

BANK SECURITY NEWS

INSIGHTS ON CORPORATE AND INFORMATION SECURITY

WWW.ROYALMEDIA.COM

NEWS INSIDE

VULNERABILITIES

FinCEN gets phished **page 2**

Hong Kong Financial Authority warns of fraudulent bank **page 2**

Banks meet to address vendor vulnerabilities, solutions **page 3**

COURTSIDE

More identity theft in Arizona, as two enter guilty pleas **page 3**

ONBOARD

IBM partners with Mantas to market banking-compliance and anti-fraud platforms **page 4**

MFS Investment Management taps Foundstone for network security **page 4**

TruSecure to provide network assessments for AIG cyber-risk policyholders **page 5**

FEATURE

Managing customer-identification programs under the U.S. Patriot Act, and "knowing your X" **page 8**

DEPARTMENTS

Calendar **page 4**

Market Monitor **page 6**

Equities Monitor **page 7**

RMG
ROYAL MEDIA GROUP

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

MYDOOM'S MONSTER SETS SITES ON MICROSOFT

Make way for the "DoomJuice" virus — a byproduct of the MyDoom worm that infected thousands of computers with malicious code weeks ago.

The main focus of the MyDoom attack, according to security experts, was to assemble an army of remotely-controlled "zombie" computers to facilitate a denial-of-service (DOS) on Lindon, Utah-based **SCO Group Inc.** SCO outraged Linux advocates last year, when it filed a lawsuit claiming proprietary rights to elements of that open-source operating system. A DOS attack is caused by thousands, even millions of requests for a web site that overwhelm the server and force it to shut down.

Linux proponents range from **International Business Machines (IBM)** to self-described anarchist virus writers. A cadre of the latter, it is widely assumed in the security industry, wrote MyDoom to exact revenge on SCO.

But MyDoom, it seems, now has other secret missions. One is to use your company's computers to launch a DOS attack on **Microsoft Corp.**

On Feb. 8, security firms around the globe discovered DoomJuice, a new virus that appears to have been written by the author of the MyDoom worm, according to a report by **Martin Reynolds**, vice president at **Dataquest Inc.**, a unit of **Gartner Inc.**

Doomjuice is creating zombies to launch a DOS on Microsoft, according to evidence gathered by Glendale, Calif.-based **Panda Software**, a virus-protection firm, which posted free digital vaccine for DoomJuice on its web site www.virusportal.com, on Feb. 9.

Though a virus, DoomJuice is designed to spread like a network worm, and is not visible to users via their email programs. It attacks computers through back doors implanted in them by the original MyDoom infection.

WORLD EXPERTS WORK TO MAKE MONEY-LAUDERERS WARY

MIAMI — Nearly 1,000 people from more than 50 countries, many wearing language-translation headsets that evoked images of a United Nations meeting, gathered to pore over America's anti-money-laundering (AML) regulations, which toughened in 2003 under the U.S. Patriot Act.

U.S. efforts to thwart anti-terrorist financing went global this month at the ninth annual International Money Laundering Conference and Exhibition hosted here.

An array of industry and government experts laid out the fundamentals for the AML-best-practices standards that are emerging internationally to fight corruption and other crimes, as well as to mitigate the heightened compliance exposures banks face today. Such practices range from filing suspicious activity reports (SARs) on irregular funds transfers to maintaining written comprehensive customer-identification programs to verify the identities and sources of income of a bank's account-holders.

"Our No. 1 priority should be to keep the bad money out of our institutions," **Richard Small**, managing director of global AML at **Citigroup**, told his peers during the opening panel discussion. But, he added, "we also have to have a reasonable approach to managing our AML and anti-terrorist financing risk."

Foreign attendees paid special attention to discussions on the "extraterritorial reach" of the Patriot Act, which allows the U.S. government to seize "dirty" money from accounts held in non-U.S. banks or, in some cases, even a foreign bank's American correspondent account.

