



## **Reduce Your Shrinkage and Payroll Losses While Improving Productivity: Biometrics in Retail**

A Digital Persona, Inc.  
White Paper  
April 2006

© 2006, Digital Persona, Inc.  
+ 1 650.474.4000  
[www.digitalpersona.com](http://www.digitalpersona.com)

## Table of Contents

Executive Summary .....	2
Introduction – The Power at Your Fingertips .....	2
Passwords – Poor Security Combined with High Cost of Support .....	3
Authentication – The Special Case of Retail.....	4
The Choices for Improving Authentication and Access Control.....	5
The Answer, as we said, is at Your Fingertips.....	6
The Benefits of the Fingerprint-based Single Sign-on Solution for Retail .....	7
Successful Retailer Deployments of Fingerprint Authentication .....	8
About Digital Persona .....	10

## EXECUTIVE SUMMARY

Using passwords to authenticate employee access to computers, cash registers, and other resources subjects retailers to significant risk of financial loss, coupled with a heavy burden of password support. Increasingly, retailers are turning to biometric fingerprint authentication – which uses an employee’s fingerprint to generate a unique and hack-proof “personal barcode” – to verify an end-user’s identity and authorization to use a system.

Fingerprint authentication is a password-free Single Sign-on solution that can be used easily by retailers to:

- Improve security, access control, and accountability company-wide.
- Reduce shrinkage at the cash register.
- Track time and attendance and eliminate buddy punching.
- Help relieve HR of the mountains of paperwork which complex benefits programs entail.
- Eliminate the heavy cost of password management and support.
- Help comply with laws requiring auditable protection of credit card numbers, customer information, medical information, and corporate financial records.

Financial savings can be significant. Companies can save from \$150-350 per employee per year by eliminating the burdens of password management.<sup>1</sup> They can successfully attack the 5% increase in payroll caused by buddy punching and other non-productive aspects of traditional time and attendance systems. By eliminating passwords as a feature of self-service HR kiosks, the experience and effectiveness of these systems can be vastly improved. And, finally, using fingerprint authentication can substantially improve loss prevention efforts at the most vulnerable point in a store – the cash register.



## INTRODUCTION – THE POWER AT YOUR FINGERTIPS

Michelangelo’s frescoes on the ceiling of the Sistine Chapel contain one of the most famous images in art: portraying the power in the touch of a mere finger.

Each of us is endowed with a unique and powerful authenticator, right at our fingertips, which can help retail businesses lower costs and raise security in so many ways.

In good times and bad, retailers are challenged to control their costs -- of personnel, of shrinkage, of computer technology and networks, of security systems, of employee authentication, and of complying with government regulations. Several causes of rising cost can be reduced by adopting fingerprint authentication technology at points of key access to the store, its cash registers, and its networks. It is possible to enjoy these savings without making fingerprint authentication part of a larger IT project.

“Biometrics are going mainstream,” says Jonathan Penn of Forrester Research. “It’s evident in both enterprise deployments and point-of-care, retail and restaurant deployments at the register.”

This white paper will discuss the problems with passwords and the challenges retailers face which can be alleviated by improving the verification of employee identity. It will then discuss the options for improving authentication, and examine the retailer

benefits of fingerprint authentication technology.

### **PASSWORDS – POOR SECURITY COMBINED WITH HIGH COST OF SUPPORT**

A key driver of rising retail operating costs is the use of passwords. Passwords serve as “the keys” to let employees gain access to the tools needed to do their jobs. A password authenticates its user – who is the only person who is supposed to know it – as the person authorized to have the access in question. Passwords are used to open cash registers, access employee benefits applications, clock in and out of work, open locked doors, and log in to the store’s or company’s computer networks.

But passwords have proved vulnerable to unauthorized use, and many laws have been enacted which require companies – including retailers -- to protect vital private customer information such as credit card numbers, social security numbers, personal health records, and corporate financial records. These laws require companies to be able to prove that access has been controlled and is audited.

#### **The trouble with passwords**

Over 90% of large organizations rely on static, reusable passwords to authenticate user identity and grant access. But passwords have typically been the major security risk an organization faces, and not just from people outside the company. The 2005 CSI/FBI Computer Crime and Security Survey<sup>2</sup> reported that 65% of companies reported network security breaches in 2005, and about half of the breaches were by insiders.

