

# BANK SECURITY NEWS

INSIGHTS ON CORPORATE AND INFORMATION SECURITY

WWW.ROYALMEDIA.COM

## NEWS INSIDE

### TECHNOLOGY

A smart card manufacturer unveils a product designed to ensure that online access to bank accounts is available only for legitimate accountholders  
page 3

XL Capital taps Voltage to beef up its email security measures  
page 3

### RULES & REGS

Arizona passes a law to facilitate the reporting and prosecution of cases of identity theft  
page 4

### PHISHING

The IRS is the latest target of an email phishing scam  
page 6

### SMART CARDS

Some technology vendors expect at least a five-year lag in smart card implementation by U.S. banks  
page 6

### DEPARTMENTS

Market Monitor  
page 5

Calendar  
page 5

Equities Monitor  
page 7

## BILL TO REGULATE ATMS ADVANCES IN CALIFORNIA

A bill that aims to stem fraud by regulating operators of automated teller machines advanced in the California Assembly on April 22. The progress has generated mixed reaction from industry players.

The bill, referred to as Assembly Bill 1810, passed the **Banking and Finance Committee** and was referred to the **Appropriations Committee**, where it is scheduled to be discussed on May 19. The bill must be passed by the assembly by May 28, or it will have to be reintroduced in the next legislative session.

The earliest Gov. **Arnold Schwarzenegger** could sign the bill into law would be late August or September, said a spokeswoman in the office of the California state legislature.

Introduced in January by State Assemblyman **Dario Frommer**, the bill establishes compliance, regulatory, and licensing standards and requires independent sales organizations to regulate non-bank ATMs. ISOs link non-bank ATMs to electronic funds transfer networks, thus enabling terminals to perform transactions.

For instance, the bill mandates that ISOs, or "operators" as the law refers to them, must verify ATM owners' federal and state tax-identification numbers and conduct background checks, among other things. Under the bill, ISOs must also ensure that non-bank ATM owners comply with local, state, and federal regulations.

There are currently 371,000 ATMs deployed in the U.S., according to *ATM and Debit News*. Of the \$1 trillion transacted at those ATMs last year, about \$50 million was stolen, according to the **Electronic Funds Transfer Association**.

Despite the proliferating fraud, some industry executives consider California's bill unnecessary.

"I think it attacks more the perception than the

## BANKS IN TALKS WITH MAGTEK FOR CARD VERIFIER

WASHINGTON, D.C. — A handful of banks, some of them perhaps among the nation's largest, have entered negotiations to buy fraud-protection technology aimed specifically at stemming the practice of "skimming" consumer information from automated teller machines.

The vendor, **MagTek Inc.**, is talking with the banks about implementing the anti-skimming product in the next five months, **Kiran Gandhi**, MagTek's vice president of business development, said at a recent industry conference here.

The move comes as ATM fraud becomes more sophisticated and banks are increasingly relying on technology to counteract it.

Skimming is a scheme in which fraudsters may affix a device to the card slot of an ATM to copy an accountholder's card data. Meanwhile, the fraudsters may mount a pinhole-sized camera near the ATM that records footage of the user entering his PIN code. A thief can then use this information to make a "magnetically altered," or counterfeit card, and drain the customer's bank account.

While Gandhi would not specify MagTek's potential clients, mega-lenders including **Bank of America Corp.**, **Citigroup Inc.**, and **J.P. Morgan Chase & Co.** are just a few of those whose customers' data has been "skimmed" in recent months. Both Citigroup and J.P. Morgan Chase are already MagTek clients, according to the vendor's web site.

MagTek's anti-skimming technology, called **MagnePrint**, consists of a reader that enables financial institutions to determine the legitimacy of a bankcard by analyzing the magnetic stripe on the back. Specifically, during a bankcard transaction, the MagnePrint reader sends the



Bank Security News is published by Royal Media Group  
1359 Broadway  
Suite 1512  
New York, NY 10018  
www.royalmedia.com  
2004 © Royal Media Group  
All rights reserved  
ISSN 1098-8335

Continued on page 2

Continued on page 2

## IN BRIEF

### CTST ISSUES HEALTH WARNING TO ATTENDEES

The lunch may have been free, but some attendees at Thomson Media's CardTech/SecurTech conference ended up paying for it in other ways.