Continued on page 2

IN BRIEF

FINCEN UPGRADES

MIAMI — The **Financial Crime Enforcements Network** (FinCEN) will implement new suspicious-activity-report (SAR) filing technology by the end of 2005, the agency's director, **William Fox**, announced Feb. 5

The new plan, dubbed "BSA Direct" by Fox, is expected to streamline the process under which banks must file SARs under the Bank Secrecy Act.

FinCEN will also introduce an electronic, and simplified SAR, "a SAR-EZ if you will," said Fox, to shorten the time it takes banks to file them and law-enforcement agencies to analyze them.

Under the plan the agency will replace its current SAR database, which is more than 10 years old, with a new platform.

The funds will come from a 12.7% budget increase called for by the White House last month.

ANTI-MONEY-LAUNDERERS MEET

continued from page 1

But whether they hailed from the tiny Pacific island nation of Narau or from the heartland of America, attendees with varying levels of expertise came to learn from one another.

Anna Weese, a certified bank auditor for **Wells Fargo Bank** with more than 20 years of experience, rubbed shoulders with newcomers like **Olga Kubas**, a native of Colombia and compliance officer in the U.S. office of **OrderExpress**, a Mexico-based money services business serving the Latin American immigrant community in Chicago.

"I love my job," said Kubas, who has worked with OrderExpress for two years. She described the great personal satisfaction she gets when she reports a suspicious transaction, and learns she has assisted law enforcement in locating criminals wanted for drug trafficking or other charges. "It is challenging," she added. "There is a lot to learn here."

Special Agent **William Harper** of the **U.S. Drug Enforcement Agency**, whose Miami field office works alongside banks to hunt down money-laundering narcotics traffickers, wanted to better understand the compliance challenges faced by his agency's private-sector partners. "I came to learn the banks' perspective of the laws and rules, and see what gripes they may have," he said. "It's been rather informative."

Vulnerabilities

FINCEN PHISHED

Criminals are impersonating the **Financial Crimes Enforcement Network** (FinCEN) in a new email fraud racket, the agency warned, Feb. 3.

In a spin on phishing schemes, in which email fraudsters masquerading as known, legitimate businesses send out mass emails in attempts to mine the personal information of the message's recipients, the FinCEN fraudsters are looking for cash, not data.

An unknown number of consumers have received a fraudulent electronic document labeled "anti-terrorist stop order," which purports to come from FinCEN's "European

Headquarters, Office of the Secretary Terrorist Investigations," in Geneva, Switzerland. No such office exists, according to FinCEN.

The fraudulent document tells recipients that the dollar amount of a recent bank transfer "exceeds the amount of money to be transferred within international monetary regulations," and that to complete the transaction, they must pay a \$25,000 fee for an "anti-terrorist certificate." The criminals' letter requests that wire-transfer payment information be faxed to FinCEN's "New York account."

FinCEN, the Treasury Department's criminal enforcement wing, is working with law enforcement to determine the origin of the fraud, and asks anyone who receives any similar attempts to obtain account information or funds, to notify them by email at webmaster@fincen.treas.gov.



This fraudulent "anti-terrorist stop order" appeared in email boxes around the world.

"BRITISH BANK" IS A FRAUD, SAYS HONG KONG BANK REGULATOR

A web site with the domain name www.facbltd.com is likely a fraud, the **Hong Kong Monetary Authority** warned in an alert issued late last month.

The web site purports to be for "**First Atlantic Chartered Bank Ltd.**," which claims to have a head office in the United Kingdom, and offer services throughout Hong Kong, China, and Singapore.

Visitors to the site are directed to open an account with a minimum deposit of £3,600 (\$6,700). The HKMA warns that no such bank is licensed to take deposits in Hong Kong and that no such bank is registered with the **Financial Services Authority** in the U.K.

