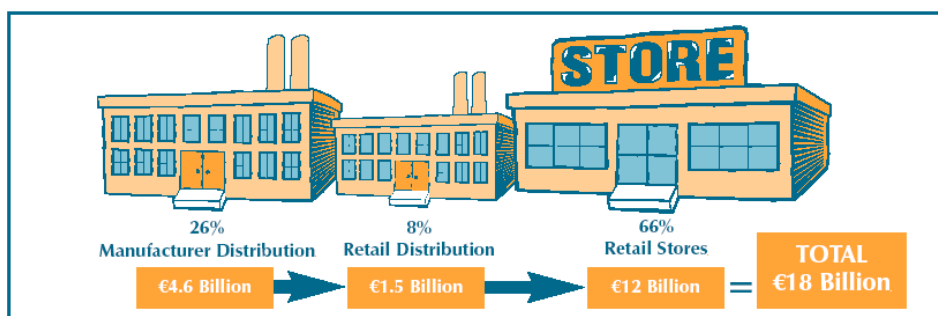
<sup>54</sup> Duncan, K., Gale, S., Tofflemire, J. and Yaksick, R. (1992) ‘Conceptualizing a Value-Added Approach to Security Management: The Atkinson Security Project I’, *Security Journal*, Vol. 3.

have much to offer both in terms of identifying future problems and helping to implement potential solutions. Likewise, co-operation between companies throughout the supply chain was found to be largely absent. As the ECR report found, ‘shrinkage is a problem that transcends ... company boundaries – it is something that requires genuine partnership and co-operation if it is to be managed efficiently and effectively’<sup>55</sup>. To date this has not happened to any great extent.

## Myopic Management

The final factor affecting shrinkage practitioners is a tendency to see the problem as only occurring at the end of the supply chain – after the products eventually reach the store. This is in part a function of the prioritisation of shoplifting as the primary cause of stock loss. The store is the point at which customers are allowed to interact with the products and where many of the current technology ‘solutions’ are most easily applied. But as the ECR survey found, up to one third of loss takes place before the goods have reached the retail outlet, highlighting the need to look at losses of goods in transit and while being stored in distribution centres. Certainly the stores are a very vulnerable part of the supply chain, but they are very much *a part* of the chain and stock loss practitioners need to look beyond the retail outlet and recognise that good loss prevention is about securing the entire supply chain.

**Figure 8 Losses in the Supply Chain<sup>56</sup>**



<sup>55</sup> Beck et al (2001) op cit.

<sup>56</sup> Ibid

## **Current Shrinkage Solutions**

The types of approaches adopted by stock loss practitioners to tackle shrinkage can be broadly categorised under four headings<sup>57</sup>:

*Procedures and Routines:* such as annual stock loss awareness campaigns; company-wide stock loss refresher training; customer returns & refund controls (operator & customer database); damaged goods resale controls; employees exit searches; hot product identification; hot product management; point of sale information or data checks; random till cash checks; rigorous delivery checking procedures; shelf replenishment techniques.

*People and Processes:* such as anonymous phone lines; civil recovery; covert surveillance of customers or employees; employee awareness and training; employee incentives; employee integrity checks; stock audit function; internal compliance monitoring; internal security/loss prevention function; store detectives; test purchasing (mystery shopper); uniformed security guards.

*Equipment and Technology:* such as CCTV; automated ordering processes; cash protection tactics and equipment; EAS hard and soft tagging; intruder alarm systems; protector display cases applied by retail outlets; secure lockers for employees; security-sealed containers/shippers; shoplifting and theft policy posters; specialist anti-theft display equipment.

*Design and Layout:* such as appropriate product location strategies; designing-out blind spots; designing-out crime programme; distribution centre secure storage; employees entry/exit access control; external security – fences, anti-ram raid, roll; shutters; risk-based design and layouts; robust anti-theft packaging; single direction product flow.

Of particular interest to the Auto ID debate is the use of EAS because it has been seen as a possible replacement/enhancement of this technology and a means of developing commonality of purpose between suppliers and retailers. This section, therefore, focuses particularly on this approach to stock loss reduction only.

## **Electronic Article Surveillance**

One of the chief methods adopted by many retailers to tackle shoplifting has been the use of EAS. These technologies have been in use for about 40 years and are designed to increase the

---

<sup>57</sup> This categorisation has partly been driven by existing organisational cultures and a paucity of available data (see earlier).

perceived risk of the offender being caught. This is normally done by overtly marketing the presence of the system in the store. This is done in four ways: overt tags on products; the positioning of 'gates' at the entrances of stores; an audible alarm should the system be activated; and in-store notices alerting customers to the use of the system. The offender must then believe that the system will detect a tagged item leaving the store, that a member of staff will respond and apprehend the offender, and that the store will then proceed with some form of sanction (handing them over to the civil police for prosecution and so on).

