

Biometrics comes to life

Fingers, hands, eyes, face, voice, all are in use and could relegate PIN-based security to history.

By Orla O'Sullivan, senior editor/technology

One might expect consumers to resist any institution's request that they offer up part of their anatomy for review, especially if this was a prerequisite to gaining access to what is rightfully theirs. Fingerprinting, for instance, carries Orwellian, if not downright, criminal connotations. Banks and others who have tested biometric-based security on their clientele, however, say consumers overwhelmingly have a pragmatic response to the technology. Anything that saves the information-overloaded citizen from having to remember another password or personal identification number comes as a welcome respite. Adding a statistical footing to this anecdotal evidence, a nationwide survey by Columbia University reported that 83% of people approve of the use of finger imaging, and don't feel it treats people as criminals.

There are, of course, cultural nuances to which institutions must be sensitive. As Ben Miller, publisher of the Personal Identification Newsletter and biometrics consultant, puts it, "I think the Feds love it, they think it's cool, whereas if you tried to impose biometrics in a creative workplace, like Apple Computer, they might see it as Big Brother." Another surprise is that the United States is a late adopter of biometrics--a term which describes automated methods of establishing someone's identity from their unique physiological or behavioral characteristic(s). A distinction is made between recognition--a database search for a match--and authentication, where the search is whittled down by the user first giving a name or PIN to identify themselves.

John Parselle, managing director of Fingerscan Pty Ltd., Sydney, Australia, reckons U.S. banks lag their foreign counterparts partly because the market here is not so consolidated and it is harder for smaller players to invest in biometrics. To date, the order of adoption has been Australia, followed by South Africa, South America, Europe, and the U.S., he says. That said, Parselle notes, "there's a huge amount of interest by banks around the world in biometrics right now." Parselle's firm, a subsidiary of Sunnyvale, Calif.-based Identix Inc., recently won what he says is the biggest bank contract for biometric security. Fingerscan is working with the Bank of Central Asia, in Jakarta, Indonesia, to replace numeric passwords for employees at 500 branches with fingerprint-based system access. The bank is Indonesia's second largest and the contract is expected ultimately to be worth \$8 million, Parselle says.

Fingerscan also has the world's largest application of biometrics in the servicing of automated teller machines. In conjunction with a contractor called Armaguard, which services ATMs for Australian banks, 1,400 ATMs now are unlocked by the representative's fingerprint. The representative brings a portable scanning device that plugs into the back of the ATM and connects to the bank's server, which grants him admittance. Unequivocally identifying who entered and how long he stayed helps keep the representative honest, Parselle says. Internal fraud is a bigger problem for banks than is external fraud, Parselle maintains, adding, "All commercial applications of our technology are for internal use." (Indeed, sources at Atalla Inc., a hardware security division of Tandem Computers, estimate that 70% of fraud is an inside job.)

Last November, a leading government supplier of biometric technology enhanced its finger-based identification system to add an extra security layer to the log-on process for Windows NT. The system, NRIdentity, also works with Unisys's Navigator software. Its supplier, The National Registry Inc., says it is in contract negotiations with domestic and foreign banks. "Password maintenance alone is a huge burden for companies," says Colleen Madigan, director of marketing with the St. Petersburg, Fla., firm. A "top 100, East Coast bank" plans to use the technology initially to replace passwords, and later to authorize wire transfers and identify customers, she added. Perdue Employees Federal Credit Union, a \$200 million institution in West Lafayette, Ind, already uses NRIdentity to identify customers. Its self-service kiosk application was the first banking implementation of the technology and served as a prototype for a new breed of kiosks from Real Time Data Management, a kiosk vendor. (They start at \$500 per kiosk.)

Besides system access, biometrics are used internally to restrict physical access, for instance, to vaults in which computer records are stored. One key area of system access is corporate cash management. Says Ben Miller, "if you're sending a message, 'invest \$100 million in a derivative' you want to be sure someone with the necessary authority said it." Likewise, when the lead bank co-ordinates all pertinent information on a company for the company's investors, it wants to be sure that the information doesn't get into the wrong hands.

Credit cards next The beauty of a biometric trait is that it is as unique as the individual from whom it was created. Unlike a password or PIN, a biometric trait cannot be lost, stolen, or recreated.

This makes biometrics an obvious antidote to identity theft, a problem that is mushrooming alongside databases of personal information. The U.S. Public Interest Research Group estimates that up to 6% of all card fraud in 1995 (\$1.5 billion) was identity fraud while, in 1996, identity fraud at Mastercard International Inc. quadrupled from the previous year. Publicity of this issue, lately, probably ensures that the specter of The-Invasion-of-The-Bodysnatchers probably outweighs the Orwellian one for most people. A spokesperson for the Associated Credit Bureaus Inc. Washington, D.C., says it has a task force considering how to limit access to credit reports. The task force shortly will make recommendations on which of the options, including biometrics, to adopt, he said.

Mastercard, meanwhile, has been testing biometrics at its corporate headquarters in Purchase, N.Y. Since July 1996, visitors have had the option of finger-based check-in. The firm, which typically receives 25,000 guests a year, also is conducting research on consumers' attitudes toward biometrics. Mastercard is not proposing to store images of individuals fingerprints (in fact, its promotional literature emphasizes, "we will not have a database of fingerprints anywhere.") Instead, it is testing finger minutiae, an approach whereby the details of someone's finger are expressed as an algorithm. The technology vendor is San Bruno, Calif.-based Indenticator Inc. Oscar Pieper, company president, told ABA BJ, "we have been working with Mastercard for about a year-and-a-half now."