A list of authorized financial institutions operating in Hong Kong, and law enforcement contacts for anyone taken in by this apparent scheme, are available at HTMA's website at www.hkma.gov.hk.

BANKS ADDRESS VENDORS' VULNERABILITIES

Software security holes that threaten the nation's critical infrastructures cost U.S. banks as much as \$1 billion annually, according to BITS and the Financial Services Roundtable.

At an invitation-only cybersecurity summit held Feb. 4 in Arlington, Va., the two industry groups called on vendors to meet the ISO 15408 security standard when developing software products for the financial industry. ISO 15408, also known as the "Common Criteria," is the information-technology security standard of the Geneva, Switzerland-based **International Organization for Standardization (ISO)**.

As well, vendors must strive to make patch-management more secure and less expensive, said the groups.

Responding to software vulnerabilities costs BITS and FSR members almost \$400 million a year, said **James E. Rohr**, chairman and chief executive of **The PNC Financial Services Group Inc.** and chairman of the BITS board of directors. BITS members, he said, hold about half of the nation's \$18 trillion in assets.

The summit, said BITS and FSR, was held to open the dialogue with vendors, rather than to point fingers.

"Financial institutions are ultimately responsible for ensuring the safety and soundness of financial services," said **Cathy Allen**, chief executive of BITS, and a member of the *Bank Security News* board of advisors. "We are working with vendors to see that the products offered to our members are safe and reliable, and will not burden companies with applying costly fixes."

Courtside

ARIZONA IDENTITY THIEVES PLEAD GUILTY IN FEDERAL COURT

Want more proof that Arizona is the identity theft capital of the U.S.?

A pair of Arizonans pled guilty to identity theft within two weeks of one another at a U.S. District Court in Phoenix.

The two pleas underscored that state's dubious claim to fame as the Grand Canyon of American ID theft. Arizona led the nation in per-capita incidents of ID theft in 2003, according to a recently released report from the **Federal Trade Commission**.

John Edward Christensen, 63, of Mesa, Ariz., pled guilty on Jan. 20 to one count of student aid fraud and one count of identity theft. From 1999 to 2003, according to the indictment, Christensen obtained more than \$300,000 in federally guaranteed student loans from various lenders using the personal information of 50 different individuals, mostly prison inmates serving long sentences.

Christensen's indictment sought forfeiture of more than \$58,000 from 10 bank accounts, \$11,600 in cash, a house, and a car — all alleged to be proceeds of the scheme to defraud. The names of the banks being used were not announced.

Christensen was caught on Sept. 2, when a staff member at the Mesa Community College financial aid office recognized him as the same person who had claimed an aid check under a different name. Christensen fled the scene but was captured by campus security and Mesa Police.

An investigation determined that Christensen had applied for student loans under six different names at three local colleges. He faces a maximum penalty of five years imprisonment and a \$20,000 fine for the charge of student-aid fraud. A conviction for ID theft carries a maximum penalty of 15 years in prison and a \$250,000 fine. Sentencing is scheduled for March 22.

Less than two weeks after Christensen's court date, **Dorothea Lewis Oien**, 54, formerly of Phoenix, but currently living in Raleigh, N.C., pled guilty to misuse of a Social Security number and other fraud charges.

Oien used eight different names, two dates of birth, and two Social Security numbers to finance the purchase of five different vehicles in a nine-month period, according to the complaint. Oien's fraudulent credit accounts totaled more than \$200,000. The names of the defrauded lenders were not made public.

Oien faces a maximum penalty of five years and a \$250,000 fine. She is scheduled to be sentenced April 19.



James E. Rohr, Chairman
PNC Financial Services

STAFF

BANKSECURITY NEWS

Jonathan S. Hornbliss
EXECUTIVE EDITOR
hornbliss@royalmedia.com

Michael Juhre
ASSOCIATE EDITOR
mjuhre@royalmedia.com

Mike Gibb
SENIOR EDITOR
mgibb@royalmedia.com

Jon Hendrix
Adelene Lee
CONTRIBUTING EDITORS

Ed Jennett
STAFF REPORTER
ejennett@royalmedia.com

Danielle Cattani
AVP, CONFERENCES
dcattani@royalmedia.com

Meredith Krantz
AVP, ADVERTISING
mkrantz@royalmedia.com

Jean Gazis
MARKETING MANAGER
jgazis@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.

