WHITE PAPER

Biometrics - Retail's Best Kept Secret

Simply put, biometrics are any metrics that derive data from the features of a human that uniquely identify that person. Fingerprints, palm prints, eyes (retina and iris scans), faces, handwriting, voices, and DNA are some examples—with fingerprint biometrics being the most frequently used.

As the digitalization of retail increases and becomes the new normal, retailers are being forced to adapt and respond to this new business model—or face a dismal and shrinking future. Forward-thinking companies are reimagining what it means to be a brick-and-mortar retailer, inventing new ways to attract customers to their stores while engaging in-store customer experiences and near real-time delivery of product. All these innovations are designed to create a memorable experience so that the customer wants to return.

More than ever, this digitalization has placed IT departments in the limelight as strategic partners in reinventing retail and driving revenue. However, the "opportunity" to transform retail is fraught with danger. Retail has traditionally been a fairly risk-averse sector, and the huge investment in technology and systems required to compete in today's market is an uncomfortable reality. Retailers are challenged to make these IT investments fast enough to remain competitive. Added to their concerns is the very real possibility that they might not achieve the desired results, or that these seemingly open-ended investments might coincide with an economic slowdown.

The truth is that revenue expansion—or, at the very least, preservation—is a critical part of the profitability equation. Another part is loss prevention and asset protection, which has become a major contributor. Indeed, an increasing C-suite expectation is for loss prevention to become a key partner in enhancing the customer experience and contributing to bottom-line profit. The new loss prevention metric for success is built on how much an organization can enhance profits. In many instances, traditional loss prevention departments have evolved from "loss prevention" to "asset protection" and now to "asset and profit protection."

The Problem

Retail continues to be plagued by shrink, which is a critical metric of whether many retailers have a good or bad year. According to the 2018 National Retail Security Survey (NRSS), shrink took a $46.8 billion bite out of the US retail economy in 2017. It is no longer acceptable just to beat the shrinkage goal. The new norm, dictated by the C-suite, is by how much an organization can beat the goal. As shrinkage reduction programs continue to challenge loss prevention professionals, the emerging technologies and programs used to combat theft (both internal and external) have also become more sophisticated. This increase in sophistication is just one reason why the educational needs of the profession are changing and have led to the creation of such resources as the Loss Prevention Foundation, its certification courses LPQualified and LPCertified, and the Loss Prevention Research Council.

The danger and cost associated with making any external apprehension, the strain placed on criminal justice resources, and the exposure to adverse litigation all continue to make many leaders question whether they should be making external apprehensions. Even alternative shoplifter programs, which is only one element of the external issue, have been challenged, questioned, and abandoned. The traditional civil recovery approach, as regulated by state statutes, still seems to be a highly effective post-apprehension program for many retailers. According to the Jack L. Hayes International 29th Annual Retail

Theft Survey, only 7.8 percent of total retail theft losses resulted in recovery. So how cost effective are the industry's internal and external apprehension efforts?

Based on these grim facts, retailers who rely too much on after-the-fact detection and apprehension are fighting a losing battle. It has never been truer that you cannot apprehend and prosecute your way to a good shrink result, especially as retailers continue to grapple with the risks and costs associated with injury to customers and employees when attempting the recovery of stolen merchandise.

Employee dishonesty still accounts for 33 percent of total losses, according to the 2017 NRSS, and many believe that point of sale (POS) presents an easy opportunity to decrease these losses. Employee theft is actually one of the easiest loss components to be addressed. Since so many incidents occur in confined and controlled areas, it is easier to focus on these areas than on an entire store, as shoplifting requires. Unfortunately, many professionals rely on traditional programs and policies that have limited impact.

There is, however, a ray of hope. One technology has proven to be highly effective in both preventing employee theft and improving operational efficiencies—biometrics.

What are Biometrics?

Simply put, biometrics are any metrics that derive data from the features of a human that uniquely identify that person. Fingerprints, palm prints, eyes (retina and iris scans), faces, handwriting, voices, and DNA are some examples—with fingerprint biometrics being the most frequently used.

Implementation into our smart phones and other technology devices has made fingerprint recognition very common. In fact, it has quickly become the most secure and convenient method to replace passwords, pins, swipe cards, and keys—traditional authentication credentials that can easily be shared or stolen. When confronted with evidence of theft utilizing these outdated credentials, employees can simply say, "Someone must have stolen my password." In other words, it is incumbent on the retailer to prove culpability in these cases.