Thomson, the event's organizer, discovered through questionnaires completed by attendees after the exhibition, that several people became ill while attending the conference, held April 26 to April 29 in Washington, D.C.

Thomson sent an email to exhibitors and attendees on May 10 informing them that the District of Columbia Department of Health was investigating several "possible cases of food-borne gastroenteritis among attendees of CardTech/SecurTech."

The DC DOH and the Centers for Disease Control and Prevention were "conducting an investigation to determine the source of this outbreak, with the goal of preventing additional illnesses," the release said.

Gastroenteritis is an infection caused by a variety of viruses that results in vomiting or diarrhea, according to medical web site WebMD.com, which did not have a listing for food-borne gastroenteritis.

Thomson did not release any details about the number of people who were infected or on which date the illnesses were contracted.

### MAGTEK, BANKS IN TALKS

*Continued from page 1*

financial institution not only account data, which is encoded in the card's magnetic stripe, but also a snapshot of the formation of the ferrous particles suspended in the stripe. The financial institution would then match the snapshot with a stored file detailing the card's particle formation. If the two pictures differ, the transaction would be denied.

The MagnePrint reader, developed last year, works with both credit card terminals and ATMs.

Although a cloned card bears the same data as a genuine one — enabling it to fool point-of-sale terminals and ATMs — it is virtually impossible for the bogus card to exhibit the same particle formation as the original, Gandhi said.

"The diameter of the magnetic particles is less than 1/100<sup>th</sup> of the diameter of a human hair," he said. "Each stripe has billions of particles from one edge of the card to the other, each with a unique shape and size. MagnePrint relies on one simple rule of nature: Nature doesn't make anything perfect."

A bank using MagnePrint's technology can make a "fingerprint" file of a card's particle formation either upon issuance of the card, or as a customer performs transactions with merchants or at ATMs.

In addition to the card readers, Carson, Calif.-based MagTek sells debit and credit terminals with the MagnePrint technology built in. MagnePrint can also be adapted for installation in ATMs. Remote readers, which attach to terminals, cost about \$60 each when purchased in quantities of at least 5,000, Gandhi said. Integrated units are cheaper, and the cost is less to install the technology in a debit or credit terminal than in an ATM, he said.

While the implementation may be smooth, one consultant wondered whether the industry would perceive the cost as worthwhile. "If you're talking about taking the new

reader and replacing the old ones, it's a stretch for the industry," said Bob Buccieri, senior consultant for the Electronic Funds Transfer Association.

### CALIF. ATM BILL ADVANCES

*Continued from page 1*

reality," said Bob Bucceri, EFTA's senior consultant. A bank is under great pressure to manage risk, so it aggressively checks independently owned ATM operators for fraud or criminal behavior, he said.

"Anyone who accesses regional or national networks has to either be a bank or go

through a bank. That bank is not going to give you a pass," said Bucceri. "That bank is going to do pretty serious due diligence to make sure that they're dealing with responsible parties."

Some ATM manufacturers are on the

opposite side of the debate, though. The history of fraud at independently owned ATMs indicates a need for regulations even tougher than those mandated in A.B. 1810, said Rob Evans, director of industry marketing at ATM manufacturer NCR Corp., Dayton, Ohio.

"At the moment, the attitude is, if you've got money, you're good to go," Evans said. "That is unconscionable and that cannot continue," he added, mentioning as an example the December arrest of Iljmija Frljuckic, a fraudster who stole \$3.5 million from 55 ATMs that he had purchased and installed himself.

"If you're going to operate an ATM, I don't think it's unreasonable to say that it needs to be licensed, and I don't think it's unreasonable to pay for that license, nor to submit to a background check, nor that anyone who is a convicted felon should be ineligible to own and operate an ATM," Evans said.