CALENDAR

February 23-27

RSA Annual Conference, Moscone Center, San Francisco.
www.rsaconference.com

March 21-25

CISO Executive Summit (March 21) and InfoSec World Conference and Expo 2004 (March 22-25), The Rosen Centre Hotel, Orlando.
508-879-7999 or
www.misti.com

March 24-26

American Bankers Association/*Foreword Financial Bank* Technology Convention, Renaissance Orlando Resort at Seaworld.
www.aba.com

April 1-9

SANS 2004 Information Security Mega Conference, Walt Disney World, Orlando
www.sans.org/sans2004

April 19-21

SearchSecurity.com's Information Security Decisions, Hilton New York.
www.infosecurityconference.com

April 26-27

Financial Fraud Forum, The Omni Colonnade Hotel, Miami.
www.frallc.com

April 26-29

CardTech/SecurTech Conference and Expo, Washington Convention Center.
www.ctst.com

On Board

IBM PARTNERS WITH MANTAS FOR MUTUAL FUND CLIENTS

MIAMI — **International Business Machines** and **Mantas Inc.**, a provider of compliance-software services for the financial service industry, have agreed to jointly market and support compliance technology and services to financial institutions.



The partnership allows IBM clients to use their existing IBM systems to integrate Mantas banking-compliance software, including anti-money laundering and fraud-detection platforms.

The two companies will also offer investment-broker surveillance and trading compliance platforms to mutual fund companies to help them detect late-trading and market-timing violations and to avoid the regulatory pitfalls that were highlighted by the recent wave of mutual fund scandals.

"Clearly it's time for a thorough review of how regulators and the industry harness technology to detect and deter abusive and illegal behaviors," said **Nancy Smith**, a securities consultant to Mantas and former regulator with the **Securities and Ex-**

change Commission. "Advanced technologies may very well result in the better enforcement of existing rules and limit the need to adopt reforms that lead to more complex and costly rules."

Mantas's compliance products are currently used by **Citibank**, **ABN Amro**, and **Merrill Lynch**, among others. IBM also provides technology services for Merrill, as well as for numerous other financial services clients, including **AXA Group** and **Bank of Tokyo-Mitsubishi**.

Terms of the deal were not disclosed.

MFS INVESTMENT MANAGEMENT CHOOSES FOUNDSTONE

Boston-based **MFS Investment Management**, a mutual fund and financial services firm, has chosen Mission Viejo, Calif.-based **Foundstone Inc.** to secure its networks from attack, the company announced, Jan. 20.

MFS implemented Foundstone Enterprise Risk Solutions to replace a maze of off-the-shelf and home-grown network security applications that had become too slow, cumbersome, and resource-intensive, said **Tom Clark**, MFS's vice president of corporate systems security.

Foundstone ERS detects, inventories, and

Continued on page 5

Board of Advisors

The following executives comprise the Board of Advisors for *Bank Security News*. Their insights and advice help shape the scope and coverage of each issue.

CATHERINE A. ALLEN
Chief Executive Officer
BITS

ALLAN LUBITZ
Chief Information Officer
Option One Mortgage

SERGIO PIÑON
Senior Vice President
MasterCard

PAT RUCKH
Executive Vice President and Chief Technology Officer
First Tennessee

HERB SLATTERY
Chief Information Officer
Saxon Mortgage

ERIK STEIN
Director, Fraud Prevention & Investigation
Countrywide Home Loans

KELLY WILLIAMS
Chief Information Officer
First Franklin Financial

The opinions expressed in *Bank Security News* are not necessarily shared by the board or its individual members.