The reason passwords are insecure is because they are a shared responsibility between the password user and the IT administrator. No matter what the IT administrator does to make passwords

secure, these safeguards are only as good as the employee using them. Passwords can be stolen, guessed, hacked, given away, shared, and lost. Employees write their passwords on Post-it<sup>®</sup> notes left on their monitors or on cards in their wallets or purses. Many use easily-guessed personal information for their passwords, such as birth dates, family or pet names. (Telesis Community Credit Union, a Digital Persona customer in Southern California, was able to determine the passwords of 80% of its employees in less than a minute using a standard network password cracking program.)

If a password serves for access to multiple applications at home and at work and is stolen, it becomes a digital master key to all of that person’s information. For companies who do not require employees to use different passwords for their personal and professional lives, no amount of control may be enough.

The first response of many companies is to “strengthen” their passwords. They increase the number and length of passwords, and generate them randomly. Each application will have a different password. Passwords may change every 45, 60, or 90 days.

While these policies may in theory improve security by making passwords harder to crack, they maintain the partnership between IT administrators and the end-users. And because strong passwords also carry increased complexity, cost, and management responsibilities, their new strength is still only as strong as the employee using it.

How can employees be expected to remember and not write down as many as 15 or 20 passwords which have to change every few months? In short, they can’t, and find it demotivating, unproductive, and frustrating to try. The result is a significant cost of password support and management. In fact, the more you look at passwords as the preferred “key” to a company’s digital and cash assets, the worse they look.

## Passwords carry a heavy price

- ☞ *PriceWaterhouseCoopers estimates that the average employee spends 16 minutes each day authenticating and signing in to networks.*<sup>3</sup>
- ☞ *Gartner Group reports that 30-40% of help desk calls, an average of 1.2 calls per user per month, are password related. Each call costs \$20-45 to resolve.*<sup>4</sup>
- ☞ *PriceWaterhouseCoopers also concluded that up to 45% of all level one help desk calls are made to assist employees with password resets.*<sup>5</sup>
- ☞ *In 2003, one survey at a conference found that 12% of attendees used "password" as their password, 75% knew a co-worker's password, 66% had given a password to a colleague, and 66% used one password for all log-on functions.*<sup>6</sup>
- ☞ *Each year, companies spend up to \$150 per employee maintaining secure passwords.*<sup>7</sup>
- ☞ *In 2003, Giga Information Group estimated that moving to a Single Sign-on (SSO) system could save more than \$350 per user per year.*<sup>8</sup>
- ☞ *And META Group concluded that SSO can increase user productivity by 18% and user efficiency by 15% for large companies.*<sup>9</sup>

## AUTHENTICATION – THE SPECIAL CASE OF RETAIL

Retail is a business sector where, in addition to the basic problems faced by all who use passwords for authentication, companies face additional risks which are exacerbated or created by weak authentication practices. In an environment where operating margins are between 1-3%, all of these risks could critically impact profitability:

### 1. Shrinkage at the Cash Register

Retailers know the importance of loss prevention. According to the University of Florida's annual National Retail Security Survey, in 2004 retailers lost \$31 billion or about 1.6% of annual sales, to employee theft, shoplifting, fraud, and error. The biggest losses -- 47% or \$14.6 billion -- came from employees.<sup>10</sup>

It's important to note that these loss rates were achieved **EVEN THOUGH** retailers had strengthened technological controls and procedural oversight over cash operations. Closed circuit video surveillance of registers is almost universal, for example, yet still the shrinkage continues.

According to the National Retail Security Survey, this shrinkage reduced profits an average of 17.8%. Less than 3 percent of the losses were ever recovered, confirming the importance of prevention. It and other

surveys found that employees steal 6-10 times as much per incident as shoplifters.

The supermarket industry provides more compelling evidence of cash register vulnerability. The National Supermarket Research Group's 2003/2004 Shrink Survey reported supermarket shrinkage was 2.32% of sales in 2002. Cashier-caused shrink rose to 35% of these losses, while shoplifting dropped to 20%. On average, a supermarket lost more than \$450,000 that year to shrinkage. Compare the 2.32% shrinkages with the average supermarket profit of 1.1% and it's no wonder the study concludes: "Best in class supermarket operators have realized that shrink recovery can be their top profit source."<sup>11</sup>

### 2. Time and Attendance

It's called buddy punching, and everyone knows it's there -- where one employee punches the time clock for another who is late, had to leave early or isn't even coming to work. How much does this cost? The consensus is that compensation is inflated by 5% from buddy-punching and other limitations of current time and attendance systems<sup>12</sup>.

