Biometric Digest

March 2005

Finger Scan • Fingerprint • Voice Scan • Retinal Scan • Signature • Iris Recognition • Hand Scan • Facial Recognition

In This Issue March 2005

Bill Rogers
Editor.Publisher

Viisage Technology Sued for Stock Fraud

An investor has sued Viisage Technology, Inc. (NASDAQ: VISG), claiming that the Company misled investors about its finances.

Berman DeValerio Pease Tabacco Burt & Pucillo (http://www.bermanesq.com) filed the class action on March 16, 2005 in the U.S. District Court for the District of Massachusetts. The lawsuit seeks damages for violations of federal securities laws on behalf of all investors who bought Viisage publicly traded securities during the period of July 22, 2004 through and including March 2, 2005 (the "Class Period").

(Continued on page 2, Col. 1 - Viisage)

Florida Credit Union Members Use Biometric Hand Readers

Recognition Systems announced that members at South Florida's largest credit union, Eastern Financial Florida Credit Union, are using its biometric technology to access safe deposit boxes at three of its existing branches, with plans to add the HandKey units at several to-be-built branches.

In the same way Bank of America, Wells Fargo, and other credit unions throughout North America have previously reported using HandKeys for entering deposit box vaults, the HandKeys at Eastern Financial Florida Credit Union automatically take a

(Continued on page 6,. Col. 2 - Credit Union)

Biometric Directory Adds 60 New Vendors; Profiles on 592 Companies Now Available

The Biometric Digest newsletter announced a major update of its biometric directory. The update added more than 60 new vendors and organizations providing a range of biometric identification products and services. The Biometric Information Directory (**BID**) now includes profiles on more than 590 biometric suppliers plus a free demonstration at their web site.

Biometric identification technology identifies individuals based on their fingerprint, iris, facial scan, voice, signature, hand print and other personal characteristics. More companies and organizations ranging from large corporations to the smallest employers

(Continued on page 10, Col. 2 - BID)

Viisage

(Continued from page 1)

To receive a copy of the complaint, contact the court or call the firm at (800) 516-9926 or go to the law firms' web site - http://www.bermanesq.com/pdf/Viisage-Cplt.pdf.

The lawsuit claims that the defendants violated Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 and the rules and regulations promulgated there under, including U.S. Securities and Exchange Commission ("SEC") Rule 10b-5.

According to the complaint, Viisage portrayed itself during the Class Period as a turn around company in the high growth sector of secure identity solutions. In reality however, (i) Viisage engaged in improper conduct with respect to a $20 million contract; (ii) the Company improperly inflated its reported revenues in the third and fourth quarters of 2004; and (iii) Viisage's internal accounting controls were so flawed that the Company qualified as a having "material weakness" under the accounting standards set by the Public Company Accounting Oversight Board.

As a result of misleading financial statements issued during the Class Period, the Company's stock soared to $9.64 per share on December 23, 2004, up from $6.95 per share on July 22, 2004, a 38.7% increase in just six months.

Then, on February 7, 2005, Viisage announced that the Company would not meet its previously issued earnings guidance for 2004. In addition, rather than report a $1.5 loss as previously projected, Viisage anticipated a loss of approximately $7-8 million.

The market's reaction was immediate. On February 8, 2005, Viisage's shares plunged as much as 24.3% -- from $7.27 to a low of $5.85.

On March 2, 2005, Viisage again shocked the market by announcing that the Company's auditor would "issue an adverse opinion with respect to the effectiveness of the Company's internal controls over financial reporting." In addition, Viisage announced that revenues for the first quarter 2005 would be between $15-$17 million -- well below expectations of $19.7-$21 million.

On this news, Viisage's shares plunged as much as 27.2% on March 3, 2005 to a low of $4.30 -- down from the close of $5.47 the previous day.

Investors who purchased Viisage publicly traded securities from July 22, 2004 through and including March 2, 2005 you may wish to contact the following attorneys at Berman DeValerio Pease Tabacco Burt & Pucillo to discuss your rights and interests.

Jeffrey C. Block, Esq.
Leslie R. Stern, Esq.
One Liberty Square
Boston, MA 02109
(800) 516-9926
law@bermanesq.com ❖

Technician Matthew Schenk puts the keyboard back on a laptop computer after installing a fingerprint sensor module at AuthenTec Inc. in Melbourne, FL. AuthenTec is expanding its operations on the strength of demand for its fingerprint-sensor products. ❖

More than one-third of IRS workers and their bosses freely gave up their computer logins to callers who identified themselves as computer technicians trying to fix a network problem. In reality, they were inspectors from the Office of the Inspector General for Tax Administration at the Treasury

Fingerprint Scanner Without Touching Skin

Mitsubishi Electric Corp. announced the world's first scanner that reads fingerprint without touching the skin. The new device uses the LED, a red light-emitting diode to read fingerprints under the surface of the skin, the usual fingerprints scanners do it using physical contact on a glass plate. But the regular systems are inefficient when the skin is damaged, wrinkled or covered with perspiration.