Continued from page 4

prioritizes all assets on a computer network, including custom web applications and wireless access points, then conducts a high-speed vulnerability assessment.

"Initially overwhelmed by [the number of] vulnerabilities reported, we found that Foundstone's prioritization of vulnerabilities by criticality enabled us to direct resources to the most important network elements first," said **Mark Turner**, senior security architect for MFS, in a statement. "Now we can remediate vulnerabilities that affect mission-critical systems much faster; our response time has been reduced from months to hours."

Foundstone experts have managed information technology security risks for a host of financial firms, including **Merrill Lynch**, **Salomon Smith Barney**, and **Instinet Group Inc.**, a New York-based institutional investment brokerage.

AIG PARTNERS WITH TRUSECURE FOR SECURITY ASSESSMENTS

Some cyber-risk insurance policy holders now have another company to access for a second opinion about their security procedures.

AIG eBusiness Risk Solutions, a unit of **American International Group Inc.** announced a partnership with network-security risk-management services provider **TruSecure Corp.**, on Feb. 4.

AIGeBRS underwrites insurance for network hacking attacks, electronic identity theft, and other computer-related risks.

Through the new partnership, AIGeBRS customers will receive discounts on TruSecure's comprehensive information security audits and business vulner-

ability assessments.

"TruSecure helps organizations develop and maintain a healthier security posture, while reducing overall security risk," said **Robert Parisi**, senior vice president and chief underwriting officer for AIG eBusiness Risk Solu-

tions, in a statement. "Together, we are offering companies a way to reduce their information security risk, while also protecting against the potential financial losses resulting from

a cyber-attack."

Herndon, Va.-based TruSecure, provides products and services to banks, including Denmark's **Danske Bank**, as well as to other financial services technology providers, like Brookfield, Wisc.-based **Fiserv**. AIGeBRS maintains partnerships with a number of security-audit and assessment firms, including **Qualys**, **Unisys**, and **Computer Associates**.



Call us today at (212) 366-8686 for a FREE consultation on your current technology environment. Learn how the right solutions can make you money by saving money and working smarter.

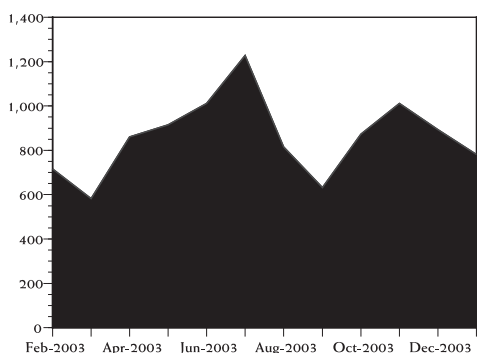
www.comgroup-inc.com



T Services >Networking >Project Management >Outsourcing >Firewalls >Desktop Support >De
Installation >Structured Cable >Telecommuter >Maintenance >WAN >LAN >Client/Server >ACD
Turnet >Unified Messaging >Security >Disaster Recovery >VOIP >Remote Office >Telecommunic
Data Communications >Maintenance >Help Desk Functions >VPN >Internet >Network Monitoring
T Services >Networking >Project Management >Outsourcing >Firewalls >Desktop Support >De
Installation >Structured Cable >Telecommuter >Maintenance >WAN >LAN >Client/Server >ACD
Turnet >Unified Messaging >Security >Disaster Recovery >VOIP >Remote Office >Telecommunic
Data Communications >Maintenance >Help Desk Functions >VPN >Internet >Network Monitoring
T Services >Networking >Project Management >Outsourcing >Firewalls >Desktop Support >De
Installation >Structured Cable >Telecommuter >Maintenance >WAN >LAN >Client/Server >ACD
Turnet >Unified Messaging >Security >Disaster Recovery >VOIP >Remote Office >Telecommunic