### 3. Employee benefits for a widely distributed, high turnover employee population

Human Resources departments in all companies are charged with managing the hiring, compensation, benefits and

termination of employees. In the retail sector, this challenge is magnified by the distributed nature of the business, across multiple locations, and the higher rate of employee turnover which lower-paying businesses typically experience.

#### **4. Compliance with a broad range of privacy laws**

Like all companies, retailers in the US must comply with Sarbanes-Oxley, the federal law requiring controlled and protected access to corporate financial records. In addition, retailers are required by an increasing number of states, more than 20 to date, to protect private customer information which they collect in the course of business such as credit card and social security numbers. Further, if a retailer has in-store banking, it will be subject to additional banking laws such as two-factor authentication, and if it runs a pharmacy or optician, will find itself subject to the requirements of HIPAA. If that weren't enough, if the business operates internationally then it also has to comply with similarly strict foreign laws.

In short, what makes retail different and more vulnerable than other business sectors to losses caused by weak authentication are fundamental aspects of the business: handling cash, operating in many locations, having a changing employee population, complex scheduling of floor time, and compliance with privacy laws.

#### **THE CHOICES FOR IMPROVING AUTHENTICATION AND ACCESS CONTROL**

Over time, organizations have undertaken many different approaches to strengthening their user authentication technology and processes in order to eliminate or alleviate the costs and vulnerabilities associated with password authentication. While we believe fingerprint authentication is the superior solution, other options exist.

These options can be characterized as one-factor or two-factor authentication. There are three basic types of authentication factors; the first is a secret, which is usually a password or a PIN; the second is a token - something that you possess, this is usually a smart card, ATM card or a one-time

password token; and the third factor is a biometric, something you innately possess, such as your fingerprint, iris, hand geometry, or voice.

A password is a one-factor authenticator: all you need to authenticate yourself to a network is the password. Two-factor authentication requires that you have two items to authenticate yourself, typically a password plus something else. There is even three-factor authentication, which requires two items in addition to the password. Increasing the factors required increases security, by making it harder or impossible for the wrong person to acquire all the factors needed to gain access, but they come with significant costs.

**One-Factor Options:** One factor options really fall into two categories: improved or strengthened password programs, or biometric authentication.

☞ **Passwords:** We have already discussed the "strong password" policies which many companies have adopted. These make life harder for the bad guys, but also make life harder for the administrators, and still have their vulnerability. One twist which eliminates much of the help desk support needed is to provide users with automated password reset capability. This cuts down on help desk costs, but does not eliminate the threats of loss, theft, or human engineering to password security.

☞ **Biometrics:** This is the use of a personal characteristic of the person that is uniquely theirs to authenticate identity. It could be a fingerprint, a voice print, a scan of the iris, a handprint, or a photograph (the traditional ID card authenticator.) Fingerprint authentication technology tends to be the simplest, least expensive, and easiest to deploy of these mechanisms. All have their costs of implementation, management and data storage, which, in the case of fingerprint authentication, is typically recovered through other savings in as soon as 6-12 months.

**Two-Factor Options:** These typically involve tokens, or smart cards with a password or fingerprint.

☞ **Smart Cards** are cards the size of a credit card embedded with a computer chip which stores some personal data of the holder such as a password or fingerprint template. To gain access to a system, the user has to insert the card into a card reader and then provide the second factor – entering a password or placing a finger on a reader – in order to first authenticate themselves to the card, and then jointly authenticate themselves to the system. This is very secure, but quite expensive, since the technology to issue and manage smart cards entails substantial investment in security, management, and administration.

☞ **Tokens** are small devices, usually carried on a keychain, which are programmed to generate what's known as a One-Time Password for the user. Each token is unique, and operates a unique algorithm triggered by the time of day. When the user demands a password, the token computes one and displays it on an LED. The user then enters this password into the computer, and an identical program on the server, using the same personal algorithm and running off the same clock, calculates what the password should be. If the two match, authentication is provided. This technology is more than two decades old, and has been proven to be secure beyond all doubts, but its implementation has such high and continuing costs associated with it that its deployment is not always justified due to the ongoing cost and management required.