With the new Mitsubishi system, the person places a finger nails up, the device scans through the finger and analyzes the patterns of the skin layer below the surface.

Financial institutions and airport are expecting this to enhance security especially regarding thefts of personal data.

It will be priced at about 100,000 yen or less (about $900). ❖

CARDTECH/ SECURTECH Conference & Expo

Leading ID experts from federal government agencies and corporate enterprises will present their experiences with a wide range of logical and physical access technologies at SecurTech during the 15th Annual CardTech/SecurTech (CTST) Conference, April 12 – 14, 2005 at the Mandalay Bay Convention Center in Las Vegas, NV.

(Continued Col. 2 at bottom) ☞

Security's New Face: 3-D Face Recognition

Many organizations are using or testing 3-D face-recognition technology, although most international technology standards still support 2-D face-recognition systems, which remain the industry standard. Face-recognition technology faces opposition from privacy advocates, who fear the technology will be used to establish ubiquitous surveillance.

There are several regulatory and technological barriers to the widespread adoption of 3-D systems, and the 3-D systems must prove that they have greater accuracy than the 2-D systems. Identix CEO Joseph Atick says that, compared with 3-D systems, 2-D systems are inexpensive and easy to use. However, proponents of 3-D systems claim that 2-D systems are overly dependent on factors and characteristics such as camera angles, light conditions, or facial hair.

After some early failures, the reliability of face-recognition systems is improving, test results show. A test is being conducted this year on the reliability of 3-D scanning, but the results from that test have not yet been released. David Fisch, a consultant with the Independent Biometric Group research organization, says that both 2-D and 3-D face-recognition technologies are lagging behind iris scanning or fingerprinting in terms of accuracy. Fisch says that 3-D systems do provide more data points than 2-D systems, which increases depth and improves accuracy.

(Continued from Column 1)
The highly interactive three-day conference program will feature more than 70 speakers. Attendees will hear about the latest advances and market experiences in biometric, smart card, contactless and emerging technologies for authentication and identity management in government, healthcare and business. ❖

Face Recognition Comes to Mobil Phones

A company in Japan has developed a technology for camera-equipped handheld devices that uses face recognition technology to authenticate users. Omron says its Okao Vision Face Recognition Sensor can increase the security of mobile devices such as camera phones and PDAs, and protect the data they contain.

The user configures the software by taking a reference picture of themselves. Thereafter, in order to unlock and use the phone, they must snap another picture of their own face, which the software compares to the original. Authentication happens "within a second" of snapping the picture, Omron says (on some processors).

Omron claims that the camera need not be held in the same position each time, and that the sensor will detect the owner regardless of the location of the user's face in the frame.

Okao is available for embedded Linux, Symbian, BREW, and ITron, but not for Microsoft Windows Mobile or Windows CE. The footprint size is 450KB of Flash (and 1.5MB for the reference image) and the software requires a minimum of 370KB of RAM. ❖

"The Human Factors Involved When Implementing A Biometric System" - Part II

Our last article examined the Human Factors issues involved when implementing a biometric system. Specifically, privacy rights issues, sharing of biometric data to third parties, and the safety of biometric systems were discussed. We now continue with other Human Factors issues which should be addressed.

As the biometric system is being implemented, you ***must*** provide for a training program for your employees before the biometric system goes live. By having a good training program, many of the fears, objections, and anxieties will be overcome. Also, your employees will have acquired the necessary knowledge in how to properly enroll and verify themselves before going live. What should be included in the training program? You should design the training program to suit the needs of your employees. However, the topics that should be covered include a brief primer into the science of biometric technology, as well as conducting pilot runs so your employees will know how to use the devices properly. Also, you may want to give your employees printed material which consists of the key points covered in the training program. This can be used as a reference later on.

Although having a training program may sound like a lot of work and effort on your part, you will be saving a lot of money, frustrations, and headaches in the long term. There is a biometric management methodology called BANTAM-which stands for Biometric and Token Technology Application Modeling Language-it was developed by biometrics pioneer Julian Ashbourn from England. This methodology contains a training program which you should consider using. For more information about BANTAM, visit (http://www.htgadvance systems.com/Advance/services/index.html), or contact Mr. Ashbourn at rd@htgsolutions.com.

Another Human Factors issue raised was the use of biometric technology as a form of high level "electronic tattooing". You must give your employees the choice of whether or not to use the biometric system-it cannot be forced upon them. For example, if you address employee fears and have a good training program, most of your employees will be accepting of the biometric system. However, there could be a small number of employees who will just object outright to using such a system, or you may have some employees that simply cannot use a biometric system because of physiological reasons. In these cases, you must have a back up system in place (such as a manual ID check, etc.).