If ratified, the law would become effective on Dec. 31, 2005.

The legislatures in New Jersey and New York are at the early stages of drafting proposals to regulate independently owned ATMs, too.

## VENDOR OFFERS PRODUCT TO STEM ONLINE BANKING FRAUD

Smart card manufacturer **CardLogix** unveiled a fraud-prevention product late last month designed to ensure that online access to bank accounts is available only for legitimate accountholders.

In essence, the product, called **ATMobility**, curtails fraud by generating a unique password each time a bank customer attempts to gain access to his account online. Even if a fraudster gets hold of account information, without the ATMcard and reader, he can't access the account because the password is never the same twice.

ATMobility consists of an ATM card with an embedded microprocessor chip and a handheld card reader. Those two components work in tandem with a bank's web site and server — equipped with **CardAuth**, the software that powers the product. CardAuth runs on **Microsoft, Linux** and **Macintosh** operating systems.

Here's how it works: When an accountholder initiates the log-in process on his bank's web site, the bank's server sends a random eight-digit number that appears on the customer's browser window. The customer then activates the card reader by inserting his ATM card and entering his PIN. He then uses the reader's keypad to enter the number that appeared in his browser window. Simultaneously, the card and the bank's server perform an algorithm on the original number. They generate a six-digit figure that appears in the reader's LCD window, and which the user then enters into a field on his browser window. When he completes all the required fields, the figure he has entered is compared with the figure generated by the bank's server.

The cards perform the same algorithms automatically when inserted into properly equipped ATMs.

Banks can use ATMobility-generated numbers

as passwords or layer them with other identification factors like usernames and account numbers, for example.

CardLogix hopes to make waves in a niche of the bank security market that is in flux. Banks, such as **Citibank** and **Wachovia Corp.**, have changed their web log-in procedures in recent months to eliminate the PIN-code prompt. Instead, their web sites prompt customers for usernames and passwords in an attempt to impede fraudsters who may have stolen an accountholder's information, including PIN code, during a customer's ATM transaction, for example.

Several financial institutions have expressed interest in ATMobility, said **Emil Nastri**, a vice president of CardLogix. While no American financial institutions have agreed to use it as yet, some European banks, including **ABN Amro**, have implemented it. European banks are more "smart card-centric," Nastri explained.

ATMobility costs \$10 per reader for a minimum order of 250,000, Nastri said. For banks requiring fewer readers, the price is higher, he added, though he would not be more specific.

The product setup, which entails equipping bank servers with CardAuth and distributing the ATM cards and readers among accountholders, requires two to three months, Nastri said.

A lithium battery with a four-year life powers each card reader, Nastri said. The readers

measure two-and-three-eighths inches by four inches, and are three-eighths of an inch thick — or about the size of a pack of cigarettes.

Irvine, Calif.-based CardLogix, founded in 1994 as a research company, began manufacturing smart cards in 1998.

## XL AMPLIFIES EMAIL SECURITY WITH VOLTAGE PRODUCT

Insurer and financial service provider **XL Capital Ltd.** inked a deal with **Voltage Security Inc.** last month to simplify the security and technical maintenance of its internal email system to better comply with financial reporting and privacy regulations.

*Continued on page 4*

## STAFF

### BANKSECURITY NEWS

Jonathan S. Hornblass  
EXECUTIVE EDITOR  
hornblass@royalmedia.com

Jon Hendrix  
ASSOCIATE EDITOR  
jhendrix@royalmedia.com

Marcie D. Belles  
SENIOR EDITOR  
mdbelles@royalmedia.com

Mike Gibb  
Adelene Lee  
Vincent Ryan  
CONTRIBUTING EDITORS

Stephen Silver  
STAFF REPORTER  
ssilver@royalmedia.com

Ethan Byun  
PRODUCTION EDITOR  
ebyun@royalmedia.com

Danielle Cattani  
AVP, CONFERENCES  
dcattani@royalmedia.com

Meredith Krantz  
AVP, ADVERTISING  
mkrantz@royalmedia.com

Stephen Sullivan  
MARKETING MANAGER  
ssullivan@royalmedia.com

Claudia Peralta  
CUSTOMER SPECIALIST  
cperalta@royalmedia.com

*Bank Security News* is published every two weeks except in September and December, during which it is published monthly. Tax ID #13-3852425. Contact: Royal Media Group, 1359 Broadway, Suite 1512, New York, NY 10018. T: (212) 564-8972, F: (212) 564-8973. E: connect@royalmedia.com, www.royalmedia.com