Many readers have probably noticed and experienced the CLEAR difference at many airports and large professional sports entertainment facilities. Even when a traveler has TSA Precheck or Global Entry, CLEAR helps get through screening even faster—by verifying their identity, so they can walk right up to the security bins. CLEAR uses biometrics—a person's fingerprints and eyes—to confirm identity. Even rental car agencies such as Hertz Fast Lane are using this technology to speed up service.

Other industries such as health care, travel, and government have been using fingerprint biometrics for years, and now the technology is gaining tremendous traction in retail. Biometrics are very compatible with most retail technology systems and have an attractive ROI, thus contributing easily to the bottom line. Further, biometrics have become a safe and proven technology, providing an easy win for organizations, especially important as these organizations are dealing with the risks and complexities of retooling their infrastructures for new models such as omnichannel.

How do Fingerprint Biometrics Work?

Instead of using something you have (like a key) or something you know (like a password), fingerprint biometrics use the physical characteristics of your fingerprints to identify and authenticate you. There are two separate stages involved in using a fingerprint biometric system:

These unique attributes, called minutiae, are then stored in a mathematical abstraction called a template. Commercial fingerprint biometric systems don't store actual fingerprint images; rather, they only store a representative binary code.

Enrollment. During enrollment, a person's fingerprint is scanned to identify their unique attributes, such as where ridges converge or separate. These unique attributes, called minutiae, are then stored in a mathematical abstraction called a template. Commercial fingerprint biometric systems don't store actual fingerprint images; rather, they only store a representative binary code. This code is used in the next step, verification.

Verification. In this step, a person's fingerprint is again scanned to extract the data points of their unique minutiae when they touch a fingerprint reader. These minutiae are then compared to those in the stored template. If they match, the person's identity is verified. The whole verification process takes just a few hundred milliseconds and delivers highly accurate matching results.

The Solution

It is well known that point-of-sale (POS) terminals have become a critical focal point for controlling retail businesses. The challenge is that these systems have also created more opportunities for employee theft. In fact, the systems themselves have become easy targets for theft and fraud since so many financial transactions flow through them, including payroll record keeping. While our industry has focused much on "after-the-theft" solutions by creating sophisticated exception reporting, video analytics, and more, many retailers have simply neglected preventing and eliminating the opportunities for theft in the first place.

Why Should Retailers Consider Using Biometrics?

Biometric technology is one of the quickest, easiest, and most cost-effective ways that retailers can prevent theft at the POS. It has an incredible ROI, and results are seen quickly. Fingerprint authentication has become easier to implement because it interfaces seamlessly with almost every retail technology currently being used. If it doesn't immediately interface, it is relatively easy to make modifications so that it will.

Biometric technology also:

- ***Reduces Losses.*** It is one of the quickest and most cost-effective ways to significantly prevent and reduce employee theft losses at the POS by deterring employee theft.
- ***Eliminates Time and Attendance Fraud.*** When employees are required to use their fingerprints to clock in and out, they must be physically present to punch in, and "buddy punching" is eliminated. Further, the peer pressure and resentment that oftentimes exist in an environment where buddy punching is rampant disappears as well.
- ***Improves Operational Efficiencies.*** No fumbling with or forgetting PINs and passwords. Customers are served more quickly and are happier with the in-store experience because transaction times are greatly improved. Employees simply touch the fingerprint reader to login to the POS terminal.
- ***Reduces Operational Costs.*** Expenses are eliminated by not having to replace worn-out or lost swipe cards or recover forgotten passwords and PINs, which require costly helpdesk calls to reset. Fingerprint biometrics simply don't have these expenses.
- ***Holds Employee Accountable.*** Fingerprint biometrics provide proof of presence, which irrefutably links individuals to their transactions. Employees are held accountable: they cannot pretend to be someone else or share their credentials. Fingerprint biometrics also ensure that managers follow operational procedures: they cannot delegate their authority to approve overrides and discounts to employees.

- ***Eliminates Employee Turnover Costs.*** Since thefts at the POS are eliminated, so are the costs associated with investigating, apprehending, terminating, and prosecuting dishonest employees. The costs of recruiting, hiring, training, and waiting for new employees to become as proficient as the tenured employees are also lessened, impacting bottom-line profitability in a positive way.
- ***Improves Safety During a Robbery.*** Fingerprint biometrics reduce the risk of serious injury or death during robberies. When under extreme stress, employees can forget their passwords. Fingerprint biometrics allow employees to appease a thief more quickly, keeping employees and customers safer.
- ***Viewed as a Profit Enhancer.*** When all of the operational benefits of biometric technology are conveyed to senior leadership, it's easy to demonstrate that loss prevention is taking a savvy approach to improving profitability. Traditional loss prevention methodologies tend to be viewed by senior leadership as under-performing. The addition of biometric technologies to any loss prevention strategy elevates it to a true business partner by improving the bottom line.