In theory this is an excellent form of crime prevention for dealing primarily with the specific problem of shoplifting<sup>58</sup>. However, many difficulties have arisen, which have undermined the deterrent impact of these systems. One of the key problems has been the high level of false alarms (the system being activated by a non-theft event). Some studies have found that as many as 93-96 per cent of activations are false<sup>59</sup>. False activations of alarms can be caused by a wide range of factors, including: customers leaving the store with a tag that has not been properly de-activated by store staff; customers entering the store with a non-de-activated tag from another location; tags reactivating themselves after de-activation; and electrical items carried by customers triggering the system (bleepers, lap top computers etc<sup>60</sup>).

The impact of this has been to markedly reduce the confidence store staff have in the system and create a massive credibility gap (the crying wolf syndrome<sup>61</sup>). This in turn has an impact upon the thought processes of the would-be offender: the likelihood of apprehension is perceived as much lower and hence increases the rationale to offend.

---

<sup>58</sup> It should be noted that EAS technologies are not designed to deal with many of the other problems faced by retailers such as burglary, robbery, internal theft, process failures or supplier fraud.

<sup>59</sup> Handford, M. (1994) 'Electronic Tagging in Action: A Case Study in Retailing, in M. Gill (Ed.), *Crime at Work: Studies in Security and Crime Prevention*, Leicester: Perpetuity Press; Beck, A. and Willis, A. (1995) *An Evaluation of Security Hardware, Vol. 4*, Leicester: University of Leicester.

<sup>60</sup> The list of objects that can activate different types of EAS system is almost legion, ranging from pacemakers and metal legs, to personal identity cards and library books.

<sup>61</sup> Handford (1994) op cit; Shapland (1995) op cit.

In addition, professional shoplifters have become accustomed to finding ways to defeat the system. Once again, there are many methods adopted, including: removing the tag<sup>62</sup>, bending the tag, enclosing the tag within a substance that prevents it from sending a signal (aluminium foil lined shopping bags for instance), or purposefully activating the system to enable others to leave with stolen goods while store staff are responding to the intentional system activation (or resetting it).

Current EAS systems also suffer from a lack of compatibility between competing proprietary technologies. There are currently three main types in general use: Acousto-Magnetic (AM), Radio Frequency (RF) and Electromagnetic<sup>63</sup>. Each has positive and negative aspects, depending upon the circumstances in which they are used<sup>64</sup>. However, the overall lack of standardisation and considerable variation in sectoral and geographical adoption has created real problems for retailers and manufacturers alike. For instance, in the retail store environment some types of tags from one system can inadvertently trigger alarms in another system, while some products are unsuited to the application of tags (such as batteries or other metallic items). For manufacturers, meeting competing demands from numerous retailers to source tag products with a multitude of different types of EAS tag technologies<sup>65</sup> can add

---

<sup>62</sup> Some retailers have argued that source tagging would reduce this problem, enabling manufacturers to more effectively incorporate the tag into the product or its packaging. While this would be true, there are considerable difficulties in implementing EAS source tagging, not least the lack of agreement on a standard global system (what type of tag should manufacturers adopt, will it have to vary around the world, will it have to vary depending upon the retailer being supplied?). Such matters can have a dramatic effect upon the production costs for manufacturers, with companies such as Gillette estimating that applying EAS tags to their products slowing down their production lines by as much as 35 per cent. In addition, who pays for the tag is a thorny issue, particularly given that the sole purpose of EAS is to deal only with shoplifting. Not surprisingly, manufacturers are reticent about investing in a technology that has a dubious track record and will deliver little real value to their businesses (This issue is discussed again at the end of this paper).

<sup>63</sup> There has also been some limited use of microwave technologies.

<sup>64</sup> There appears to be little consensus within the EAS industry about which technology is most suited to use in the retail environment, although there has been some recent discussion of creating a single industry standard security tag for the US market, IDTechEx Limited (2002) 'EAS Defeated in the US', *Smart Label Analyst*, Issue 15, April.

<sup>65</sup> Some companies have resorted to applying more than one type of tag to a product.



dramatically to production costs, not only through the initial cost of the tag, but also because of the impact of applying the tag can have on rates of productivity<sup>66</sup>.