2004 © Royal Media Group

### WARNING!

It is illegal to photocopy or reproduce any part of *Bank Security News* without the written consent of Royal Media Group. Call 212-564-8972 to obtain duplication rights.

Continued from page 3

The arrangement, which entails implementation of an identity-based encryption system, is part of a more sweeping effort by Hamilton, Bermuda-based XL Capital to migrate the email accounts of all 3,000 of its worldwide employees to a single platform, namely, Microsoft's Outlook 2002 Exchange 5.5. The move should also reduce costs for the company.

Requirements in the Sarbanes-Oxley Act and with European Union data-privacy laws spurred XL Capital's embrace of the new encryption system, said **Thomas Dunbar**, the company's global IT chief security officer.

"As an insurance company, and because it's our business to manage risk, we needed to manage our own risk with messages that were traveling through Outlook," Dunbar said. "We set a goal in 2003 to get everyone onto one email

platform to provide security — so they could live up to our policy, and so we had regulatory compliance and could send confidential email through the system."

XL Capital is the first financial services client for Voltage Security's identity-based encryption product.

In choosing identity-based encryption — as opposed to the more common and slightly more unwieldy public key infrastructure — XL has opted for one of the newer email-security methods available in the market.

Voltage's **SecureMail** product, and IBE in general, require fewer steps and less maintenance than PKI encryption. In a public-key-infrastructure system, each user has a public key and a private key.

The public key encrypts an email such that only the intended user may decrypt it. In turn, the recipient decrypts a message using a private key, or password. To receive PKI-encrypted email, users must file their public keys with a certificate authority, a third party that verifies the identities of emailers. Hassles with PKI can include inaccuracies in public-key listings or private keys lost by users. (The certificate authority electronically verifies a person's identity with the public key he has filed.) A sender must retrieve a recipient's public key each time he wants to email that person.

In identity-based encryption, an email address can serve as the public

key, thus eliminating the step of key retrieval from a certificate authority. Recipients store their private keys on a key server. Emails are then decrypted almost immediately upon arrival by a proprietary software program.

Voltage sells key servers for \$50,000.

"With Voltage, you didn't have all the overhead that comes with traditional PKI: the issuing of keys, maintaining revocation lists, registration authority, certificate authority," Dunbar said. "PKI requires a lot of external pieces. With Voltage, we can keep everything in-house. It's low overhead — one server. It's easy to issue keys, and easy to keep track of them. It's also extremely easy, if someone leaves the organization, to change the keys. We have very low overhead, and therefore the cost was less than what the PKI would cost."

XL expects to have all of its employees using IBE by July.

## RULES & REGS

### ARIZ. PASSES ID THEFT LAW

Arizona passed a law late last month to facilitate the reporting and prosecution of cases of identity theft.

Residents of the Grand Canyon State were the most likely U.S. citizens last year to be victimized by ID fraud, according to data from **Consumer Sentinel**, an online investigative database maintained by the **Federal Trade Commission**. Overall, 122.4 Arizonans per 100,000 were victimized by ID theft in 2003.

The new legislation, which Gov. **Janet Napolitano** signed into law on April 19, consists of two primary components. The first enables identity theft victims to report the fraud to local authorities, rather than tracking down officials in the jurisdiction in which the fraud occurred.

"This makes it easier to report crime" and to put investigations in motion, said Republican Rep. **Bob Robson**, the bill's sponsor.

The second component of the law allows prosecutors to litigate identity theft in a single jurisdiction, even if the crime occurred in more than one county. In the past, some cases in which identity fraud occurred across various jurisdictions were piecemealed out for trial in multiple courts.

