

ID Newswire®

Trends in Personal Identification and Biometrics

www.cardtechnology.com

Vol. 2 No. 21 October 15, 2003

Identix Awarded DHS Deal Pg. 4
Identix Inc. announced a deal with the U.S. Department of Homeland Security with a potential value of \$27 million over five years.

Digital Persona Inks DOD Deal Pg. 4
Digital Persona announced that the U.S. Department of Defense has purchased 1,300 fingerprint readers for computer network access.

Hand Geometry Secure Hospital Pg. 4

The Long Road To High-Tech Driver's Licenses

Using smart cards for driver's licenses is an idea that has been bandied about in the United States without much serious movement toward using the high-tech microprocessor cards.

But late last month, the Australian state of Queensland unveiled a plan to begin issuing smart card driver's licenses to its 2.5 million drivers in 2006. The embedded chip would store licensing information and driver data, including a digital photograph of the cardholder, which could be read by a smart card reader to verify that information

printed on the card has not been tampered with. While the specifics of that project are not yet finalized, the Queensland card may include several optional applications in addition to its primary driver's license function.

In early September, the Arlington, Va.-based American Association of Motor Vehicle Administrators called for the inclusion of a 2D barcode for storing machine-readable driver data, in addition to a hologram-like standard security measure known as a 3D optical variable device, on all licenses in North

America. But AAMVA stopped way short of advocating smart card technology, and it is not recommending the use of biometric identifiers on licenses.

AAMVA's recommendations do not preclude states and provinces from adding a chip to their licenses. But for now there seems to be scant momentum behind a move to use smart cards for licenses in North America, largely because of the added cost of adding chips and concerns about the durability of smart cards. Privacy concerns and regulations have also contributing to

slowing the addition of chips to licenses in Europe as well. But recent successes in several nations around the world may signal that chip-based licenses are ready to make a big impact.

The Queensland project, which will incorporate public feedback regarding cardholder privacy and potential license applications into the final proposal, could serve as a roadmap for other nations to follow. This could be especially true in North America where driver's licenses are the de facto form of identification, as they are
> **Driver's License**, Page 2

Interoperable Fingerprint Templates Are Around The Corner



A lack of standards remains a big obstacle to the adoption of biometrics. Today, a company that installs fingerprint scanners to control employee access to its facilities, enrolls its workers using a system from a particular vendor. If that vendor later goes out of business, or if the company is unhappy with the system, the customer has to start all over again with a different biometric vendor.

Considering these options, many companies haven't been open to deploying biometrics for security systems.

But this all may be coming to an end. The biometrics community has submitted a standard that would allow users to deploy fingerprint scanners from multiple vendors. Fingerprint vendors would have to change their software to comply with the standard format. Once they do, individuals could enroll with one scanner and use another one to log on to a computer network or gain entry to a secure area.

However, there is one catch. There are two different ways of creating a template, that is, a mathematical representation of the fingerprint. And templates creat-

> **Templates**, Page 3

Is Lockheed Martin The Front-Runner For U.S.-VISIT?

Either Lockheed Martin Corp., Computer Sciences Corp., or Accenture LLP will be the prime contractor for the U.S. Department of Homeland Security's border control project.

U.S. VISIT may be the largest implementation of biometrics ever, as Homeland Security attempts to use the technology to secure the nation's borders and track travelers from non-Visa Waiver countries. The project is budgeted for \$330 million in fiscal year 2003, which began this month, and could cost anywhere between \$3 billion and \$10 billion over the next 10 years, according to estimates from the General Accounting office.

A contractor's past experience with biometric systems may play a role in the final award. Of the three finalists, Lockheed Martin looks to be the only systems integrator with significant biometric experience. Insiders say this gives Lockheed Martin an inside track. But some say whichever systems integrator wins the contract may wind up with a hugely complex project on its hands.

Spokespeople at CSC and Accenture declined to talk about their company's experiences with biometrics or whether they have formed partnerships with any biometrics vendors to gain needed expertise. Washington

> **VISIT**, Page 4



Biometrics And The Financial Services Market

Last week's International Biometric Group conference call looked at how the financial services market views biometric technology and the issues institutions need to watch out for when deploying the technology.

> **IBG**, Page 5

Canada Studies A National ID

The Canadian government is seriously considering a national identification card that would include biometrics.