Evidence on the effect of EAS on levels of loss is mixed, with some studies suggesting it is very effective (particularly concerning the use of ‘hard’ tags)<sup>67</sup>, while others conclude it is of limited value<sup>68</sup>. Most of the studies, however, suffer from a lack of rigour in the way they have been carried out, undermining the extent to which lessons can be drawn from them. What would seem clear is that for certain types of offender (particularly the opportunist) the deterrent impact of tagging systems, if properly managed, is evident. The impact of EAS on the more determined offender is much less certain. Hence, the significant cost of installing and maintaining such systems are unlikely to be justified on the grounds of savings in reduced losses from theft. Above all, the limited scope of what the current EAS technologies (particularly soft tags) are designed to achieve (deal with shoplifting only and simply notify staff when a tagged product has left the store without being deactivated<sup>69</sup>) should mean that their future role in managing stock loss throughout the supply chain remains limited.

---

<sup>66</sup> Methods to deal with the impact upon production rates have included ‘fractionalisation’, whereby goods are selectively tagged at point of production (for instance every third item). This approach clearly relies upon the deterrent aspect of the tags being very clearly ‘advertised’ to would be offenders.

<sup>67</sup> Some recent data from the US on the impact of EAS source tagging pre-recorded music and video products suggests that it has been effective in reducing losses, although it did take 20 years to get consensus on what product should be used, Wanke, E. (2002) ‘How EAS Source Tagging Rewrote Shrinkage History in the Music and Video Sector’, *Loss Prevention*, May-June.

<sup>68</sup> Sherman, L., Gottfredson, D., Mackenzie, D., Eck, J., Reuter, P. and Bushway, S. (1997) *Preventing Crime: What Works, What Doesn't, What's Promising*, Washington, DC: Office of Justice Programs.

<sup>69</sup> The author recognises that some EAS management systems are now slightly more sophisticated, and can interact with EPOS systems and record what caused tag activations. However, their scope is still considered to be relatively limited.

## **Meeting the Challenges – What Role for Auto ID?**

If, and it is a very big if, the technology providers and standards agencies can deliver the concept of a supply chain where each product can be uniquely identified and tracked as it makes its way from the point of production through the distribution network and into the retail stores and beyond, then the potential benefits for stock loss management are dramatic and far reaching. Hence, the purpose of this section of the paper is to take the vision of ‘a supply chain where all objects can be identified and tracked automatically’ and consider how it may impact upon the problems of shrinkage and its management. What needs to be recognised from the outset, however, is that Auto ID alone is not the answer to shrinkage. It will not replace the need for good management, for tried and tested security solutions, be they high or low tech, and high quality and well-motivated staff. However, it does raise a series of interesting prospects for the possible uses of, and issues relating to, Auto ID.

### **Process Failures**

Process failures are an area where item level tagging could have a dramatic and profound effect. As detailed earlier, process failures are a non-malicious unintentional outcome of a breakdown in the management of the movement of products through the supply chain. They are mainly caused by a lack of transparency in knowing where things are. The Auto ID scenario directly tackles this problem by providing a mechanism for tracking products automatically. It will provide accurate and timely answers to the key questions: what products do we have and where are they? By doing this, it will eliminate many of the problems outlined earlier. In particular, errors in inventory should become a thing of the past. Because product recognition and recording will be automated, the problems associated with accuracy (staff not counting stock properly) and timeliness (the physical and cost limitations of

carrying out stock audits<sup>70</sup>) will be dramatically reduced. In effect, organisations would be able to maintain real time inventories of their stock and do so without the need for staff to be constantly counting products in warehouses, back room areas and on the shelves.

In addition, because staff will know exactly at any moment in time what stock is currently out on the shelves, they will be able to better manage the rotation and replenishment of stock (hence reduce the amount that goes out of date or has to be reduced in price). In theory the management system will be able to decide at what time which stock needs to be reduced and by how much in order to reduce losses to a minimum (directly impacting upon data lag and enabling staff to access product specific information). It will also directly address the problem of out stocks caused by theft – staff will always know exactly how many units are currently on display and replenish accordingly.

For many large retailers, checking the contents of pallets and roll cages as they are delivered to the store is no longer considered an efficient use of staff time, with many companies operating an across the board error in delivery correction quotient, compensating stores for presumed errors in what was requested and what was eventually picked and ultimately delivered. Auto ID technologies could be used to reduce these errors in delivery – receiving staff will know precisely what stock has arrived as it crosses the threshold of the building (this is particularly important for mixed pallet deliveries to stores). This information can then be automatically cross-checked with original order requests and any discrepancies noted. This in turn could then be traced back to the original distribution depot and indeed the picker tasked to collate the deficient order.