With regards to the fears of "Big Brother" watching, really about the only thing you can do is to make sure your employees have the knowledge they need to use the biometric system effectively. The stigma of Big Brother watching is a worldwide one, and only time can take care of this issue. It is the media which fuels the fear of Big Brother watching, and the government misusing biometric data. For example, the days after 9/11, biometrics received a great boon by the media, by making claims that this will be the ultimate security tool-especially facial recognition. In fact, even the stock prices of major biometric companies skyrocketed to unprecedented levels. However, a few months after 9/11, and after facial recognition technology failed to live up to its high expectations, the media went totally negative on the use of biometric technology. This happened because the media did not look at the use of biometrics objectively or try to understand it. People were under the impression that facial recognition technology would be as good or even better than the human brain in terms of identifying people. The human brain has evolved over thousands of years, and when facial recognition technology is compared to this timeline, it is still in its infancy stage. This is a prime example of the media over hyping and totally condemning the use of a particular technology.

Finally, as you approach and embrace the use of biometric technology at your place of business, remember to look at it from an ***objective*** point of view. Remember, it is only a piece of technology. There is nothing mysterious or wonderful about it. It is just another security mechanism that can be used like any other-such as CCTV, card swipe, smart cards, etc. Biometric technology has its flaws just like any other technology-computers, cell phones, PDA's, etc. The bottom line is that why should we be afraid to use biometric technology if we use these other types of technology everyday in our lives?

About the Author:

Ravi Das is a consultant for HTG Solutions a software company based in Chicago, IL. The company offers a total security solutions package, utilizing biometric technology. The author can be reached at:
rd@htgsolutions.com,
http:www.htgsolutions.com
❖

Silex Technology America Introduces Access System Using Fingerprint Optical Reader

silex technology america, Inc., launched the FPA-70 fingerprint physical access system with an optical fingerprint reader providing secure authentication for door access control, and time and attendance management.

The FPA-70 is designed to enhance fingerprint based security of corporate and government enterprises. It can be used as a standalone physical access controller, or it can be networked, providing IT managers with centralized control of all physical locations.

The FPA-70 uses an optical sensor that scans at 500 dots per inch resolution providing sensitive authentication with a false rejection rating of 1-3.3 percent and a false acceptance rating of 0.0001 – 0.001 percent.

Authentication can take place in less than a second with the door opening in less than three seconds. The durable optical sensor shows verification on both a wide LCD monitor and voice message feedback to ensure authentication and status.

Additionally, the standalone system includes anti-threat alarms that sound when the device is illegally damaged or detached from the terminal—locking down the entryway of the location. It also provides centralized enrollment for 1,200 different individuals and registration of up to three fingers each.

The FPA-70 is a rugged fingerprint device that can be managed over a network for many other applications including those for bank vault guards, military firearm access control, prison management, healthcare insurance, aviation and transportation security, lunch payment, and time and attendance management.

SDK development packages are available for customized applications of the FPA-70.

Contact silex at 866-765-8761in the U.S. for more information on availability.

Additional information is available at: http://www.silexamerica.com. ❖

Vending machine spies and RFID kids

Think twice before stealing that Coke, kid. The Japanese city of Osaka has got your number — via a seriously high-tech method of crime prevention. They'll be outfitting vending machines with surveillance cameras (to be called "Unmanned Police Station Robots"). The best part? The cameras will be triggered by kids bearing RFID tags with push buttons. In an emergency, kids will trigger the tags and the nearest

(Continued at bottom, Column 2)

vending machine will start snapping pictures of the area and beaming them back to the police mother ship. Incidentally, the RFID chips will be serving a dual purpose: to track the kids. Is anyone surprised? How about adding a finger capture device to the vending machine. ❖

The Biometric Mailbox, And What People Think Of It

Do you find your mailbox pillaged of valuable samples, coupons, and your monthly subscription to that 'special' magazine before you get home? Introducing the Biometric Mailbox. Using Iris and/or fingerprint scanners, only you, your family, and your mailman will be able to get into your mailbox.

And what some people think of it.

- What happens when the postman is away ill or on holiday, no one but him will be able to put stuff in it?
- Yeah this is a LOVELY addition to any home. Does Darth Vader know his chest box is missing? How anyone could put this Taliban looking death box on their home is beyond me. Oh,...and I'm sure the freaking mailman is going to love you for making him have to be a "safecracker" to deliver your mail.
- But it is the mailman who keeps stealing the cash out of my birthday cards....
- UUmmm....How would this cut down on snail mail spam when most of it comes FROM the mailman? ❖

Supermarket Chain Goes To Fingerprint Checkouts

Customers of a German supermarket chain will soon be able to pay for their shopping by placing their finger on a scanner at the checkout, saving up to 40 seconds spent scrabbling for coins or cards, bosses say. An Edeka store in the southwest German town of Ruelzheim has piloted the technology since November and now the company plans to equip its stores across the region.