> **Canada**, Page 3

> Driver's License, Page 1

in Australia. Ongoing projects in El Salvador, and other countries may also help point the way to more widespread acceptance of a chip-based license. And lastly, rising political pressure to boost the security of documents is triggering increased interest in the technology among license issuers around the world.

"I think that the identity theft problem will create some heat (in government) that hasn't been there before, and politicians will have to do something about it," says U.S.-based smart card consultant Tate Preston.

Queensland is the first state in Australia to move ahead with a proposal to issue smart card driver's licenses. In an announcement Sept. 29, Queensland Premier Peter Beattie said the license should help protect Queenslanders from identity fraud, which costs the nation approximately A\$2.4 billion (U.S.\$1.6 billion) each year, according to the Australian Crime Commission. The new license would replace the current laminated card, which has been in use for more than 15 years and has been vulnerable to tampering and fraud.

As proposed, the new license will feature a visible digital photograph and a digitized signature, which would also be stored in the Queensland Transport computer system, in addition to the license information stored on the chip. No decision has been made as to whether the card will carry a contact chip, which must be inserted into a card reader, or a contactless chip, which is read by an antenna-equipped reader when the card is held within a range of a few centimeters.

According to proposal documents, the new system would enable cardholders to renew their licenses online using a PC-connected smart card reader. Licensees could also order replacements for lost or stolen licenses by phone or online. The new card would include special license information – for bus or taxi drivers – and allow cardholders to check their traffic history online, and to transfer vehicle registration online.

The Queensland proposal outlines several optional features that the new driver's licenses may carry. For example, license holders may be able to add emergency contact information to the chip that could be accessed by police or qualified emergency medical personnel in case of an accident, but would be protected from all others with a PIN. Cardholders could add or update that emergency contact information themselves using a reader attached to their PC, or have the data updated at the time of issuance or renewal.

The license may also include a digital certificate to enable cardholders to digitally sign documents or gain electronic access to various Queensland government services. Further, as part of the proposal evaluation process, the government will consider offering license holders' access to commercial services. For example, the card could contain electronic purse or loyalty applications tied to various financial institutions or merchants.

These add-on features to the driver's license would likely be developed by the private sector in partnership with the Queensland government. This approach could help offset the cost of the new license's rollout, the proposal states. The government estimates that the card project will cost A\$60 million (U.S.\$41.3 million).

The Queensland government has called for community input on the proposal – particularly focused on its security features, issuance procedures and optional commercial services – during a consultation period, which will last until Nov. 21. The government will then evaluate the private sector's interest in partnering with the government to keep the cost of the license down.

A source familiar with the project tells *IDNewswire* that the final proposal will likely call for a fairly straightforward smart card designed specifically to be a driver's license, "but with the option to add multiple applications if there's a business case." By focusing on the need for a smart card driver's license as a standalone document, the government hopes to protect itself in case demand for additional applications never materializes. "If multi-app doesn't work, it doesn't matter. It's a classic way of minimizing risk," the source says.

Queensland bills itself as the "Smart State," and the license project illustrates its aggressive push to be at the forefront of new technologies. The adoption of high-tech licenses "would be good publicity for Queensland, and it might help lure businesses that wouldn't already be there," the source says.

In 1997, El Salvador was less concerned with publicity than with eradicating rampant driver's license fraud. The Central American nation's decision to upgrade from a low-security driver's license to a smart card was also designed to streamline and centralize paper-based license and vehicle registration administrative processes.

Sertracen SA de CV, a consortium of



A design of the proposed Australian smart card driver's license that could store more than driving information.

Salvadoran technology suppliers, won the systems integration contract for the licensing project and selected France-based Gemplus International SA to supply the cards. The licenses are 1K cards, and El Salvador has issued approximately 675,000 of them since the program's launch five years ago, according to Sertracen director Roberto Siegrist. The chips store driver's identification data, a digital fingerprint, a digital photo and a signature.

Government authorities check applicants' fingerprints against El Salvador's Automated Fingerprint Identification System at the time of issuance to make sure criminals are not attempting to obtain a new ID using a false identity. Siegrist says the fingerprint system has detected decreasing numbers of attempted frauds in recent years, which he attributes to a growing knowledge among fraudsters about the probability of detection under the new system. The presence of the biometric on the card also allows police officers in the field to verify a driver's identity using handheld smart card readers equipped with fingerprint scanners.