---

<sup>70</sup> Hayes, R. (1991) *Retail Security and Loss Prevention*, Stoneham: Butterworth-Heinemann; Jones, P. (1998) *Retail Loss Control*, Oxford: Butterworth.

Auto identification should also markedly reduce the scanning errors made by till operators. Indeed, they could simply become product identification authenticators – providing a visual check between what has been read and what appears on the customer’s receipt (this may be a reassuring middle ground between the current system and the future vision of a checkout-less shopping environment) – and the receivers of payment (not too dissimilar to the self-scan systems used by some supermarket chains).

## **Supplier Fraud**

Like process failures, supplier fraud, especially for retailers could also be radically reduced through the introduction of Auto ID. The majority of supplier fraud occurs because the recipient of the goods is usually unable to physically check that the items claiming to be delivered have in fact arrived or are those that were ordered in the first place. This also works in reverse, when retailers return unwanted or out of promotion goods to the supplier. Once again, the transparency and visibility of product provided by Auto ID is the key. Recipients of arriving tagged stock will be able to immediately cross check the delivery note with the original order and the goods presented at the point of delivery. Any overages and underages can be quickly identified and reconciled. Similarly, the authentication of each of the arriving products could be cross-checked with the manufacturer’s database of products to check the credibility of the delivered stock. Likewise, goods being returned can also be better managed, with retailers being better able to quickly identify and reconcile any discrepancies between what was claimed to have been returned and what was actually sent back.

## **Internal Theft**

Because of the nature of this type of shrinkage, as outlined earlier, it is a difficult problem to solve, but Auto ID could play a role in a number of different ways.

### ***Theft by Staff***

Most staff theft in retail stores is considered to take place in the back room areas, where staff have the greatest opportunity for removing goods and remaining unobserved. They then have a number of options as to how the product is removed from the premises. There are four main ways: consume it; secrete it in their personal belongings and then carry it out as they leave; place it outside the store, usually in a garbage receptacle for recovery at a later date; or use the internal post to have the items delivered to their home or some other 'safe' location.

The first is difficult to combat, and there is an argument that the normal physical limits on what staff can consume in a day preclude the need for such a problem to be prioritised. Carrying items out (either directly by staff or being dumped for later recovery) could be countered by tag readers being placed at all staff exists. Likewise, internal post boxes could either be located within known reader areas, or alternatively, a reader could be attached to the post box itself. Either way, the existence of product within the post box will be able to be detected. The readers could then either activate an audible alarm and or inform security staff of the illicit movement of goods outside the accepted boundaries. In this respect, it would act very much like the existing EAS tagging systems, but with the added benefit of security staff knowing the identity of the product that has triggered the alarm<sup>71</sup>.

### ***Collusion***

Staff colluding with shoplifters, particularly at the point of purchase is notoriously difficult to detect. In the 'checkout less' scenario<sup>72</sup>, the opportunity for this type of activity would be completely removed. The system would automatically 'detect' each and every product as it

---

<sup>71</sup> This works on the assumption that staff have not been able to remove the tag. If the stolen products were for future re-sale, then overly damaging the packaging (in order to remove or de-activate the tag) would be counter-productive. However, many of the problems highlighted earlier, concerning professional shop thieves and their attempts to counter EAS tags may also apply for members of staff engaged in stealing from the company.

<sup>72</sup> One of the elements of the 'vision' put forward by the Auto ID Centre is that in the future, stores may not need tills, as customers would be billed automatically once the products have passed through the store exit.

moves through the checkout area, nullifying any attempts to either not scan the product in the first place or, ‘fool’ the system into thinking that one product was in fact another, cheaper item. Even if check-outs remain, then the ability to intentionally ‘mis-scan’ a product would be dramatically reduced, as the item information would be transferred independently of the till operator.

### ***Smart Management: Deterring Dishonesty in the Workplace***

Perhaps one of the biggest impacts Auto ID may have on internal theft is through the deterrent impact of the information it can provide to managers and loss prevention staff. As detailed earlier (see Figure 5, page 18), internal theft is a function of opportunity and a lack of disincentives. By radically improving the visibility of product and its movement throughout the working environment (including if it leaves through exits at the back of the building), not only should staff have less opportunity to remove goods, but also security managers should be able to respond more quickly and effectively to incidents as they occur. These two factors (supported by judicious advertising of the system by the company, reinforced with a tough policy for those caught stealing and carefully planned access control) will act as a powerful deterrent to all staff.