"All customers need do is register once with their identity card and bank details, then they can shop straight away," said store manager Roland Fitterer.

The scanner compares the shopper's fingerprint with those stored in its database along with account details. Edeka bosses said they were confident the system could not be abused. The chance of two people having the same fingerprint is about one in 220 million. ❖

Biometrics: It Just Won't Wash

Scientists have invented a washing machine that forces men to share the chore of doing the laundry. The smart machine is fitted with a fingerprint sensor that will not allow one person to load it twice in a row.

It means couples will have to alternate between who puts the wash on, otherwise the machine won't work. Guaranteed to put traditionalists in a spin, its Spanish inventor Pep Torres hopes the first ones will be in the shops within a year.

Designed to bring equality to the kitchen, the Te Toco - Spanish for It's Your Turn, has been fitted with a fingerprint recognition scanner in the front panel. The software, developed by Intuate Biometrics, makes it impossible for one partner to be lumbered with all the washday blues. Torres, boss of a design agency, said: 'The days of women being chained to the washing machine are over.

The Te Toco will make sure that men take their turn, otherwise they won't have any clean clothes, socks or pants to wear. The sensor has been designed to switch on the machine with a different fingerprint so husband and wife must work as a team and load it one after the other.

Chauvinists will hate it but women will love it. It is hoped the prototype will go into production and be in stores by Christmas.

Not all Spaniards share their countryman's passion for the invention. One married man from Madrid said yesterday: Chores like laundry are woman's work. This machine may be smart, but it will never catch on here. ❖

Veridicom Completes Capital Raise

Veridicom International Inc. (OTC Bulletin Board: VRDI) announced that it has received the first of three equal installments in a private placement totaling $5.1 million. The funding is being supplied by several institutional funds lead by funds managed by entities affiliated with the NIR group. The placement agent for the transaction is Joseph Stevens & Company, Inc. The three equal installments are attached to specific milestones, the first of which has been completed. Veridicom will file a Form 8-K with the SEC, which will include a more detailed description of the financing and copies of the financing agreements.

For more information visit: http://www.veridicom.com. ❖

Credit Union

(Continued from page 1)

three-dimensional reading of the size and shape of a hand and verify the customer's identity in less than one second. Recognition Systems was named recipient of the 2004 Application Market Penetration Leadership Award for access control and time and attendance applications in Frost & Sullivan's study, *World Biometrics Market*.

"We wanted to streamline our services and increase security for our safe deposit box areas," explains Mark Holmes, Vice President of Marketing for Eastern Financial Florida Credit Union. "The HandKey units provide easy, safe access to the safe deposit boxes. Now, members can let themselves in without waiting for someone to assist them."

HandKeys are currently placed in front of the door to the safe deposit area at credit union branches located in Boca Raton, Countryside, and Pembroke Pines in South Florida. Only one customer at a time is allowed in the safe deposit vault.

Eastern Financial officials considered other security measures, including alternative biometric technologies, but ultimately opted for hand geometry.

So far the credit union has found the HandKey units to be stable and user friendly. Feedback has also been favorable from members of the Credit Union ❖

Good News Biometrics – Recent Biometric Signings

>>> **Golf club installs biometric ID lockers**
A golf club in Kasama, Ibaraki Prefecture, has installed a fingerprint authentication system for its lockers housing customers' valuables.
http://www.yomiuri.co.jp/newse/20050312wo35.htm

>>> **Sequiam Biometrics Partners With Unicorp National Developments, Inc.**
Unicorp National Developments Inc. to provide 2,000 of its biometric residential deadbolts for use in Unicorp's new large golf course developments in Augusta and Charlotte.
http://biz.yahoo.com/prnews/050308/latu036_1.html

>>> The Arab National Bank in Saudi Arabia Selects Bioscrypt's V-Prox Finger Scan Reader
Arab National Bank (ANB) has selected V-Prox finger scan readers to supplement and strengthen the security of its headquarters and offices.
http://biz.yahoo.com/prnews/050315/to151_1.html

>>> Fingerprint Identification Technology To Be Adopted At Internet Cafes
Fang Chunming, head of the Anhui Provincial Youth League, has disclosed to local media that a fingerprint identification system will be adopted in all Internet cafes across China's Anhui province by July this year.
http://www.chinatechnews.com/index.php?action=show&type=news&id=2456

From the PDF electronic copy of this newsletter, place your cursor on the web address, and click to hyperlink for more information.