El Salvador expects to issue 800,000 licenses over the next five years at a cost of approximately \$50 for a five-year license, according to Siegrist. Still, Siegrist says 80% of Salvadoran adults do not have driver's licenses – instead, most rely on the mandatory national ID card, which does not carry a chip, for identification.

Other countries have also started issuing smart cards for driver's licenses. India, Malaysia, and Beijing in China are using the high-tech smart card IDs.

But in North America, where the 300 million driver's licenses serve as the de facto ID document people use for everything from air travel to proving they are old enough to purchase alcohol or tobacco, a migration to smart cards might be trickier. "<

Canadians Eyeing Biometrics And National ID

The Canadian government is seriously considering a national identification card that would include biometrics.

A House of Commons report issued last week investigates deploying a new high-tech ID card, and Denis Coderre, minister of Citizenship and Immigration Canada, held a forum last week that discussed the use of biometric technology with IDs.

If Canada issues a national ID its primary use would be to identify Canadian citizens traveling abroad, but there are many other possible applications, says Catherine Johnston, president and CEO of the Advanced Card Technology Association of Canada, a trade association. "If one sat down and crunched the numbers there would be a significant benefit to a national ID," she says. The new ID could help prevent identity theft, fraud with Canada's Social Insurance Number cards, and serve as a voter registration card, Johnston says. The ID would also most likely include some sort of biometrics.

Johnston is skeptical of cost estimates in a House of Commons report issued last week on a possible national ID for Canadians. The Interim Privacy Commissioner of Canada suggested that start-up costs alone would be between C\$3 billion and C\$5 billion dollars (U.S.\$2.3 billion and U.S.\$3.8 billion). Those projections were based on cost currently in place in Canada and cost projections made in the United Kingdom and the United States for a

similar scheme. Johnston says she has not seen enough documentation to be convinced of the figures in the report.

The report noted that the province of Ontario estimated it would cost C\$500 million (U.S.\$378 million) to roll out a smart card for establishing eligibility for government benefits. And a proposal to replace the Social Insurance Number with a national identity card was rejected by the government in 1999 due, in part, to a projected cost of as much as C\$3.6 billion (U.S.\$2.7 billion). A SIN card allows Canadians access to medical benefits and is also used for tax purposes.

The report also looked at the new permanent resident card introduced in 2002, which uses optical stripe technology. The card is biometric-ready, but does not yet contain biometrics. To date, the Canadian government has spent approximately C\$68.5 million and projects further spending of \$55.9 million for 2003-2005. There are roughly 1.5 million permanent residents who are eligible for the card.

But exactly which applications the national ID would be used for has not yet been defined, thus leaving open the question of which card technology should be used, Johnston says. One possibility is a hybrid card that uses both a smart card chip and an optical stripe. Optical stripe technology allows up to 2.8 megabytes of data to be stored on the card, whereas smart cards typically hold 64K of memory. "If you have something that requires

a lot of information you might want to look at a hybrid card," she says. "But not knowing the applications, it's hard to say."

The Canadian government is also exploring the use of biometric identifiers on a variety of ID cards and documents, according to Denis Coderre, minister of Citizenship and Immigration. "One thing is certain, the biometric train has left the station," Coderre said at a forum on biometrics he convened last week. "We have to ask ourselves: where do we want to sit on that train? Status quo is unacceptable."

The forum brought together more than 100 experts to discuss how biometrics could prevent document counterfeiting and reduce identity theft. Coderre says Canada will eventually incorporate biometrics onto such documents as ID cards for legal residents and the Citizenship card issued to foreign-born individuals who become Canadian citizens.

Other possible uses include storing biometric data on a smart card chip embedded in a passport, which has been designated as a feature of future passports by the International Civil Aviation Organization. Biometrics may also be used on an ID card planned for airport workers, a joint frequent traveler program with the United States called Nexus, and on the driver's license in the Manitoba province. Ministry sources expect a mandate to begin work on ID documents carrying biometrics within a month. <

> Templates, Page 1

ed with one technology will not be compatible with readers based on the other.