## **External Theft**

### ***Intelligent Electronic Article Surveillance (IEAS)?***

As detailed earlier, current strategies for responding to shop theft have focused on the use of EAS technologies – usually based upon tags activating an audible alarm at the point of exit. This strategy requires a reaction from a member of staff to either apprehend the offender or confirm that goods have been legitimately purchased and that the tag has either not been removed or deactivated. As research has shown, the level of false alarms on current EAS systems has resulted in extremely poor levels of confidence in the system by staff and a resultant low-level response to alarm activations at store exits. Dedicated shop thieves know

this too and regularly rely upon store staff apathy and disbelief in the system to defeat EAS systems. For example, shoplifters working as part of a team will purposefully trigger the system to enable others members of the team to then exit the store while the system is either activated or being reset by store staff.

One of the real dangers in the 'all item' tagged world, if the tags are used in the same way as current EAS tags (i.e. to trigger an alarm if the tag has not been deactivated at the point of sale), is that the level of reliability at the point of deactivation needs to be dramatically and consistently higher than currently achieved. If it is not, then the shopping mall of the future will resonate to a constant cacophony of alarms as a proportion of the many millions of tagged items moving from the point of sale to the store exit falsely trigger the security gates. This would not only irritate and embarrass honest customers, but also further reduce the confidence staff have in the system and provide yet more 'background noise' for shoplifters to exploit.

### ***Dynamic Hot Product Lists***

What is perhaps more realistic, is to be product sensitive in the activation of the 'EAS component' of the tag. The notion of hot products<sup>73</sup> is now a familiar concept within shrinkage management, where particular items are highlighted as being far more at risk of theft than others and hence deserve greater attention. In addition, by having access to better quality information on the products being targeted (through the greater visibility of products in the supply chain), stock loss managers could develop a much more dynamic, context driven hot product list, enabling them to decide which products should be EAS active given the local circumstances (such as store location).

---

<sup>73</sup> Clarke (1999) op cit.

In addition, even if the tag is not used to activate an EAS type alarm, the system could still notify staff when a product has been removed from the store illegally, which would provide valuable data for the purposes of replenishment (reducing out of stocks) and for creating a better profile of the products most likely to be targeted for theft.

### ***Sweep Thefts***

As outlined earlier, sweep thefts are a major problem for retailers, as they can result in significant losses through offenders taking large numbers of products at one go from the shelf. Developing a proactive response to this problem requires raising the risk of apprehension to the potential offender. This can be done in two interrelated ways. First, making the offender 'aware' that the 'system' has noted the number of products that have been removed from the shelf. This could be done through innovative active on-shelf displays with remarks such as 'thank you for purchasing x number of x product' being shown. Secondly, through alerting in-store staff that a multiple number of pre-defined 'risky products' have been removed at once. They in turn could then be provided with additional information to enable them to either track the offender (for instance through linking the activation to in-store CCTV), and or be better prepared when the multiple stolen items eventually activate a store exit alarm. If this level of risk awareness and response can be achieved, then it could send a powerful deterrent message to the offender community and further reduce the threat.

### ***Tag Visibility and Deterrence***

For the opportunistic shop thief at least, the deterrent impact of overt security measures has been found to be relatively successful. Overt security tags, the presence of CCTV, security signs and the presence of security guards can all act to 'put off' the casual offender. In order



to maximise the ‘security potential’ of a tagged product, the prospective offender needs to know that it has been tagged in the first place<sup>74</sup>.

Much of the technological drive of Auto ID is to make the chips and antennae as small as possible, principally to enable them to be embedded in the product or the packaging, so that they are virtually invisible to the consumer. The danger with this is that any deterrent impact may be as small as the eventual chip!<sup>75</sup> Therefore, careful consideration needs to be given as to how the tags will be advertised. This can be done at three levels: at the micro level through notices on the product packaging; at the mezzo level through the use of displays in the shopping environment; and at the macro level through raising general public awareness through the media.

### ***Removing Tags***

One of the problems with existing tagging systems is that the applied tag is vulnerable to removal by the committed and wily shop thief. Certainly some of the proposed ideas on embedding the tag within the product or the packaging will overcome many of the current tag removal strategies, but it may not necessarily stop those offenders who use other methods to nullify the ability of the chip to communicate with readers (such as placing the tagged product within an aluminium foil lined bag). The tracking capabilities of the proposed Auto ID system may however help with this problem too. For instance, the ‘disappearance’ of a tagged item between the shelf and the till could alert store staff to its possible theft. This would obviously, however, require a very dynamic and interactive information management system together with an extremely prompt response from security staff for it to be a realistic proposition.

---

<sup>74</sup> A study by Beck and Willis found that only 13.4 per cent of customers were aware of the presence of EAS tags (Beck and Willis [1995] op cit), while Hayes and Rogers found that 86 per cent of apprehended shoplifters were unaware products were EAS tagged (quoted in Hayes, R. [unpublished] EAS Impact Analysis: A White Paper).