Biometric Calendar—Trade Shows, Seminars, Expositions

>>> ISC West Expo/Las Vegas
Sands Expo, Las Vegas, Nevada USA
Reed Exposition
Start Date: 04/06/2005 End Date: 04/08/2005
http://www.iscwest.com

>>> CardTech/SecurTech
Mandalay Bay Convention Center
Las Vegas, NV
Thompson Financial
Start Date: 04/12/2005 End Date: 04/14/2005
http://www.tmconferences.com/conferences/CTST05/

>>>ASIS International European Security Conf.
Copenhagen, Denmark
American Society for Industrial Security
Start Date: 04/17/05 End Date: 04/20/05
http://www.asisonline.org/education/programs/noframe/2004seminar/default.html

>>> InfoSecurity Europe
Grand Hall, Olympia London, England
Reed Elsevier
Start Date: 04/26/05 End Date: 04/28/05

>>> Voice World Europe 2005
Olympia Conference Center, England
Voice World
State Date: 05/04/05 End Date: 05/04/05
http://www.voice-world.com/

World Wide Biometrics

Reporting From China - John Mao, fswewi@pub.foshan.gd.cn

Domestic Signature Recognition System Tested Good

To verify the true identity of individuals and also supply evidence for forensic use, the newly released "Writing Recognition Computer System" by Professor Ding Xiao Qing of Electric Engineering Department, Tsing Hua University, was recently tested in Beijing. The results were reported as "excellent, the accuracy is quite close to 100%".

Tsing Hua University is the No.1 University in China, it is also the major base of biometrics research and development in China. Many departments and professors are involved in biometrics.

As introduced by Professor Ding, this system is now mainly designed for use by the police. It recognize the suspect's writing with his/her previous writing sample such as letters and diaries. They are then processed by the computer software in several minutes. They then generate the characteristic matching table and automatically report the conclusion.

Compared with the traditional manual matching procedure, this system is much more accurate, effective and efficient.

The shortage of this system, as Prof. Ding agreed himself, is that the operation is mostly based on the sample input.

If the number of samples is not enough, the words, which are in Chinese, the system can not provide any conclusion. Besides, if someone who is specially trained to imitate another person, the system may provide the wrong results.

An expert appraisal which was organized by the No.2 Research Institute of Public Security Department last month, the system acquired high praise. In fact, the system has been in a pilot operation for quite sometime and helped police solve some cases.
Prof. Ding is a top researcher on facial recognition in China.

First Biometric Smart Cell Phone Rolled Out

The No.1 cellular phone manufacturer in China, the Bird Communication Corp, announced recently that they will roll out the first smart phone with fingerprint verification later this year.

The Bird Corporation, with their biometric technology supplier, the Beijing Fingerpass Software Co., Ltd, produced a sample of their fingerprint smart phone which passed the quality and functionality test in Jeijing.

The Fingerpass is a joint-venture of the Bird Communication and The Institute of Automation of Chinese Academy of Sicience. The Fingerpass has focused on fingerprint biometrics for over 5 years in China.

From year 1999 to year 2004, the Bird Communication has been number one in sales figures and revenue in the Chinese cell phone industry. They began to sell their smart cell phone (with embedded OS, the combination of PDA and cell phone) in 2003. They have sold over a half million smart cell phones, valued at over 1 billion RMB (about $120 million USD). The new model, with fingerprint verification, will be their seventh smart phone model.

This smart phone, which features biometric authentication, was recently tested in Beijing. Experts gave high appraisal to the design. The designers alleged proudly

"using the wholly proprietary technologies, hardware as well as software".

Although some models of cell phones from Japan and Korean, rolled out in China, also use fingerprint verification. The model from the Bird Communication is exciting because of the powerful market promotion and cost control ability of Bird in the past.

With the implementation of the China Digital Signature Law one month later, e-business on wireless network seems to be a quite promising segment with tremendous growth potential.

Biometrics Speed Entering and Exiting Hong Kong & Mainland

The Secretary for Security, Hong Kong Special Administrative Region, Mr. Lee Siu-Kwong spoke recently that more flexible human deployment, simpler exit and entering procedures, and more new technologies will be adopted to ease and speed passengers and cargo transportation between Hong Kong and the mainland China. The is a rapidly growing concern.

A new border control station for checking will soon be set up at the Shenzhen-Hong Kong border to provide more convenience to Hong Kong residents entering and return-

(Continued on page 9, Col 3 - China)

China

(Continued from page 8, Col. 3)

ing from the mainland.

As announced by the Hong Kong government to ease the border control, some laws need to be adjusted. Hong Kong has been issuing a smartcard-based ID card with fingerprint verification for residents. It's estimated the new ID card will be held by every resident by March 2006.

From last year, Hong Kong has tested the biometrics-based border control system for both passengers and cargo transportation. Fingerprint verification tremendously increased the efficiency of checking the exit and entering process.