The two technologies are pattern-based templates, which create a template from the swirls and ridges of a fingerprint, and minutia-based templates, which maps points on a fingerprint to create the digital representation of the finger. Colin Soutar, chief technology officer at Toronto-based Bioscrypt Inc. says the two standards may eventually merge.

But minutia templates from different vendors will be interoperable as will pattern templates from different vendors. The standard calls for fingerprint vendors to use the same number of characters in their template files, says Frances Zelazny, director of communications at Minnetonka, Minn.-based Identix Inc., a fingerprint biometric vendor. The first set of characters in the template file would be identical, no matter the vendor, and would allow for interoperability between vendors using the

same types of templates.

Creed Jones, strategic engineer at Tacoma, Wash.-based Sagem Morpho, who chairs the subcommittee working on the minutia fingerprint standard, says the standard should be approved by the American National Standards Institute before the end of the year. Then it will just be a matter of vendors programming their templates for the new standard. "It wouldn't be a major research project," he says of the changes vendors would have to make.

Jones says Sagem is already using the standard. Identix is also committed to the standard, says Zelazny.

Systems integrators are looking forward to vendors adopting the standard. Jeremy Grant with Reston, Va.-based Maximus Inc., says interoperable fingerprint templates would be "a colossal step forward."

Jones says the standard, if implemented, will break down some of the obstacles to the implementation of biometrics. "Vendors feel

that the lack of standards is lowering adoption," he says. "This could open up applications for driver's license security and at the point-of-sale."

Zelazny says the government may be more willing to use biometrics once standards are adopted. "It will help push some of the larger government smart card programs," she says. "Many agencies aren't willing to go beyond the pilot stage. The government doesn't like to be locked in to one solution."

In fact, Soutar says the government may require fingerprint vendors to adopt the standard in order to be eligible for contracts. "The introduction of these standards, which are fundamental to the interoperability requirements for large-scale government deployments, will provide the assurance that such deployments can proceed without the risk of being locked into proprietary solutions," he says. "This will have a very positive effect on the number of large-scale deployments of biometrics systems around the world." <

> **VISIT, Page 1**

officials following U.S.-VISIT say CSC and Accenture will most likely surround themselves with knowledgeable partners to handle the bulk of the work.

On the other hand, Lockheed Martin issued a press release in August detailing the partnerships the company has in place to compete for the U.S.-VISIT contract. Booz Allen Hamilton, IBM, Unisys, and Science Applications International Corp. are just three of Lockheed's partners with experience in biometrics and government projects.

Some may be surprised that DHS narrowed the field to three contractors relatively quickly. But those knowledgeable about the project say Lockheed, Accenture and CSC were the only ones interested. "Integration of these systems will be a daunting task," says one official. "They're dealing with legacy systems from different agencies and different developers."

Then why would an integrator want the con-

tract? Because whoever successfully puts together the U.S.-VISIT project will have that experience on its resume, a potential advantage in bidding for future projects. "If I'm the successful integrator I have a huge leg up," the official says.

Industry insiders, who did not want to be identified, say Lockheed has the inside track on the project because of its experience with Automated Fingerprint Identification Systems (AFIS). The company supplied the FBI's Integrated AFIS, a criminal fingerprint database of more than 50 million sets of images.

Lockheed also has experience with IDENT, the AFIS biometrics system that the former Immigration and Naturalization Service used to track those expelled from the country. The IDENT system will initially serve as the core for U.S.-VISIT, which the U.S. government plans to deploy at all U.S. international airports by Jan. 1. "Lockheed seems to be the front-runner due to their AFIS experience, but

it is still early and teams are still forming," says one Washington insider.

Officials say CSC has formed a potent team to compete for VISIT, including EDS and Northrop Grumman Mission Systems. Both EDS and Northrop have a wide range of government experience.

Accenture's only known partner for VISIT is Raytheon, a government defense contractor. "Accenture, as the late starter, is probably going to have to depend on Raytheon's connections with IDENT and other INS/DHS programs. But they're working well outside their traditional business base and have to be considered a long shot," says one insider.

Behind the scenes, biometric vendors are busy trying to ally with the three systems integrators, analysts say.