<sup>75</sup> The degree to which the tag is embedded and hence difficult to remove (without destroying the product or raising the suspicions of would-be purchasers) presents a potential conflict of interest for addressing different shrinkage problems. Tags need to be overt for deterring would be offenders and yet sufficiently covert to address some of the problems discussed later in this paper on indirect shrinkage, such as the sale of stolen goods.

### ***Returning Stolen Goods***

A common method adopted by shop thieves is to return stolen goods in order to try and get a cash refund. There are many variants of this, including: the purchase of the same product as the one stolen and then using the genuine receipt to refund the stolen item; using a stolen or invalid cheque book/credit card to purchase items and then returning the goods and getting a cash refund; intimidating store staff, claiming that receipt-less items were genuinely purchased. Whatever the method adopted, they rely upon the same factor – store staff are unable to tell whether the particular item being returned was ever purchased in the first place. By being able to uniquely identify each product and whether it has legitimately passed through a checkout, store staff will be quickly able to verify the status of a product. In the situation where a stolen or invalid cheque book/credit card has been used, then store staff should be able to link the item to the payment and either return the cheque (if it is still within the store), or cancel the financial transaction. In turn, they should be able to better link the offender and the item through the transaction. Either way, the ability to identify individual products and their status (legitimately purchased or not) could be a powerful tool in reducing the losses created by refund fraud.

The current debate about when the tag should be ‘killed’<sup>76</sup> does, however, raise issues about the effectiveness of dealing with the legitimate return of goods and their subsequent theft by staff. If the tag is killed when the product leaves the store, then the reintegration of that product back into the supply chain could be problematic and may provide opportunities for staff to then exploit this loophole and ‘help themselves’ to returned stock.

---

<sup>76</sup> Concerns about privacy and generating interference outside the retail supply chain has led to a view that the tag should be physically ‘destroyed’ as it leaves the retail store.

## **Developing an Information-Led Strategic Approach to Shrinkage Management**

As detailed earlier, stock loss management is blighted by a number of key problems, not least the dearth of reliable data on how, when and where shrinkage occurs throughout the supply chain. Auto ID offers the very real prospect of providing shrinkage managers with a window on real stock loss. It could for the first time enable an accurate understanding of what percentage each of the shrinkage factors (internal and external theft, process failures and supplier fraud) actually make up of the whole. This would be a dramatic breakthrough, enabling stock loss managers to begin to develop a much more strategic approach to managing the problem. It would also give shrinkage managers greater credibility within the organisation (by having access to high quality, reliable and timely data), enabling them to argue more persuasively for the greater prioritisation of the problem of shrinkage.

By making the supply chain considerably more visible and transparent through the unique identification of all products, Auto ID could open up a whole series of opportunities for stock loss practitioners to significantly impact upon the current losses attributed to shrinkage. As detailed above, process failures and supplier fraud are particular areas that could be effectively targeted through the information made available by Auto ID. In Europe alone, this could be a saving of €9 billion.

Within the areas of external theft and internal theft, the impact may be less dramatic, but there are certainly considerable benefits to be gained. With both problems, stock loss practitioners are disadvantaged by the delay between the incident occurring and the event being detected (if at all). This time lag is particularly exploited by offenders within organisations, who quickly recognise the opportunities (see Figure 5, page 18) presented by complex, unwieldy and poorly managed stock inventories – ‘stock gone missing? Must have happened in the warehouse/in-transit/back of the store (delete where applicable)’. Once again stock visibility

data will provide a powerful lever for shrinkage managers to develop more effective and lasting processes and procedures to tackle the malicious theft of stock from throughout the supply chain. This will be done not least because of the ability to create accurate and auditable records of accountability, increasingly connecting the movements of goods to people. Irrespective of the detection capabilities offered by this, the deterrent impact on staff could be significant, providing a truly proactive and lasting solution to the problem (providing it is regularly reinforced).

In terms of external theft, particularly shoplifting, simply considering Auto ID as a replacement for current EAS technologies would be a mistake – it is a concept currently low on credibility. However, the opportunities provided by the information made available about the movement of products and their relationship with other products could enable stock loss practitioners to begin to target their resources much more effectively in dealing with this problem. Certainly relating to returns fraud and sweep thefts, it could play a key role.