Market Monitor

VIRUS & WORM TALLY*



Source: Central Command Inc., www.centralcommand.com

*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, 1/04	% of Total, 12/03
Worm/MyDoom.A	77.4	—
Worm/Sober.C	5.9	1.9
Worm/Bagle.A	2.0	—
Worm/MiMail.I	1.7	12.8
Worm/Gibe.C	1.5	21.4
Worm/Klez.E (& G)	1.3	—
Worm/MiMail.J	1.1	12.8
Worm/BugBear.B	0.7	5.2
Worm/MiMail.A	0.5	3.7
Worm/Dumaru.A	0.5	—

THE 10 MOST COMMON VULNERABILITIES AND EXPOSURES (CVE)

TITLE	CVE ID#
1. Microsoft IIS CGI Filename Decode Error Vulnerability	CVE-2001-0333
2. Microsoft IIS Malformed HTR Request Buffer Overflow Vulnerability	CVE-2002-0071
3. Apache Chunked-Encoding Memory Corruption Vulnerability	CVE-2002-0392
4. Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability	CAN-2003-0109
5. Sendmail Address Prescan Possible Memory Corruption Vulnerability	CAN-2003-0161
6. Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	CAN-2003-0352
7. Microsoft Windows DCOM RPCSS Service Vulnerabilities	CAN-2003-0528
8. Microsoft Messenger Service Buffer Overrun Vulnerability	CAN-2003-0717
9. Microsoft Windows RPCSS Code Execution Variant Vulnerability	CAN-2003-0813
10. Writeable SNMP Information	No CVE assigned

Source: Department of Homeland Security. For detailed information on CVEs, visit <http://cve.mitre.org>

REPORTED PHISHING AND SPOOFING SCAMS IN 2004

DATE	COMPANY	EMAIL SUBJECT HEADER
Feb. 11	ibillingservices.com	"We have problems with your order."
Feb. 10	Fleet Bank	"Regular Fleet bank verification of the account"
Feb. 9	Bendigo Bank	"Bendigo Bank updates"
Feb. 7	e-gold	"Notification of e-gold account update"
Feb. 2	Shadowcrew	"Your card has been billed for \$149.95"
Jan. 30	Earthlink	"Urgent notification for xxx"
Jan. 23	FDIC	"Important News About Your Bank"
Jan. 22	Visa	"Visa Security Update"
Jan. 10	Citibank	"CITIONLINE EMail Veerification-name@domain.com"
Jan. 8	AT&T	"Billing Update Requested (URGENT)"

Source: Anti-Phishing Working Group

OFAC TERRORIST LIST

ADDITIONS

The Treasury Department's Office of Foreign Assets Control (OFAC) publishes a list of Specially Designated Global Terrorists, or SDGTs, with whom the federal government forbids dealings by financial institutions. SDGTs added between Jan. 29 and Feb. 13, 2004:

The following "SDGT" entries have been changed:

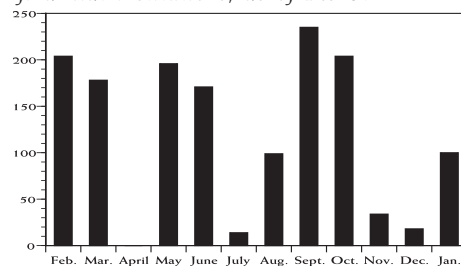
Army of Mohammed (a.k.a. Jaish-i-Mohammed; a.k.a. Jaishe e-Mohammed; a.k.a. Khudamul Islam; a.k.a. Khuddam-ul-Islam; a.k.a. Kuddam e Islami; a.k.a. Mohammed's Army; a.k.a. Tehrik ul-Furqaan); a.k.a. Kuddame Islami; a.k.a. Mohammed's Army; a.k.a. Tehrik ul-Furqaan), Pakistan