The official proposal for U.S.-VISIT is due to the integrators in November, with an award scheduled for May, Homeland Security officials say. <

Identix Awarded DHS Deal

Minnetonka, Minn.-based Identix Inc. announced earlier this month a multi-million dollar deal with the U.S. Department of Homeland Security. The contract has no spending cap, but is expected to be worth around \$27 million over five years. Identix will provide DHS with its live-scan booking stations and separate desktop systems to the Citizenship and Immigration Service of DHS. The CIS uses live-scan electronic fingerprint systems to capture and electronically submit an applicant's fingerprint images for criminal background checks prior to determining whether to grant immigration benefits. <

Digital Persona Inks DOD Deal

Redwood City, Calif.-based Digital Persona Inc. announced Tuesday that the U.S.

Department of Defense has purchased 1,300 fingerprint recognition systems for access to secure computer networks. The fingerprint scanners will be used with the DOD's Common Access Card ID and will allow users to be authorized with a fingerprint and have access to all authorized applications. However, the fingerprint template to gain access to networks is not being stored on the Common Access Card, but on the computer network. <

Hand Geometry Secures North Carolina Health Care Facility

Campbell, Calif.-based IR Recognition Systems installed 39 of its hand geometry reader at Rex Healthcare of North Carolina to heighten security for patients and 3,500 employees at its 61-acre main hospital campus. At the hospital, users enter a PIN and

place their hands on the reader. The system then verifies if the hand presented matches the one associated with the PIN, and, if so, permits access. HandKey terminals are now used in the birth center, IT data center, other major IT areas, the operating rooms, and the emergency department. <

Daon Opens Washington Office

Daon, a provider of biometric identity management software, announced last week the opening of an office in Washington and the appointment of Jim Byrne as senior vice president responsible for the company's U.S. government business. The company's global headquarters is located in Dublin, Ireland. This new office is part of Daon's expansion and plan to focus on the government sector. Byrne is an identity management and security industry veteran from Precise Software. <

Editor

Zack Martin

zachary.martin@thomsonmedia.com

Group Editor

Donald Davis

don.davis@thomsonmedia.com

Contributing Editor

Michael Fenner

michael.fenner@thomsonmedia.com

European Editor

Dan Balaban

daniel.balaban@thomsonmedia.com

Advertising Sales

Jim Baker

james.baker@thomsonmedia.com

Group Publisher

Timothy Murphy

timothy.murphy@thomsonmedia.com

Thomson Media: Pres. & CEO: James M. Malkin; Pres./CEO Publishing & Conference Group: Bruce Morris; CFO: William Johnston; SVP, Operations: Celie Baussan; CTO: Raymond Ouellette; VP, Business Development and Strategy: Greg Mazzanobile; VP, Human Resources: Robert DeNoia.

IDNewswire® is published biweekly by Thomson Media. Visit our Web site at <http://www.cardtechnology.com>. The contents of IDNewswire are, and remain, the property of Thomson Media. Reproduction or forwarding of this publication is strictly prohibited. Individuals who infringe on these rights will be prosecuted to the full extent of the law. IDNewswire is a registered service mark used herein under license.

Subscribers who want multiple copies of IDNewswire should contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com for information. The annual subscription rate is \$695. For subscription, renewal or licensing information, please contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com.

For advertising information, contact Jim Baker at 312-983-6179 or james.baker@thomsonmedia.com. Editorial offices are located at 300 S. Wacker Drive, 18th Floor, Chicago, IL 60606. Telephone: 312-983-6168. FAX: 312-913-1365.

© 2003 The Thomson Corporation and IDNewswire. All rights reserved.

IBG Looks At Biometrics In The Financial Service Market

The following is an edited transcript from the October 9 International Biometric Group teleconference by Lem Sanders, a consultant with IBG.

Today, we will be touching on opportunities for biometrics in the financial services sector. We plan to discuss emerging applications and solutions, review key growth drivers and enablers, and examine impediments to adoption on the part of financial services institutions.

Financial services has long been an area of interest for IBG, as our company's genesis was in providing biometric services for major financial services institutions. While we have long since branched out into a broad range of applications, we continue to provide research and solutions for financial institutions, and therefore closely monitor developments in this space.

In our experience, security, accountability and trust are fundamental to financial institutions' decisions on implementing emerging technologies. Opportunities for biometric vendors and solution providers are based in large part on the technology's ability to enhance security, accountability, and trust in day-to-day operations.