The fact is that handling biometric data is no different than handling other sensitive personal information for which most organizations already have policies and procedures. It boils down to getting informed consent and establishing data management policies.

Privacy Concerns

Fingerprint biometrics extract data points from a fingerprint image that cannot be used anywhere outside the system. Fingerprint images are not stored, so privacy concerns over the use of biometric data can be addressed quite easily. The fact is that handling biometric data is no different than handling other sensitive personal information for which most organizations already have policies and procedures. It boils down to getting informed consent and establishing data management policies. Organizations can reap the benefits of biometrics while maintaining the privacy of individuals if they do four basic things:

- Inform the person in writing that their biometric identifier is being collected.
- Inform the person in writing of the specific purpose and length of term for which their biometric information is being collected, stored, and used.
- Inform the person in writing how and when their biometric information will be destroyed.
- Receive a written release executed by the person.

How are Fingerprint Biometrics Being Used in Retail?

Pharmacy/Drug Stores. Standalone pharmacies and those within other stores are using fingerprint biometrics to control the workflow process of filling prescriptions. Errors in filling prescriptions have a very costly impact, causing serious injury and even death. Retail pharmacy operations have discovered the benefits of having every step in the process documented and verified using fingerprint biometrics. Each time an employee completes their part of the process, they swipe their fingerprint before passing it on to the next person. That person must verify what the previous person did before they can complete their step. Once verified, they complete their part, swipe their print, and pass it on until the prescription is given to the customer and payment is received. Fingerprint biometrics have become a great tool in preventing costly errors by creating a very effective system of checks and balances.

General Retail. Many organizations are using biometrics for time and attendance, logging in and out on the POS, and transaction control points—authorizing voids, refunds, and discounts. In addition, many retailers are realizing additional cost savings by eliminating lost-password and log-in difficulties as well as speeding customer service transactions and minimizing unnecessary delays.

Home Improvement and Distribution Centers. Controlling who has been properly trained and has the necessary clearance to operate dangerous equipment, such as trash compactors, tow motors, and forklifts, is easily done by implementing fingerprint authentication.

Electronics Retailers. Store trade-in programs must comply with certain states' "pawn shop regulations" that require any retailer operating a trade-in program to fingerprint customers making the trade. This ensures that police can investigate in cases where traded goods are stolen.

Corporate Offices. In order to improve data security, many corporate offices have installed fingerprint biometrics on their company desktop and laptop computers to eliminate sharing, duplicating, or stealing passwords. Fingerprint biometrics have eliminated the defense, "Someone must have used my password to compromise my device."

Restaurant and Quick Service. Biometrics have been utilized in this retail segment quite extensively to control issues involved in a high-volume POS transaction environment, with lots of cash transactions and void activity. Front-end POS employee theft is reduced significantly by eliminating weaknesses not addressed by traditional loss prevention or operational controls. Other cost savings are realized immediately through eliminating the need to replace worn-out or lost swipe cards and forgotten passwords and PINs that require costly help desk support to reset.

Why Use Fingerprint Biometrics Rather than Other Forms of Biometrics?

Fingerprint biometrics are the easiest type of biometrics to implement from a hardware, software, IT support, and overall cost standpoint. While other biometrics such as facial recognition might be more intriguing, so are the issues surrounding implementation. Store employees, mid-level managers, and senior leaders are often very resistant to new programs and procedures. Implementing most loss prevention programs and operational controls normally requires a change in company behavior, which affects workplace culture. Fingerprint authentication is simply the lowest risk, easiest to implement, and most reliable form of biometrics to adopt. Most employees will already be familiar with it on their own devices. And, success in implementing fingerprint biometrics can be the foundation for gaining credibility and support to move toward other advanced solutions as company needs grow.

Fingerprint biometric authentication is being adopted at increasing rates by retailers because it offers so many cost-effective benefits. It is easy to implement, requires minimal IT support, has a very quick ROI, and solves many other issues that lead to employee theft and operational deficiencies at the POS. Furthermore, it tends to support efforts to demonstrate that loss prevention contributes to a good omnichannel strategy, since there are so many operational improvements that directly enhance the customer POS one that will demonstrate an immediate positive impact on business. Fingerprint biometrics should be strongly considered as an integral part of any modern retail loss prevention strategy.

2019-10-04-hid-eat-retail-biometrics-wp-en

PLT-04738