

How to integrate biometrics

What are the challenges of integrating new biometric technologies within existing business frameworks? *ERS* asks **Jay Fry**, President and CEO for identiMetrics, for his views.

Many functions in organizations such as access and security, time and attendance, cash register log-in, and cafeteria require identification. The most common kinds of identification currently in use are smart, swipe, bar code or picture ID cards, PINs, and, of course, visual identification. Each of these methods creates its own issues and delays, and are also a drain on the time and resources of IT departments. Cards are regularly forgotten, lost, mutilated and shared; PINs are easily forgotten, swapped or stolen; and visual identification is a poor solution, especially with today's considerable security concerns and reporting issues.

Unauthorized system access by employees is a real problem in many organizations and disgruntled employees can be a likely source of attack on an organization's systems. The theft of proprietary company information is the most typical result of such unauthorized access, costing companies hundreds of millions of dollars. By using the unique fingerprint for identification, the problems and costs associated with the current methods are avoided and new standards of accountability are put into place. In this day and age, it's just smart business.

Law enforcement applications capture the rolled images of all 10 fingers on the entire finger surface in order to collect the maximum number of unique identifying points. The purpose is to identify suspects based on fingerprint images directly taken from a crime scene. Minutiae based systems, on the other hand, don't store an actual fingerprint, just unique identifying points. Minutiae based systems, like the one identiMetrics employs, uses flat images of only two fingers to create templates. Flat images reveal the center of the finger and require only a minimum of unique identifying points in order to make a match. The purpose is to identify a person already enrolled in the software. Fingerprints can never be recreated.

There are very few technologies that undergo an overnight change but that is precisely what happened to biometrics after 9/11. The government sector has catapulted biometric interest. In addition, the fear of identity theft is changing the perception of biometrics. Between 2005 and 2007, there will be about two trillion dollars in financial fraud. People are beginning to understand that biometrics actually protects privacy. Biometrics is boosting the healthcare industry as a result of HIPPA, which requires two unique forms of identification from individuals accessing a system with patient medical records.

Lastly, lower transaction fees and increased ROI are driving large retail chains to consider fingerscan biometric solutions. Retail leaders are looking closely at biometric checkout systems which allow consumers to pay via fingerscan, saving as much as 20 percent in processing costs. Over the past few years, biometrics was being pulled onto the market – now it's being pushed.

The greatest challenge is educating people regarding privacy concerns. Most people think that biometric identification is for high security or science fiction movies. They are learning that the use of biometrics actually helps pro-



“Lower transaction fees and increased ROI are driving large retail chains to consider fingerscan biometric solutions”

tect privacy and that in many biometric applications, including ours, their fingerprints are not stored anywhere and their fingerprints can never be recreated from the digital template. We have found that 100 percent of our customers that have used our software in a pilot setting buy it.

Recently, we have seen biometrics introduced in a variety of areas in the consumer marketplace. Laptop computers, grocery stores, cars, cell phones, etc. are using a biometric finger scanner to identify users. We find that the more familiar people are becoming with biometrics, the more they feel comfortable and like them. In fact, a growing number of Americans believe that finger scanning is a more secure form of identity than passports, credit cards, photo IDs, birth certificates and signatures combined.

Standardization and interoperability are the main issues facing the industry. At identiMetrics, we remain device agnostic and our software assures our customers investment protection no matter what device they purchase. In addition, enrollment – particularly for large-scale deployments – is an absolute prerequisite for success. This is true in terms of ensuring the integrity of biometric databases as well as the overall usability and reliability of the system. Educating consumers and politi-

cians so they can make informed decisions on full information and not misinformed perceptions is important as well. Privacy and security issues need to be understood and addressed. And, of course, managing the customers' expectations of biometric system capabilities with real world performance capabilities is a must as well.

When implementing biometrics, businesses should make sure the solution is a single identification platform that integrates with the different applications that are already in place. Do your homework. Biometrics needs to be properly purchased, properly installed, and users must be properly trained. It's a strategic decision for your organization.

Today, biometric technology is no longer limited to just government or high security applications, but is easily accessible to the every day consumer. Like the computers that have become an integral part of our businesses, schools and homes, biometric identification is the next step in making things work faster, safer, cheaper and more reliably – exactly what our customers are looking for! ■