However, as biometrics show promise, they have not been adopted in financial services applications at the levels projected by many observers. Financial services institutions have historically been hesitant to deploy biometric solutions due to uncertainty regarding accuracy, reliability and privacy.

In order to evaluate general biometric opportunities in financial services applications, we need to define and characterize specific opportunities. Five primary biometric opportunities are present in the financial services space. Each opportunity is associated with a distinct value proposition, and each

faces impediments to deployment.

The first and largest opportunity for biometrics in this sector is PC and enterprise network access. This employee-facing use of biometrics is based on authentication at the network, application, and/or resource level. The industry has seen several thousand-plus seat deployments over the past 12 months, all based on peripheral-based fingerprint technology.

This application space is pursued aggressively by several fingerprint technology providers and middleware providers, including Identix, DigitalPersona, and SAFLINK. In many cases, biometric functionality is integrated with third party single sign-on functionality. A gating factor in this segment is the history of mergers between financial institutions – this presents challenges in terms of legacy systems integration and developing a unified authentication architecture.

A second major financial services opportunity is the use of biometrics for employment screening. Fingerprint-based background checks are mandatory for most financial services employees.

The industry is migrating from traditional card-based solutions – messy, time-consuming, and error-prone – to electronic fingerprinting solutions that reduce turnaround time from weeks to days. The business case for implementing this type of solution is clear: the costs of orientation and training disqualified employees are greatly reduced if not eliminated by identifying such employees within days as opposed to weeks.

One challenge in this application is in the logistics of enrollment – it may be cost-prohibitive to deploy electronic devices in every HR department, even with new sub-\$15,000 live-scan devices on the market. Financial services institutions may require flexible solutions that utilize multiple types of electronic

International Biometric Group

background check systems in order to control deployment costs.

A third financial services opportunity for biometrics is in access control. This employee-facing solution is not as strongly informed by deployment in a financial services environment as is logical access applications. In some respects, access control requirements are universal regardless of the deployment environment. However, there is a clear need to limit access to controlled areas in this environment. In addition, financial institutions increasingly take the opportunity to enroll individuals in logical and physical access control systems at the point of registration in background check systems.

In a recent access control deployment, American Express deployed Bioscrypt's V-smart fingerprint solution at its headquarters in New York City's financial district. Users gain expedited building access by claiming their identity with a prox card, and verifying by placing their finger on the scanner. This solution increases physical security by limiting unsupervised entry to authorized AMEX employees while demonstrating the synergies of biometrics and card technology.

A fourth major financial services application for biometrics is in voice-based telephony applications. Most major financial institutions are in the process of evaluating voice verification solutions in order to determine their performance over time, across different telephone types, and with different demographics.

The value proposition associated with this application is clearer than in most others: automated authentication directly reduces staff costs and allows resources to focus on questionable transactions. In addition, deployment of customer-facing voice solutions does not impact the IT infrastructure to nearly the degree that PC/enterprise network access solutions do. The primary impact occurs in the enrollment process.

One impediment to deployment in this space is financial institutions' insistence on degrees of security and resistance to attacks that far exceed the level of security available in operator-based systems. Institutions expect to provide near-absolute security against impostors and recordings, despite the fact that man-in-the-loop authentication is probably more susceptible to attacks such as those

> **IBG**, Page 6

Biometric Opportunities In The Financial Services Market

- **PC and network access**
- **Employment screening**
- **Physical access control**
- **Voice-based speaker verification**
- **In-person customer authentication**

> **IBG, Page 5**

based on social engineering. Regardless, biometrics are asked to perform at astronomical levels of accuracy when dealing with impostors.

The fifth and final major application for biometrics in this space is in-person customer authentication. Biometric authentication, usually in the form of signature or fingerprint technology, can be integrated into the customer-processing flow in order to enhance or replace current authentication mechanisms.

One difficulty of this type of application, from a vendor perspective, is the revenue model. While enterprise security is predicated on a roughly one-to-one ratio of employees to devices, in a customer application there may be hundreds of users for each device deployed. Unless vendor revenues are tied to transactions or aggressive client licenses, there may not be substantial revenue opportunities.