Mr. Lee said, later this year, the Security Bureau will suggest a financial bill to the Financial Committee of the Hong Kong Legislative Committee, for the new system to issue and use the new generation passport based on smart card technology. The facial image and fingerprint template will be stored in the chip on the new passport, together with other personal information. The new passport is expected to be issued starting in 2007.

E-borderpass Being Adopted in Guangdong To Speed Border Checks to Hong Kong & Macao.

According to the announcement by the officer from the exit and enter border bureau of the Chinese Public Security Department, the e-borderpass will be issued for mainland Chinese to conveniently visit Hong Kong and Macao.

With the new e-borderpass, the holder can be checked in at the border by machine. This will speed up the checking process. The new e-borderpass will be issued for mainland Chinese first in Guangdong province, which is adjacent to the both regions.

The e-borderpass is also a smart card based certificate which uses fingerprint biometrics. The personal information in the pass will all be machine readable. It can read out and record every entering and exiting of the holder automatically, plus checking the fingerprint verification for the true identity of the pass holder. This will quicken the border checking speed from the current 15 to 20 second per person to an estimated 5 seconds per person in future.

The new e-borderpass system will also save a lot of human labor, It is estimated that when the system is running smoothly, one border checking officer will be able to monitor 5 checking channels at the same time.

The trial system will be deployed in Zhuhai-Macao border in first half of this year, and the issue of the new e-borderpass will begin in the whole province later this year.

From other news, China will issue the e-passport before year 2008. The new e-passport will comply with the international standard. The 2008 Olympic Games are believed to be the major reason for the issue.

Fingerprint, iris or facial image templates will most likely be stored in the chip of the E-pass-port.

Early this month, China, Japan and Philippines started to test the e-passport in on a "cross- states" platform. The testis are conducted simultaneously in three airports respectively in the above three countries. In China, the test is in XiaoShan Airport of Hangzhou City in the Zhejiang Province.

The test includes an exit and entering evaluation, the compatibility test, and the biometric and digital signature verification. There is no information available about how long the test will take. ❖

Identity Theft On The Rise

Recent privacy invasions at ChoicePoint, payroll handler PayMaxx, Bank of America, Lexis Nexis, several universities, and a large shoe retailer called DSW all lost control of sensitive data concerning millions of people.

Credit card and other banking details, names, addresses, phone numbers, Social Security numbers, and dates of birth have fallen into the hands of potential identity thieves. Recent disclosures include:

- California State University at Chico notified 59,000 students, faculty, and staff that their details had been kept on a computer compromised by remote intruders.
- Boston College notified 120,000 of its alumni after a computer containing their addresses and Social Security numbers were compromised by an intruder.
- Shoe retailer DSW notified more than 100,000 customers of a remote break-in of the company's computerized database of 103 of the chain's 175 stores.
- Privacy invasion outfit Seisint, a contributor to the MATRIX government dossier system, now owned by Reed Elsiver, confessed to 32,000 individuals that its Lexis Nexis databases had been compromised.
- Privacy invasion outfit ChoicePoint confessed to *selling* the names, addresses and Social Security numbers of more than 150,000 people to criminals.
- Bank of America confessed to losing backup tapes containing the financial records of 1.2 million federal employees.
- Payroll outsourcer PayMaxx

(Continued on page 10, Col. 1 - ID Theft)

ID Theft

(Continued from page 9)

foolishly exposed more than 25,000 of its customers' payroll records on line.

- Desktop computers belonging to government contractor Science Applications International Corp (SAIC) were stolen, exposing the details of stockholders past and present, many of them heavy hitters in the US government.

- Cell phone provider T-Mobile admitted that an intruder gained access to 400 of its customers' personal information.

George Mason University confessed that a remote intruder had gained access to the personal records of 30,000 students, faculty, and staff.

While this is nothing new, there is an important observation here that's worth emphasizing: *none of these cases involved online transactions*.

Many people innocently believe that they're safe from credit card fraud and identity theft in the brick and mortar world. Nothing could be farther from the truth. The vast majority of incidents can be traced to skimming, dumpster diving, and just plain stupidity among those who "own" our personal data.
Only a small fraction of such incidents result from online transactions. Every time you pay by check, use a debit or credit card, or fill out an application for insurance, housing, credit, employment, or education, you lose control of sensitive data.

In the US, a merchant is at liberty to do anything he pleases with the information, and this includes selling it to a third party without your knowledge or permission, or entering it into a computerized database, possibly with lax access controls, and possibly connected to the Internet.

Sadly, Congress's response has been to increase the penalties for identity theft, rather than to regulate access to, and use of, personal data by merchants, marketers, and data miners. Incredibly, the only person with absolutely *no* control over the collection, storage, security, and use of such sensitive information is its actual owner.

For this reason, it's literally impossible for an individual to prevent identity theft and credit card fraud, and it will remain impossible until Congress sees fit to regulate the privacy invasion industry. ❖

BID

(Continued from page 1)

and from grade schools to universities are installing biometric systems.