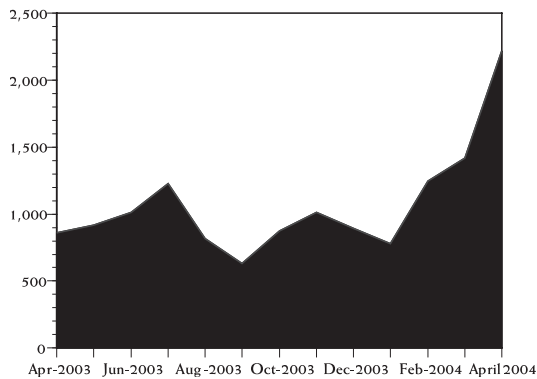
"Once a criminal has a credit card, we often see crimes being committed in multiple jurisdictions," Robson said. "This law allows the prosecutor to prosecute all elements of that crime whether it occurs in their jurisdictions or not."

Identity fraud continues to rise in the state. In 2003, 6,832 Arizonans reported some form of identity theft, 51% more than the 4,517 ID theft complaints filed the year prior, according to Consumer Sentinel. Of those victims, nearly 20% reported falling prey to multiple forms of ID

Continued on page 6

# MARKET MONITOR

## VIRUS & WORM TALLY\*



\*Reflects the number of worms, viruses, and "other malicious applications" for which Central Command updated its anti-virus software during a given month.

## THE 10 MOST COMMON VIRUSES

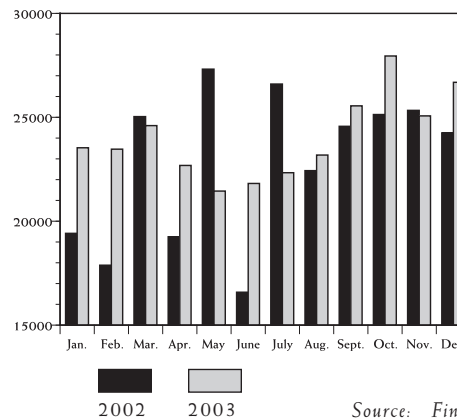
Viruses	% of Total, 4/04	% of Total, 3/04
Worm/Netsky.P	41.0	11.0
Worm/Netsky.D.DAM	12.4	—
Worm/Netsky.C	6.8	4.8
Worm/Netsky.B	5.1	16.3
Worm/Netsky.Q	4.5	0.8
Worm/Netsky.A	2.9	—
Worm/MyDoom.G	1.7	—
Worm/Netsky.Z	1.4	—
Worm/MyDoom.F	0.8	—
Worm/Netsky.A	0.6	—

Source: Central Command Inc.  
www.centralcommand.com

## SARS ON THE RISE

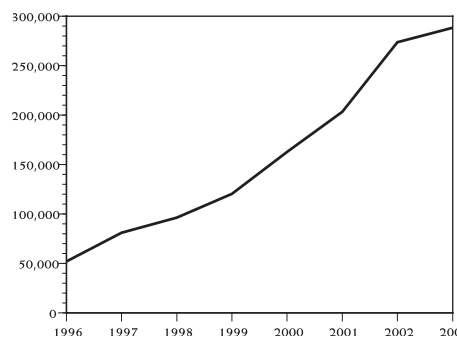
Banks filed 288,343 suspicious activity reports (SARs) in 2003, up 5% from 2002, according to data released earlier this month by the **Financial Crimes Enforcement Network**. SAR filings jumped nearly 10% — to 150,776 — in the final half of the year, from 137,567 in the first six months of 2003. FinCEN releases SAR data biannually in a report called *The SAR Activity Review*.