## **THE ANSWER, AS WE SAID, IS AT YOUR FINGERTIPS**

The best choice, after a full analysis of the options, is fingerprint authentication. Fingerprint authentication technology uses a credential that lacks all the weaknesses of a password. Fingerprints cannot be forged, forgotten, lost, stolen, or shared. As we all know, no two fingerprints are alike.

**Here's how it works:** by touching a finger to a Digital Persona reader attached to a computer or embedded in a register or keyboard, a user is instantly authenticated against their centrally managed fingerprint credentials in a central directory. Provided the fingerprint credentials match those in the central directory, the user's name and password, and any other required logon credentials are automatically and securely submitted to applications without anyone ever having to type in a password.

Enrollment is simple, quick, and secure. In most cases, it takes less than a minute for an employee to enroll their fingerprints into the system.

## **Personal Identity is Safeguarded**

Fingerprint authentication technology does not capture a picture of an individual's fingerprint. Rather, the reader notes a number of key points in the fingerprint which, using a proprietary algorithm, it then converts into a small 350-bit template. The whole process happens in a secure, encrypted communication path. The result, called the template, is, in effect a Personal Barcode, unique to the individual and virtually free from threat or counterfeit.

Employees who are worried that their fingerprints are being captured should know that this is not the case, and in fact that the template protects their fingerprints, since the fingerprint image cannot be backward-engineered from the template, even if it were successfully decrypted. Neither can the template be backward engineered into a false fingerprint image to fool a reader, thanks to the proprietary algorithm used.

**Options:** Digital Persona offers two products to cover virtually all retail environments.

☞ **DigitalPersona® Pro** is fully integrated with Microsoft Active Directory (AD), and allows organizations to maintain an identity management system in Active Directory for all their users.

☞ **DigitalPersona SDKs** permits customers with legacy or open-system

based operating environments to easily engineer the integration of fingerprint authentication at the front end into their Active Directory, LDAPs or other central identity management stores.

## Deployment

**Workstation/Network Logon:** Fingerprint authentication systems installed locally on desktops improve security and convenience. Users simply touch their finger to the reader and are quickly authenticated and logged onto the computer and network. There's no need to remember or type in user account and password information. The information about the user's finger is encrypted and stored locally.

**Server Logon:** The recommended approach. The job of storing and matching fingerprint templates can be moved to a central directory. This moves authentication to a secure administrator-controlled environment. A user places a finger on the reader to logon to the network and access applications. Passwords still exist in a central repository, but are managed, changed, and controlled solely by IT. Users are freed from all aspects of password management.

Digital Persona offers two ways to achieve this goal:

- ☞ In a Microsoft Active Directory environment, DigitalPersona Pro software permits deployment without custom integration, as it uses the existing password infrastructure.
- ☞ In legacy or open-source environments common to larger and older retailers, the implementation is achieved using Digital Persona's robust and powerful SDKs to integrate fingerprint readers into the front end of any LDAP or application environment.

## The Strength of Fingerprint Authentication

Fingerprint authentication avoids many of the security risks and cost escalators outlined in this white paper because it

removes the fallible end-user from responsibility for identity management and user authentication and puts that responsibility solely in the hands of IT.

- ☞ Fingerprints cannot be guessed, shared, stolen or lost.
- ☞ A user doesn't have to think up a "strong" fingerprint, so the security doesn't depend on human effort.
- ☞ People can't "forget" their fingerprints – eliminating a major source of Help Desk calls.
- ☞ Because biometrics technologies use a physical characteristic, they are easy to use and less susceptible to misuse than other authentication measures.

## THE BENEFITS OF THE FINGERPRINT-BASED SINGLE SIGN-ON SOLUTION FOR RETAIL

By now, it should be pretty clear that migrating to an employee authentication system front-ended with fingerprint recognition technology can offer retailers significant savings which can be translated directly to the bottom line.

### 1. Shrinkage at the Cash Registers

Current controls and technology are not stopping significant losses happening at the cash register, due to their complexity and susceptibility to error or subterfuge by cashiers and their accomplices. Adding fingerprint authentication to the POS stations eliminates all questions of responsibility for a transaction, improves productivity, safeguards honest employees from being mistakenly accused, and hence makes theft at the register much more difficult.