In addition to profiles of suppliers, the Biometric Directory includes:

- A 22-page non-technical overview of biometric identification technology
- A 6-page product showcase featuring photos of biometric hardware
- A listing of 35 conferences and expositions worldwide where biometric technology is a major portion of the conference program

A 22-page Glossary of biometric terms and definitions

Features of BID include the sorting of biometric vendors by the types of biometrics they support.

A preview of the directory is available by going to the BID web site at:
http://www.biometricinfodirectory.com.

Information is available at the above web site or by contacting the Biometric Digest at P.O. Box 510047, St. Louis, MO 63150-0047 U.S. or e-mail to publisher@biodigest.com. Telephone information is available at 800-745-2455 in the U.S. or 314-892-8632. Fax is 314-487-5198. ❖

❖ Biometric Digest ❖

Biometric Digest™
published monthly since 1996 by
Biometric Digest
Division of William Rogers & Assoc., LLC
P. O. Box 510047
St. Louis, MO 63151-0047 USA
Tel: (314) 892-8632
Fax: (314) 487-5198
E-mail: publisher@biodigest.com
Internet: http://www.biodigest.com
http://www.biometricinfodirectory.com

Publisher — William Rogers
One-year subscription 12 issues
$290 in U.S. & Int'l via e-mail
$325 Paper
Subscription includes 52 weekly issues of **Biometric Media Weekly,** a summary of biometric news every week.

How To Order

Telephone
From the US -
1-800-745-2455
From outside US -
314-892-8632

Mail
Biometric Digest
P.O. Box 510047
St. Louis, MO
63151-0047
US

E-Mail
Publisher@biodigest.com

FAX
314-487-5198

Biometric Sites of Interest

http://www.biodigest.com
http://www.biometricinfodirectory.com
http://biometricdigest.blogspot.com

Just click to hyperlink to site.

Financial Reports

SAFLINK Corp. Raises $9.2 Million In Private Placement

SAFLINK® Corporation (NASDAQ: SFLK), a developer and integrator of biometric security solutions, announced that it has raised $9.2 million in a private placement of its common stock. The funds were raised through the sale of 3,080,000 shares of the Company's common stock to a group of institutional investors, including existing stockholders, at a per share price of $3.00.

SAFLINK(R) Reports Fourth Quarter and Fiscal 2004 Results

SAFLINK® Corporation (NASDAQ: SFLK), reported its financial results for its fourth quarter and fiscal year ended December 31, 2004.

Fourth Quarter Results Revenue for the fourth quarter of 2004 was $2.3 million, compared to $2.4 million for the third quarter of 2004 and $488,000 for the fourth quarter of 2003. The Company reported a net loss attributable to common stockholders of $6.6 million, or $0.08 per share, in the fourth quarter of 2004.

This is compared to a net loss attributable to common stockholders of $7.2 million, or $0.12 per share, in the third quarter of 2004, which included a $2.2 million non-cash charge related to the modification of warrants in connection with the Company's special warrant offer in July 2004, and a net loss attributable to common stockholders of $2.9 million, or $0.11 per share, in the fourth quarter of 2003.

More information is available at http://www.saflink.com.

Diaphonics Secures $3.5 Million Venture Financing

Diaphonics, Inc., a provider of security solutions based on voice verification, announced the completion of a $3.5 Million (CAD) round of financing. New investors Covington Capital and InNOVAcorp were joined by previous investors BDC Venture Capital (a division of the Business Development Bank of Canada) and Nova Scotia Business Inc. (NSBI). Diaphonics will use the new capital primarily to expand sales and marketing efforts.

Bioscrypt Inc. Cuts Q4 Loss to US$66,834 from Year-ago US$332,084

Identity verification technology firm Bioscrypt Inc. said recently it cut its loss in the latest quarter on better sales, including to a major U.S. airport.

The fourth quarter loss for Bioscrypt, which reports results in U.S. dollars, fell to $66,834, zero cents per diluted share, from a year-ago $332,084, or a penny per share. Revenue in the period ended Dec. 31 was $3.9 million, up 23 per cent from $3.2 million reported during the same period in the previous year.

Bioscrypt (TSX:BYI) has more than 70,000 fingerprint readers currently installed, with customers such as the U.S. Army, NASA, American Express, the New York Police Department, NATO and Continental Airlines.

The earnings announcement Thursday came a day after the Toronto company announced it had signed a deal to acquire Cognizance, a private California company, for at least $7 million US.

Cogent Systems Announces Record Fourth Qtr Revenues

Cogent Systems (Nasdaq:COGT) announced financial results for the fourth quarter and year ended December 31, 2004.