Jaish-i-Mohammed (a.k.a. Army of Mohammed; a.k.a. Jaish-e-Mohammed; a.k.a. Khudamul Islam; a.k.a. Khuddam-ul-Islam; a.k.a. Kuddame Islami; a.k.a. Mohammed's Army; a.k.a. Tehrik ul-Furqaan), Pakistan Jaishe e Mohammed (a.k.a. Army of Mohammed; a.k.a. Jaish-i-Mohammed; a.k.a. Khudamul Islam; a.k.a. Khuddam-ul-Islam; a.k.a. Kuddam e Islami; a.k.a. Mohammed's Army; a.k.a. Tehrik ul-Furqaan), Pakistan

Jaish-e-Mohammed (a.k.a. Army of Mohammed; a.k.a. Jaish-i-Mohammed; a.k.a. Khudamul Islam; a.k.a. Khuddam-ul-Islam; a.k.a. Kuddam e Islami; a.k.a. Mohammed's Army; a.k.a. Tehrik ul-Furqaan), Pakistan Khudamul Islam (a.k.a. Army of Mohammed; a.k.a. Jaishe E-Mohammed; a.k.a. Khuddam-ul-Islam; a.k.a. Kuddam e Islami; a.k.a. Mohammed's Army; a.k.a. Tehrik ul-Furqaan), Pakistan

SDGTs ADDED IN PAST 12 MONTHS

The number of Specially Designated Global Terrorists added to the Treasury Department's Office of Foreign Assets Control (OFAC) list, with whom the federal government forbids dealings by financial institutions, as of Feb 9.



Source: U.S. Treasury Dept.

Equities

RECENT PERFORMANCE OF PUBLICLY TRADED INFORMATION SECURITY COMPANIES

Company	Ticker	Price 1/29	Price 1/15	2-wk ch(%)	P/E	52-wk Hi	52-wk Lo	Shrs.Out.*	MarketCap*	Avg Vol.
Alanco Technologies Inc	ALAN	0.89	0.98	-9.18	N/A	1.29	0.23	15,262	14,957	55,944
Blue Coat Systems	BCSI	30.51	24.62	23.92	N/A	31.80	4.48	10,459	257,501	136,700
Brink's Co.	BCO	26.13	23.80	9.79	76.9	26.24	12.36	54,253	1,291,221	250,700
Compudyne Corp.	CDCY	11.41	11.25	1.42	30.03	13.19	4.80	7,970	89,663	104,500
Checkpoint Systems Inc.	CKP	19.43	19.98	-2.75	23.13	22.45	8.66	34,500	689,310	306,600
Diversified Security Solutions	DVS	6.23	5.87	6.13	N/A	7.70	5.26	5,150	30,231	7,100
Entrust Inc.	ENTU	5.25	5.04	4.17	N/A	5.70	2.25	63,526	320,171	625,000
Honeywell International Inc.	HON	36.95	36.4	1.51	N/A	37.65	20.20	862,051	31,378,656	4,450,000
ICTS International NV	ICTS	3.36	3.13	7.35	N/A	6.20	2.40	6,513	20,386	16,400
International Electronics Inc.	IEIB	3.65	3.50	4.29	N/A	4.10	2.15	1,631	5,709	1,600
Invision Technologies Inc.	INVN	38.39	36.45	5.32	7.35	38.98	19.82	17,030	620,744	432,000
Internet Security Systems	ISSX	18.29	17.79	2.81	46.9	21.21	9.85	49,840	886,654	1,240,000
Kroll Inc.	KROL	24.92	25.94	-3.93	24.19	28.99	16.35	41,791	1,084,059	512,200
Lojack Corp.	LOJN	8.70	8.43	3.20	21.22	9.90	4.49	14,856	129,247	50,200
Magal Security Systems	MAGS	8.65	7.78	11.18	36.04	9.97	4.60	7,930	68,595	23,800
Markland Technologies Inc.	MRKL.OB	2.1	1.85	13.51	N/A	31.00	1.63	6140	12,894	26,200
Napco Security Systems Inc.	NSSCE	8.29	7.45	11.28	33.16	9.75	6.60	3,210	26,611	8,700
Network Associates Inc.	NET	17.42	17.10	1.87	43.55	18.90	10.42	161,439	2,812,267	2,270,000
Protection One Inc.	POIX.OB	0.67	0.35	91.43	N/A	1.63	0.15	98,283	65,850	65,000
Rainbow Technologies Inc.	RNBO	15.31	14.55	5.22	N/A	15.48	6.00	26,814	410,522	278,900
RSA Security	RSAS	17.44	16.35	6.67	72.67	17.60	5.21	60,184	1,049,609	688,600
Safenet Inc.	SFNT	41.21	38.85	6.07	46.84	44.50	15.60	13,273	546,980	272,500
Silent Witness Enterprises Ltd.	UGHO.OB	1.57	0.44	256.82	N/A	3.15	0.09	20,990	32,954	1,200,000
Universal Guardian Holdings	VRSN	18.33	16.84	8.85	N/A	21.09	6.55	241,980	4,435,493	2,980,000