### 2. Time and Attendance tracking

Fingerprint authentication eliminates the possibility that buddy punching can occur, and also permits employees to check in at their POS work station, rather than at some distant location in the store. Studies have found that time and attendance systems which rely on employee passwords or ID cards can result in payroll cost inflation of 5%<sup>12</sup>.

### **3. Employee benefits for a widely distributed, high turnover employee population**

Many retailers are implementing automated electronic HR benefits systems in kiosks in the back office of their stores. Adding fingerprint authentication makes use of these kiosks easier and less time consuming for employees, gives them assurance that their records are secure and available only to them, and eliminates any new password management and support costs which might otherwise occur.

### **4. Compliance with a broad range of privacy laws**

The key to compliance is accountability, control of access, and proof of that control. Fingerprint authentication simplifies compliance immeasurably by eliminating the liabilities of passwords that make data vulnerable to unauthorized use, and the company vulnerable to significant fines for non-compliance.

### **5. Password management**

The most certain source of savings will come from the elimination of end-user password management and support for the entire company. It is important not to forget headquarters and other non-retail facilities in the company when implementing fingerprint authentication. Depending on the environment, number of users, and the incumbent method of authentication, independent analysts have estimated an annual savings of \$150-\$350 (and in some multi-application headquarter environments, \$1000) per user from the elimination of password use by end-users<sup>1</sup>.


### **6. Future Enhancements**

Fingerprint readers can be used by anyone and can become the authentication point for any application or process. Therefore, your investment in fingerprint readers can also serve you as you implement tighter inventory and/or receiving controls, or extend authentication technology to your customers. Using fingerprints as part of a two-factor cashless payment process by customers can help you speed up transaction time, improve accuracy, eliminate errors, and help reduce your share of the over \$10 billion in check fraud losses which retailers suffer each year.

## **SUCCESSFUL RETAILER DEPLOYMENTS OF FINGERPRINT AUTHENTICATION**

Fingerprint authentication from Digital Persona is already benefiting retailers.

### **SAVING TIME, COMPLYING WITH HIPAA**

 Rite Aid is the nation's third-largest drug store chain, with more than 3,400 stores and over 30,000 pharmacists and pharmacist technicians on the job. Rite Aid replaced its password-based authentication systems in its pharmacies in order to benefit from "the efficiencies we felt we would obtain from not having to administer password resets, the speed of logging into the system, audit trail creation and compliance with role-based tasks," says Don Davis, CIO of Rite Aid. Freeing up time required for login, password resets, and help desk calls increased productivity and provided more time with customers.

### **INCREASE POS STATION SECURITY**



Holt Renfrew, a high end clothing retailer in Canada, was concerned about security at its 525 cash registers at its 11 stores across the country. They had complex procedures to manage cash and extraordinary transactions like overrides and discounts, with authentication based on password log-in. With over 1500 employees, the maintenance of passwords and employee IDs was a major task. In response, Holt Renfrew replaced the password system with Digital Persona's fingerprint authentication system because it was easier for employees to use, was invisible to the customer, and allowed tighter security and tracking in case of theft, since each transaction is now tied to the unique identifier of a particular employee. Surprisingly, they also found strong staff support for the move. "Staff now regard fingerprint biometrics as a tool to protect their privacy," says Holt Renfrew director of loss prevention, Marcel St. Jean.

## **TIGHTER CONTROL OF CASH REGISTERS, TIME AND ATTENDANCE**



**American Skiing Company** operates multiple seasonal hospitality environments at ski and golf resorts in New England maintaining over 200 points-of-sale manned by many employees during a typical day. Security of cashier log in/out was weakened by the many employees using them, leading to losses due to errors, unseen theft, stolen or borrowed passwords, and buddy punching, not to mention the cost of password resets, and all the other aspects of password management. American Skiing Company replaced passwords with fingerprint authentication from Digital Persona. Enrollment of an employee's fingerprint took less than ten seconds, and the benefits were almost immediate. "All other POS solutions relied on user name and passwords for authentication which became a heavy burden due to personnel turnover," said Carol Boden, vice president of IT operations at American Skiing Company. "Utilizing Digital Persona's technology allowed security to be implemented with simplicity and expediency."