### ***A New Role for Stock Loss Managers***

With an information led strategic approach to stock loss, the role of security staff could be dramatically different. The current approach can be summarised as ‘fire fighting’ – reacting to incidents as they occur rather than proactively managing the problem. In the Auto ID future, where reliable and timely data about the movement of product is available, stock loss managers will be concerned far more with analysing problems and developing solutions based upon informed decisions. For example, security staff in stores could be directly linked to the ‘information flow’, enabling them to respond more quickly to suspected incidents of theft (both by customers and staff).

## **Indirect Shrinkage**

In the transparent supply chain, where stock loss managers can uniquely identify each product and provide an auditable trail of where it has been<sup>77</sup>, they can begin to challenge some of the problems that have been previously perceived as beyond their remit/capabilities. The two key areas are counterfeiting and the sale of stolen goods in the ‘non-retail’ market. Counterfeiting of goods cost the business community in the EU €250 billion a year, while the figure for the global market is estimated to be \$1,000 billion<sup>78</sup>. In addition to this enormous loss of potential sales, it can also have a detrimental impact upon the reputation of a company, by inadvertently associating it with products that are sub-standard or dangerous. Manufacturers and their customers could, through the ability to uniquely identify all genuine products, quickly identify fake products entering the supply chain. Security managers could then collaborate with the policing agencies, through providing auditable and evidential-quality records, and help in investigations to bring the organisations producing the counterfeit products to account.

Similarly, security managers could liaise with the public police to begin to address the sale of stolen goods. Car boot sales or flea markets have frequently been seen as an opportunity for recipients of stolen goods to sell them in the open market. Once again, the problem has been the inability to provide evidence that the goods on ‘sale’ have been stolen (in the same way as items being returned for a refund at a retail store, as detailed above). The police could be provided with readers that enabled them to gather data on the goods being sold. This information would then be linked directly to the manufacturer/retailer database and the ‘status’ of the items quickly established.

---

<sup>77</sup> The ability to link unique items to particular paper work is especially important for some types of manufacturers. For instance, in the beers, wines and spirits industry ‘carousel’ fraud is a real issue, where legitimate paperwork (required for the purposes of customs and excise) is reused on a number of occasions to enable multiple loads of stock to be imported/exported, avoiding the payment of government duties.

<sup>78</sup> <http://www.aacp.org.uk/cost-intro.html>.

In both instances, the traceability of product is once again the key. But it also highlights the way in which the security manager of the future could take on a more expansive role, targeting problems that are seen as beyond their current remit but are malicious in nature and directly impact upon the bottom line profitability of organisations.

## **Prospects, Panaceas and Practicalities**

This paper has deliberately avoided the debate about the feasibility and, indeed, desirability of introducing unique item level automatic identification. There are considerable technological hurdles to be overcome before such a system could be introduced and it is most unlikely that the Auto ID vision of all items being tagged will be introduced in the near future. However, Maoist determinism need not prevail and a phased introduction is undoubtedly the way forward. Some products and some applications will benefit from earlier introduction than others, for example the tagging of selected products at pallet and case level. In terms of shrinkage management, then this would clearly relate to those items perceived as hot products. Its introduction will however, require common standards to be agreed, accepted and implemented.

In addition, the Auto ID vision is dependent upon manufacturers and suppliers tagging their products at source and ultimately paying for this in the first instance. The current debate on EAS source tagging is instructive on this issue. As detailed earlier in this paper, EAS tags are designed to deal only with the problem of shoplifting and only really advantage those at the very end of the supply chain – they are uni-dimensional in purpose and prospective beneficiary. Quite rightly, manufacturers have difficulty in justifying a business case to support this strategy. However, the proposed Auto ID approach has many more potential benefits to offer the manufacturer community as it can be used to directly tackle some of *their* key shrinkage problems (for instance, in the FMCG sector in Europe, process failures accounted for 78 per cent of shrinkage or €3.6 billion and this, as previously discussed, is one

of the problems most likely to dramatically benefit from this approach). In other words, because Auto ID can be used to address a range of shrinkage issues throughout the supply chain, it is multi-dimensional both in terms of prospective beneficiaries and problems addressed. Given this, then the arguments against this type of source tagging become less persuasive.

It is important not to see Auto ID as a panacea to the problems of shrinkage, as it clearly is not, but more as a powerful tool to enable stock loss practitioners to manage the problem dramatically more effectively. Current stock loss prevention practice is characterised by a paucity of knowledge that generates responses that are piecemeal, partial, unsystematic and reactionary in nature, fuelled by parts of the security sector committed to championing the use of proprietary technologies. Auto ID, by giving access to unparalleled levels of product information, could empower shrinkage managers to enable them to collaborate more successfully with the rest of their company and other organisations across the supply chain and develop solutions that are effectively targeted, sustainable and receptive to the constantly changing threats presented by shrinkage. In this respect, it fits neatly with much of the shrinkage reduction ‘philosophy’ developed by ECR Europe, including the use of the ‘Stock Loss Reduction Road Map’ and the emphasis upon developing approaches that are systematic, systemic and based upon inter- and intra-company collaboration throughout the supply chain<sup>79</sup>. Auto ID could play a pivotal role in enabling this approach to be both easier to adopt and more successful in achieving the desired outcome – reducing stock loss.