In the UK, Nationwide has rolled out dynamic signature verification from Communication Intelligence Corporation (CIC) to over 680 branches for various customer authentication applications. In addition to increasing the confidence of the authentication for transactions, the project also aims at consolidating the amount of paperwork that is processed at Nationwide by leveraging digital biometric signatures.

The fourth and fifth types of opportunity for biometrics in this space differ fundamentally from the preceding examples in that they apply to customers, not employees. The dynamics of customer authentication differ almost entirely from that of employee authentication.

Customer authentication is predicated on convenience, ease of use, and limiting impact on processes. While these considerations are also central to employee applications, it is difficult to enforce compliance with customer-facing systems to the degree that one can enforce employee-based systems.

Even with these success stories, uptake in financial services institutions has not reached the levels anticipated, with the obvious exception of mandatory background checks. There are several reasons for this slow uptake, and several steps that both vendors

and institutions can take to address the issue.

First, biometrics are often held to higher standards of performance in financial services applications than in other environments. Institutions perceive that any publicized breach of their networks – whether on the part of an employee or customer – can cause severe direct and indirect financial harm. Therefore biometrics must operate at high levels of demonstrable accuracy for both impostors and legitimate users.

However, measured in terms of false match rates, false non-match rates, and failure to enroll rates, performance can vary substantially from vendor to vendor. In financial service environments, this may result in reduced security or reduced convenience.

In customer-facing applications, customers willing to enroll in biometric systems may be unable to use the systems due to poor inherent biometric data. Certain technologies can reject authorized users at high rates over periods of time and confidence in the technology can depreciate. Biometric testing is one means of validating performance claims and demonstrating suitability for deployment.

Second, the issue of privacy presents a major concern to biometric deployers in financial services. Because biometric characteristics are unique, the general public is concerned that the technology can be used as a unique identifier. In financial services, it is imperative for solution providers to pay close attention to privacy matters and to demonstrate effective protection of personal data at both system and policy levels.

Third, financial services as an industry is reluctant to deploy unfamiliar technologies prior to extensive evaluation. Vendors can address this through adherence to consensus standards such as BioAPI, X9.84, and Common Criteria. By adopting standards for APIs, data formats, encryption, data management, and performance, vendors can demonstrate the maturity of their technology and mitigate risks associated with deploying IT solutions not widely deployed at enterprise levels.

While Common Criteria certification is applied primarily in government applications, its systematic assessment and categorization of security threats and countermeasures – as

well as its requirements for functional and assurance testing – map directly to many financial services requirements.

In sum, in order to find more widespread deployment in this space, vendors should take the following steps, and deployers should facilitate and assist in their execution.

First, vendors must provide financial services institutions with sufficient assurance that their products and solutions are accurate, reliable, and privacy-sympathetic. The world has educated itself on biometrics to the point where simple assertions of capabilities are insufficient.

Instead, vendors can be expected to provide independent test data, take steps to certify products against the Common Criteria IT security framework, and participate in privacy impact assessments for large-scale implementations. Each of these steps mitigates the risks associated with biometric deployment.

Second, vendors must be prepared to assist in developing and defending a clear business case for deployment. While we are all familiar with the supposed costs associated with password replacement – a cost which biometrics are intended to offset, if not eliminate – it is incumbent on solution providers to quantify and demonstrate precisely how deploying biometrics will positively impact an institution's bottom line.

This applies to both employee- and customer-facing solutions, although very different business cases are necessary for these respective spaces. This may require examination of an institution's current authentication processes and policies. The biometric industry has been slow to present a clear value proposition to the financial services sector, which is an extremely ROI-driven community. The focus on technology-oriented aspects as opposed to solution-oriented ones, has swayed many financial services institutions to forestall or forego biometric deployments.

To conclude, the potential for biometrics in financial service environments is tremendous. Financial institutions are eager to leverage biometrics to increase security and convenience while reducing cost and risk. However, the biometric industry must work to provide both technical and fiscal reassurance that the technology will work as promised and provide a return on investment. Action is necessary to improve the technology in terms of cost, reliability, and user perception. <

For more information contact Lem Sanders at lsanders@biometricgroup.com or 212-809-9491.

The potential for biometrics in financial service environments is tremendous. Financial institutions are eager to leverage biometrics to increase security and convenience while reducing cost and risk.'