## **SIMPLIFYING HR'S JOB AND BRINGING BETTER SERVICE TO EMPLOYEES**



**White Castle**, the oldest fast food restaurant chain in America, was swamped with employee paperwork. Burdened with an archaic paper-based system, the chain found managers visiting its 400 stores up to five times a week to collect forms filled out by employees related

to health and other benefits. The forms were sent to regional and corporate headquarters for key entry, which involved lengthy delays and typical data entry error rates. The company had to move to a kiosk-based online health benefits enrollment and maintenance system for its 13,000 employees, but wanted to avoid trading the management of paper for the management of passwords.

Having experienced first-hand the simplicity and ease of fingerprint authentication implemented in a new store security system, White Castle decided to integrate fingerprints as the identifier for employees into its new health benefits enrollment system with the aid of Digital Persona's SDK. The results were outstanding. More than 6,000 employees were enrolled in less than four weeks, with a less than one percent error rate among users, many of whom were not very familiar with computers.

"We have been able to cut out weeks of manual processing by eliminating the paperwork and streamlining the enrollment process which translates to a direct reduction in our payroll costs," says Don Long, director of information services. Next, the company plans to add an electronic hiring system, to simplify the application process and speed up the collection of up to 15 forms required from new employees. In the long run, the company hopes the savings and efficiencies will permit district managers to manage up to 10% more stores.

## **ABOUT DIGITAL PERSONA**

Digital Persona is the leading provider of biometric authentication solutions for enterprise networks and commercial applications. Founded in 1996, Digital Persona designs, manufactures and sells turnkey solutions that improve security and regulatory compliance while resolving password management problems. Its award-winning fingerprint technology is used worldwide by over 25 million people in the most diverse and challenging environments.

Digital Persona has strategic relationships with market-leading manufacturers and resellers including Intel, Dell Inc., Microsoft, GTSI Corp. and Hewlett-Packard. DigitalPersona<sup>®</sup> Pro, the company's flagship turnkey security solution for enterprise authentication, is used by leading organizations such as Sutter Health/CPMC, Rite Aid, the U.S. Department of Defense, Cargill, and United Bankers' Bank.

Additional information is available by contacting Digital Persona, Inc. at +1 650.474.4000 or at [www.digitalpersona.com](http://www.digitalpersona.com)

*© 2006 Digital Persona, Inc. All rights reserved. DigitalPersona is a trademark of Digital Persona, Inc., registered in the United States and other countries. All other trademarks referenced herein are the property of their respective owners.*

---

<sup>1</sup> Forester Research, "Justifying the 2003 IT Budget: Identity Management Brings Quantifiable ROI to Security," October, 2002, [www.forrester.com/Research/LegacyIT/Excerpt/0,7208,27969,00.html](http://www.forrester.com/Research/LegacyIT/Excerpt/0,7208,27969,00.html)

<sup>2</sup> Computer Security Institute, "2005 CSI/FBI Computer Crime and Security Survey", [www.gocsi.com](http://www.gocsi.com).

<sup>3</sup> PricewaterhouseCoopers/Meta Group Survey 2002, "The Value of Identity Management", [www.pwcglobal.com](http://www.pwcglobal.com).

<sup>4</sup> Gartner Group, Roberta Witty & Kris Brittain, "Password Reset: Self-Service That You Will Love," April 2002, Gartner Research Note T-15-6454, [www.gartner.com/DisplayDocument?ref=g\\_search&id=354760](http://www.gartner.com/DisplayDocument?ref=g_search&id=354760)

<sup>5</sup> PricewaterhouseCoopers/Meta Group Survey 2002, "The Value of Identity Management", [www.pwcglobal.com](http://www.pwcglobal.com).

<sup>6</sup> InfoSecurity Europe, "Infosecurity Europe 2003 Information Security Survey", April 2003, [www.theregister.co.uk/content/55/30324.html](http://www.theregister.co.uk/content/55/30324.html)

<sup>7</sup> Andreas Faruke, head of Deloitte & Touche's Identity Management Services in Canada.

<sup>8</sup> Forester, "Justifying the 2003 IT Budget: Identity Management Brings Quantifiable ROI to Security," Oct. 2002.

<sup>9</sup> "The Value of ID Management", August 2002, META Group

<sup>10</sup> University of Florida Security Research Project, "2004 National Retail Security Survey Final Report", <http://web.crim.ufl.edu/research/srp/srp.htm>

<sup>11</sup> National Supermarket Research Group, "2003 National Supermarket Shrink Survey," <http://retailcontrol.traxretail.com/ssurvey.html>

<sup>12</sup> American Payroll Association, PayTech Magazine, January 2002