---

<sup>79</sup> Beck et al (2001) op cit.

## **Next Steps: Setting the Research Agenda**

The issues discussed in this paper have focused on the potential of Auto ID to impact upon the problem of shrinkage. There are a number of initiatives currently underway that are beginning to explore the practicalities of using this technology. These include the work of the UK's Home Office *Chipping of Goods Initiative* that has provided part funding for a series of pilot studies to carry out trials on the use of RFID chips and their associated information management systems. These cover a range of areas, including: the chipping of mobile phones, luxury boats, spirits and wines, personal care products and jewellery<sup>80</sup>. Not all of these trials are operating at item level tagging and tracking. In addition, the Auto ID Centre in the US has field trials underway, looking first of all at the tagging of pallets and then moving on to cases and finally items<sup>81</sup>. This initiative is very much a proof of concept pilot, to begin to analyse whether the technologies being used and the standards being proposed will work in a real world environment.

Because the timescale for the introduction of this technology on a wide scale is highly unlikely in the short term (for item level tagging at least), there is a real opportunity to carry out further research to fully understand the impact the Auto ID approach may have on shrinkage. Detailed below are just a few of the possible areas on which this research could focus:

- Raising the profile of the opportunities presented by Auto ID for shrinkage managers through publications, seminars and workshops.
- Reviewing the findings from the current initiatives, looking at their particular impact on the shrinkage-related issues outlined earlier in this paper.

---

<sup>80</sup> Adams, C. and Hartley, R. (2001) *The Chipping of Goods Initiative: Property Crime Reduction Through the Use of Electronic Tagging Systems*, Police Scientific Development Branch, No. 13/01, London: Home Office.

<sup>81</sup> [http://www.autoidcenter.org/news\\_monthlyreport\\_mar\\_01c.asp](http://www.autoidcenter.org/news_monthlyreport_mar_01c.asp).



- Begin to carry out new studies looking specifically at the problems presented by shrinkage and its management. As detailed earlier, process failures and supplier fraud offer two areas where a significant impact could be made by Auto ID (and where there are significant benefits for other functions of the organisation), but there are also significant opportunities to target particular aspects of the other two key areas of loss: internal and external theft. In particular:
  - Views of offenders on the proposed approach, particularly relating to the opportunist offender who is more likely to be deterred by the presence of security devices. To understand how Auto ID should be ‘advertised’ and offenders’ responses to it.
  - Real time studies on the impact of the technology on offending behaviour to understand if it causes displacement where offenders target different products, places, times etc.
  - Potential methods that may be adopted by determined offenders (professional shoplifters and internal thieves) to circumvent the new technology. As discussed earlier, malicious shrinkage is characterised by the evolutionary nature of the methods used to carry it out. Research is needed to learn about the opportunities for new kinds of offending that Auto ID may present<sup>82</sup>.
- How can the role of stock loss staff be changed to make use of Auto ID? For instance, can the traditional role of store security staff be changed to enable them to become much more proactive in their approach, through linking them to the information flow offered by Auto ID (such as the sweep theft example)? How can stock loss managers make use of the ‘real time’ inventory information to generate the information-led strategic approach discussed earlier?
- Working with the police in different countries to find out, in detail, how they may be able to use the information made available to tackle the indirect loss generators such as counterfeiting discussed earlier. Can convictions be made through unique product identification and in what format must the information be presented?

These are just some of the possible areas that deserve future exploration so that the potential of Auto ID to impact on shrinkage can be fully understood.

---

<sup>82</sup> For instance many thought that the bar code and scanning machines would eliminate theft by collusion at the till, however, determined offenders quickly began to find ways to circumvent the system. One well known method is for a till operator to ‘wear’ a barcode of a cheap product on their wrist and then scan that barcode instead of the one on the product they are actually suppose to be scanning (usually much more expensive) – the till operator looks like they are performing their job and the machine makes the appropriate noise. For stock loss practitioners, this is a very difficult offence to detect. Technologies have now been developed that can address this issue, usually connecting the EPOS system to the CCTV system, but they still require a degree of initial suspicion to focus the system on a particular till operator and then careful and time consuming analysis of the information to identify the offence.