## SARs VOLUME BY MONTH



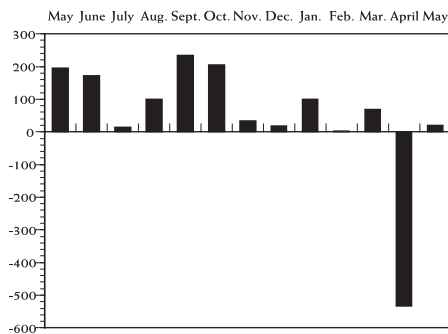
Source: FinCEN

## SARs VOLUME BY YEAR



Source: FinCEN

## SDNs ADDED IN PAST 12 MONTHS



Source: U.S. Treasury Department

The number of Specially Designated Nationals and Blocked Persons added to the **Treasury Department's Office of Foreign Assets Control** list, with whom the federal government forbids dealings by financial institutions, as of May 6.

The bar that plunges below the zero mark represents several hundred names removed from the list.

## CALENDAR

### June 7-9

Gartner IT Security, Washington, D.C.  
[www.gartner.com/us/itsecurity](http://www.gartner.com/us/itsecurity)

### June 9-11

IAPP TRUSTe Symposium: Privacy Futures, San Francisco.  
[www.privacyfutures.org](http://www.privacyfutures.org)

### June 13-17

Vanguard's Enterprise Security Expo, Reno, Nev.

[www.go2vanguard.com/expo/general\\_info.cfm](http://www.go2vanguard.com/expo/general_info.cfm)

### September 19-21

Thomson Financial's Identity Theft Symposium, Washington, D.C.  
[www.tmconferences.com](http://www.tmconferences.com)

### October 24-26

American Bankers Association's Money Laundering Enforcement, Arlington, Va.  
[www.aba.com/Conferences+and+Education/cc\\_money\\_laundering.htm](http://www.aba.com/Conferences+and+Education/cc_money_laundering.htm)

### October 26-28

IMN's Cyber Security in the Financial Services Sector Executive Summit, New York.  
[www.imn.org](http://www.imn.org)

### November 7-9

BITS Financial Servicing Outsourcing, Washington, D.C.  
[www.tmconferences.com/conferences/FSO03/index.html](http://www.tmconferences.com/conferences/FSO03/index.html)

## ARIZONA ID THEFT LAW

Continued from page 4

fraud. Nearly three quarters of the fraud occurred in Phoenix, which took the top spot in 2003 among the major metropolitan

areas with the highest per capita rates of ID theft, according to the Sentinel.

The new law becomes effective when the current legislative session ends, generally in late May.

**In 2003, 6,832 Arizonans reported some form of identity theft, 51% more than the 4,517 ID theft complaints filed the year prior.**

contact taxpayers by email," he said.

After the IRS discovered the web site and tracked down its host on the morning of April 30, the internet service provider complied with a

request to shut it down.

The IRS had not determined by press time how many people received or fell prey to the email.

The Federal Deposit Insurance Corp., another government agency, has been phished twice so far this year.

medical history, identifying physical information, important dates, and the like. A card that serves as a public transportation pass, a driver's license, and a credit card is an example of a multi-use smart card.

The infrastructure for smart cards is further along in Europe and Latin America, which have turned to the technology to battle fraud. By and large, U.S. financial institutions consider that the cost of replacing the magnetic stripe-verification system of credit and debit cards still outweighs the added security benefits that smart cards would provide. In the U.K., card fraud reached a record high in 2002, with \$747.6 million worth of phony transactions conducted, according to the Association for Payment Clearing Services (APACS), a U.K. trade group. That statistic compares with \$724.5 million of fraudulent transactions in 2001.

In 2003, though, when some U.K. banks began implementing smart card technology, the dollar amount of card fraud in Britain declined 5.2%, to \$708.5 million.

"It's probably too early in our rollout for us to claim [that the reduction in card fraud] is because of chip and PIN," the U.K. term for smart cards, said APACS spokesman **Mark Bowerman**.

Britain's banks plan to have smart cards distributed to all customers by January 2005. The cards will require users to enter personal identification numbers at the point of sale. Microchips embedded in the cards will make them more difficult to counterfeit.