Joel Lisker, senior vice-president of security and risk management with Mastercard, has said the so-called smart credit card, incorporating finger verification, could eliminate 80% of fraudulent charges. (Purchases where the cardholder is not present would remain at risk.) For the system to work, point-of-sale outlets would need a special,

finger-scanning pad, which probably would cost just \$20. Ben Miller asserts, "credit cards are considered the biggest potential application of biometrics on the consumer side, especially as cards get more sophisticated. Future smart cards will carry more value and more sensitive information." GC Tech Inc., a big technology vendor in France, the country leading implementation of smart cards, agrees biometrics might be the best way to secure smart cards. Fabrice de Comarmond, executive vice-president of technology with GC Tech, says "a digital fingerprint could be cheaper to implement than a secure keyboard." Explaining why special keyboards are required, he said, "One of the problems with smart cards today is that you enter your PIN through the computer keyboard and the PIN can be captured before it gets to the card reader."

Beyond finger scans As the photos on the opening page of this article and on the cover suggest, there's more to biometrics than finger-based measures. There's hand geometry, retina scans, and iris scans to choose from in physiology. There are also quasi-behavioral attributes that can be measured--how one speaks, or how one writes, are two in use. Then there is facial recognition, in which an image of a person's face is stored digitally when the person opens an account. At each transaction, a tiny camera feeds a live image of the person to a database which compares the image to the one stored and to the account number. Hand-based technologies are popular internally, but because one must control for a number of factors (weather conditions, cleanliness of the hand, etc.), like fingerprints, they are not so easy to implement with the general population.

Likewise, retina scans need perfect alignment of the eye to reach the retina, a point at the back of the eye. Conversely, iris scans do not require contact between the subject's eye and the biometric device in order to view the eye's colored area (the iris). Consequently, Ben Miller says "iris parts are the big area of excitement." Although the Japanese already use retina scans for ATM access, Miller predicts iris scans may become standard on Japanese ATMs. "Sensar (a Morristown, Pa., supplier of iris scanners) has just received more than \$25 million in funding from Oki Electric Industry, one of the largest suppliers of ATMs in the Pacific Southwest," Miller added.

As for facial recognition, at least two suppliers, Siemens Nixdorf, Paderborn, Germany, and Miros, Inc., Wellesley, Mass., displayed this technology at the Bank Administration Institute's Retail Delivery Conference in December. The Miros system is being installed at the Pentagon to secure the computer network there. The system could also be used for ATM access. Although the research mentioned earlier indicated people were less concerned now with the "Big Brother" aspects of biometric security, a Miros spokesman pointed out that facial recognition is nonintrusive. At an ATM, the process would begin when a person inserted her ATM card and would take about two seconds, without any customer involvement.

Chase tries voice Chase Manhattan Bank recently decided to use voice verification for customer identification following a review of several types of biometrics. Elizabeth Boyle, who led the trials and is now an independent consultant, said Chase's research found 95% of consumers would accept voice verification, compared with 80% accepting fingerprinting. Another reason it chose voice over fingerprints and signatures was that voice works remotely (by phone) whereas special readers would need to be installed in consumer's homes for the others. (FingerScan said all vendors are moving in this direction, adding that it is in talks with the Central Bank of Asia regarding a home banking application for the bank's preferred customers.) Chase conducted the first of two New York branch pilots at the end of 1995. The second concluded last September. Following the analysis of extensive follow-up research and in conjunction with the roll-out of a new teller system, Chase will implement voice verification around the end of the year, Boyle said.

One reason for waiting for the new teller system is that it can be rigged to pull the customer's file from the database before they get to the teller, she explained. The procedure will be as follows. The customer records a standard phrase. The recording is made either in the branch or from home, using auto cues. When he comes into the branch, he goes to a podium housing a modified telephone. He swipes his bank card, says the phrase, and, upon satisfying the system, receives a receipt, which he presents to the teller. The system is structured to err in the customer's favor, rejecting just two in a hundred dubious vocal matches. "Telling a customer they're not them doesn't go over well," Boyle explains. On the other hand, the system should help protect customers from fraudulent attempts to gain access to their account. A key lesson from the pilots was that the initial recording must be pristine, Boyle said. Consequently, recording cubicles will be installed in the branches and those who telephone will receive more guidance, including, for instance, "please move away from the dishwasher," she said.

The voice system vendor, Votan Corp., Pleasanton, Calif., believes Chase's application (service-marked Xtra Secure) is the only commercial application of voice verification here. Chase is also believed to have been the first bank to test dynamic signature verification. The application, from New York-based PenOp, doesn't just record an image of the customer's signature. As Boyle says, "it can tell how fast you write, how you dot your i's and cross your t's." A PenOp spokesperson said it has a number of bank clients whose names it cannot divulge. The Internal Revenue Service started last spring to accept PenOp's use in electronically filed tax returns.

Another application lending credence to biometrics and likely to bear upon bank business is electronic benefits transfer. A government task force report suggested it would be worth delaying the 1999 deadline for implementing EBT to accommodate biometrics. In fact, Indentix fingerprinting of welfare recipients currently is being tested in five states. Other banks reportedly testing/using finger-based biometrics are Bank of America, Citicorp., Mellon Bank, Bankers Trust, and Chevy Chase Savings and Loan Association, Chevy Chase, Md. Fidelity Investments Inc. is rumored to be testing voice verification. It was predicted at the BAI show that 1997 will be the big year for biometrics. Following covert tests during 1996, banks will unveil commercial applications in 1997, a number of sources said. Technical standards still need to be established so that biometrics will work universally, but ATM vendors, such as Diebold Inc., already are working to this end. New life is coming into biometrics. Ben Miller remarks, "the first application of biometrics here was in 1968: a Wall Street brokerage used fingerprints to open the vault where the stock certificates were held. That application, cost \$20,000 in 1968. It would probably cost \$1,700 today, and by the year 2000, it'll probably cost just \$300." BJ