Fourth quarter 2004 net revenues were $31.8 million, which is a 36% sequential increase over net revenues of $23.4 million for the immediately preceding third quarter of 2004. Net income on a GAAP basis for the fourth quarter of 2004 was $9.9 million, or $0.11 per diluted share, which compares to GAAP net income of $20.4 million, or $0.29 per diluted share, for the third quarter of 2004.

Cogent's fourth quarter of 2004 GAAP results included $1.7 million of non-cash charges related to the amortization of stock-based compensation. Excluding the effects of stock-based compensation and using a 38% tax rate, non-GAAP net income was $10.0 million, or $0.11 per diluted share, compared to $6.9 million, or $0.10 per diluted share, for the immediately preceding period after excluding the effects of similar items and a net income tax benefit of $11.6 million.

ImageWare Systems Reports 2004 Fourth Quarter Results

Revenues for the quarter ended December 31, 2004 were $3.5 million compared to $3.4 million in the year ago quarter. The net loss for the fourth quarter was $0.9 million or $0.08 per share, compared with a net loss of $6.4 million, or $0.88 per share, for the same period a year ago. In the third and fourth quarter of 2003 the Company took actions to reposition our foreign sales offices in Germany and Singapore to lower fixed costs and pursue significant international ID pro-

(Continued on page 12, Col. 3 - Financial Rpts)

Verbatim

Quotes & comments from within the biometric industry

"What's missing is a plan. Biometrics companies are figuring out how to get into multimillion-dollar government contracts, but there's no vision for the future. There's still a huge gap out there, just waiting to be filled."

C. Maxine Most
Principal, Acuity Market Intelligence

"It looks like the Department of Defense sees the value in doing what the NIST thus far has not been prepared to do. Congratulations to John Woodward and his team."

Henry J. Boitel
boitel@MINDSPRING.COM

"The biometrics industry is no longer in its infancy. Vast changes in the marketplace are the driving forces for biometrics. Biometrics is becoming a billion dollar market. The marketplace is now fueling biometrics research."

Grant Evans, CEO
A4Vision

"Working with our DOD and U.S. government partners, DOD Biometrics has taken significant steps to improve our use of biometric technologies, particularly in supporting U.S. efforts in the global war on terrorism."

John Woodward
Director, Biometrics Management Office

"What I find interesting is the notion that government employees have rights to information to which us mere citizens are not privy. Egad."

Jack Ring
jring@AMUG.ORG

"I find the discussion on biometrics that require physical contact to be amusing. Those persons that report that they have reservations about putting their finger on a scanner or having any physical contact with biometric hardware must be forgetting that they are opening doors, using coins, shaking hands, using the telephone, drinking from beverage bottles or cans, and dozens of other daily tasks that require physical contact with objects that other persons have had physical contact. Sitting in a doctors waiting room and reading one of those magazines that have been touched by dozens of sick people before you is far more of a hygiene problem than physical contact with a sensor."

John Franks
btbs05@YAHOO.COM

"We've seen a lot of activity in the security market, ranging from government contracts to commercial building access to fingerprint scanning for PCs," said "We're seeing forecasts for 60 percent growth over the next five years. That's why there are so many companies getting into the market."

Wayne Meyer
Product-Marketing Manager
Analog Devices Inc.

"The biometric fingerprint sensors that used to cost $50 now cost less than $6," "That's one of the results of applying consumer math to biometrics."

Jim Burke
Vice President
AuthenTec Inc.

"One major trend in 2005 will be the use of fingerprint technology in combination with national identity cards."

Christer Bergman,
CEO/President
Precise Biometrics

Financial Rpts

(Continued from page 11, Col. 3)

jects utilizing the Company's software technologies as our primary differentiator. These offices had historically emphasized the resale of third party merchandise (hardware and consumables) which generated lower gross margins than software (as a percentage of revenue) and required significant fixed costs for sales, service and support. Revenues in the quarter from these two locations were $1.08 million below their levels in the same quarter of 2003. This decrease was offset by fourth quarter sales of the Company's IWS(TM) Biometric Engine software of approximately $978,000.

The loss from operations totaled $1,066,000 in the 2004 quarter as compared to $1,822,000 in the 2003 quarter. Gross margins were 58% of revenue in the quarter ended December 31, 2004 as compared to 43% for the same period last year. The improvement is reflective of higher gross margins resulting from product mix containing higher percentages of software in 2004 and reduced operating costs at our foreign sales offices. Cost cutting measures taken by the Company over the past year resulted in a decrease in overall operating expenses of $214,000 in the quarter compared to 2003. ❖

People In The News

Accu-Time Systems Hires Stephen G. Sardi

Accu-Time Systems announced the hiring of Stephen G. Sardi as Vice President, Engineering and Operations. Steve, who has ME and EE engineering degrees, will help oversee product development for the company. Steve comes to ATS from Datastrip Products, where his most recent position was Executive Vice President of Engineering Operations. ❖