While the financial services sector in America may be slow to adopt smart cards, other U.S. industries have jumped on the bandwagon, said **Dave Whitis**, a biometric consultant at Campbell, Calif.-based **Recognition Systems Inc.**, a unit of **Ingersoll-Rand**. For instance, the U.S. **Department of Defense** has issued more than four million smart cards, called Common Access Cards, to certain military members, civilian employees, and eligible contractors.

## PHISHING

### FRAUDSTERS TARGET IRS IN PHISHING ATTEMPT

Taxpayers should not generally dismiss communications from the **Internal Revenue Service** — unless they come in the form of an email.

Late last month, an unknown number of people received an email charging that they were subject to prosecution for alleged tax fraud. The email, which appeared to originate from the IRS and contained the subject line "problems with your tax," directed recipients to an official-looking web site. The site prompted visitors for names, addresses, phone numbers, Social Security numbers, mother's maiden names, driver's license information, bank names, credit card numbers, and checking account numbers.

The bogus web site "look[ed], at first glance, like it could be real," said IRS spokesman **John Lipold**. "Obviously, they did copy the graphic layout of some of our IRS pages."

Aside from the grammatical errors in the message, which should have tipped off recipients that something was amiss, the mode of communication should have served as a red flag, as well, Lipold said.

"As a matter of policy, the IRS does not

## SMART CARDS

### U.S. BANKS SHY AWAY FROM SMART CARDS

WASHINGTON, D.C. — U.S. banks and financial institutions will likely resist implementing smart card technology for at least five years, said vendors at an industry conference here late last month.

Before smart cards take hold among America's financial institutions, customers will need to be educated about the advantages of the product. Also, smart cards will need to offer multiple uses, said **Terry Conant**, executive vice president at Fullerton, Calif.-based **ID Tech**. The company, a manufacturer of magnetic stripe, smart card, and bar-code products, was one of hundreds of exhibitors at the CardTech/SecurTech conference.

"Banks really have to [initiate multiple-use cards], and banks are notoriously slow," Conant said. "They said two years ago they wanted to [begin using smart cards more], but they discovered how much it would cost. And customers don't want to pay \$5 for a card."

Smart cards, similar in size to credit cards, can store data, run applications, and process information. They can hold virtually any data, such as a patient's

# EQUITIES MONITOR

## RECENT PERFORMANCE OF PUBLICLY TRADED INFORMATION SECURITY COMPANIES

Company	Ticker	Price 05/5	Price 04/23	2-wk ch(%)	P/E	52-wk Hi	52-wk Lo	Shrs. Out.*	Market Cap	Avg Vol.
Alanco Technologies Inc	ALAN	1.25	1.58	-21.01	N/A	2.34	0.25	18,329	23.8M	1,066,272
Blue Coat Systems	BCSI	47.56	57.00	-16.56	N/A	65.71	5.08	10,459	409.1M	294,909
Brink's Co.	BCO	30.05	29.40	2.21	0.64	31.20	12.50	56,752	1.626B	274,363
Checkpoint Systems Inc.	CKP	16.25	16.62	-2.23	19.00	22.45	12.34	37,600	570.9M	250
Compudyne Corp.	CDCY	10.20	10.20	0.00	23.81	17.46	7.30	8,019	80.1M	92,666
Diversified Security	DVS	7.05	7.44	-5.24	N/A	9.00	5.26	5,131	570.9M	11,227
Entrust Inc.	ENTU	4.53	4.67	-3.00	N/A	5.70	2.40	63,567	297.5M	325,000
Honeywell International Inc.	HON	34.61	34.88	-0.77	21.75	37.65	23.27	859,196	29.5B	2,936,954
ICTS International NV	ICTS	4.14	4.64	-10.78	N/A	10.43	2.40	6,673	29.2M	274,863
International Electronics Inc.	IEIB	5.33	5.10	4.51	N/A	15.40	2.20	1,636	7.5M	164,863
Internet Security Systems	ISSX	13.96	14.75	-5.36	36.39	21.21	10.84	50,241	694.3M	928,681
Invision Technologies Inc.	INVN	49.67	49.57	0.20	33.55	50.50	22.02	17,452	866.6M	719,090
Kroll Inc.	KROL	30.25	27.90	8.42	26.00	30.60	18.30	39,955	1.183B	511,272
Lojack Corp.	LOJN	7.53	7.90	-4.68	0.19	9.90	4.57	15,104	113.6M	82,136
Magal Security Systems	MAGS	15.36	23.30	-34.08	45.45	40.35	4.77	8,199	111.3M	2,349,000
Markland Technologies Inc.	MRKL.OB	1.40	2.09	-33.01	N/A	5.00	0.69	7,840	10.2M	783,045
Napco Security Systems Inc.	NSSC	8.21	18.71	-56.13	64.15	11.60	3.30	6,908	54.7M	224,772
Network Associates Inc.	NET	17.00	19.04	-10.71	22.68	19.75	10.55	164,743	2.777B	1,952,818
Protection One Inc.	POIX.OB	0.33	0.40	-18.75	N/A	1.50	0.15	98,283	32.4M	37,818
RSA Security	RSAS	16.69	17.84	-6.45	51.97	19.48	9.18	61,760	1.021B	759,590
Safenet Inc.	SFNT	21.95	28.60	-23.25	45.49	44.50	21.35	23,769	546.9M	426,318
Universal Guardian Holdings	UGHO.OB	1.14	1.20	-5.00	N/A	2.27	0.09	27,435	23.1M	1,233,136

\*in thousands; greatest gainer by percentage change in box.

## BOARD OF ADVISORS

The Board of Advisors for *Bank Security News* provide insights and advice that help shape the scope and coverage of each issue.

CATHERINE A. ALLEN  
Chief Executive Officer  
BITS

PAT RUCKH  
Executive Vice President and  
Chief Technology Officer  
First Tennessee

ERIK STEIN  
Director, Fraud Prevention and  
Investigation  
Countrywide Home Loans

ABBY HOSSEIN  
Assistant Vice President,  
Enterprise Infrastructure  
Option One Mortgage

HERB SLATTERY  
Chief Information Officer  
Saxon Mortgage

KELLY WILLIAMS  
Chief Information Officer  
First Franklin Financial

SERGIO PIÑON  
Senior Vice President  
MasterCard

The opinions expressed in *Bank Security News* are not necessarily shared by the board members nor their employers.

To Register: Call 800.320.4418 Ext. 106 / Fax 309.414.6476  
email REGISTER@ROYALMEDIA.COM or log on to www.royalmedia.com

## The Pinnacle of Market Knowledge and Opportunity



Royal Media Group presents the Second Annual

# Home Equity Secondary Summit '04

Join the Nation's Top Home Equity Secondary Marketing Professionals at this Exclusive Industry Conference and Exhibition

- Uncover Winning Strategies for Taking Advantage of Current Market Conditions
- Meet Tomorrow's Secondary Marketing Challenges – Today!
- Find Out What Investors Want Now — and Why
- Explore the Latest Metrics for Benchmarking Your Performance
- Get the Scoop on Funding Strategies
- Learn How to Gain Advantage from Pricing Anomalies
- Explore the Economy's Effect on the Secondary Market
- Gain Insight from Real-World Portfolio Case Studies
- Fine-Tune Your Secondary Marketing Plan
- Determine Which Wall Street Conduits Will Last — and Which Won't
- Get Up-to-Date on Servicing-Related Litigation & Regulation
- Pinpoint Which Products Are Hot Today — and Which Will Be Hot Tomorrow
- Get the Early Warning on Tomorrow's Potential Blow-ups

July 11-13 2004  
at the Hyatt Regency Lake Tahoe Resort,  
Spa & Casino, Incline Village, NV



Keynote Speaker:  
Eric Billings, Co-Chairman & Co-CEO,  
Friedman Billings Ramsey Group Inc.

Presented by:

**RMG**  
ROYAL MEDIA GROUP

Sponsored by:

HOME EQUITY NEWS • COLLECTION TECHNOLOGY NEWS • **momentic**