* in thousands

RECENT OFAC CIVIL PENALTIES ISSUED AGAINST BANKS (AS OF 02/06/04)

Institution	Location	Year(s) of Offense and Description	\$ Amount
American Express Bank Ltd.	New York	2000 Kosovo Funds transfer	3,291
American Services	Los Angeles	2000 Shipment to Cuba and funds transfer	4,236
Bank of America	Concord, CA	2001-2002 funds transfers and operation of account for a Sudan & Foreign Narcotics Kingpin (SFNK)	13,573
Bank One	Chicago	2002-2003 Iran & Sudan funds transfers	6,682
Barclays Bank Plc	New York	2003 Libya funds transfers	14,970
Bank of New York	New York	1998, 2000, 2001 Cuba, Libya & Sudan funds transfers	34,623
Bank of New York	New York	2000-2002 Libya funds transfers	27,500
Bank of New York	New York	2002 Unblocking of blocked Yugoslavian (Kosovo)	5,500
Columbia Bank	Tacoma, WA	2002 Cuban funds transfer	1,000
Commerzbank AG	New York	2002 Sudan funds transfer	5,500
Deutsche Bank	New York	2003 Libya funds transfer	5,500
Deutsche Bank	New York	2002 Sudan funds transfer	5,500
JP Morgan Chase	New York	2001, 2003 Libya funds transfers	26,980
M & T Bank	Buffalo, NY	2000 Kosovo funds transfer	2,250
Mellon Investor Services LLC	Ridgefield Park, NJ	2000 Issuance of checks to Cuba, Iran, N. Korea, Sudan, Yugoslavia	3,673
Mellon Bank N.A.	Pittsburgh, PA	2000 Kosovo funds transfer	10,400
Union Bank of Florida	Ft. Lauderdale, FL	1999 Cuba funds transfer	1,950

BANKS FIND PATRIOT ACT COMPLIANCE LESS TRYING

MIAMI — Compliance officers, sweating bullets over whether their customer-identification programs (CIP), required since last October under the U.S. Patriot Act, will pass their regulators' sniff-tests, can calm down. It's nothing to panic about, according to a panel of anti-money-laundering experts, speaking at an industry conference here earlier this month.

"There has been a lot of misplaced hysteria over [section] 326," said **Susan Galli**, senior anti-money laundering coordinator at Citigroup. She was referring to section 326 of the Patriot Act, which formalizes elements of the "know your customer" (KYC) maxim followed by major banks around the world, by requiring financial institutions to have a written CIP. The programs are designed to help banks eliminate illegal financial transactions by better scrutinizing the actions and identities of their account-holders.

"I, too, was part of that hysteria around 'what are we going to do?'," said **Daniel D. Soto**, anti-money-laundering compliance executive for **Bank of America Corp.**, and co-chairman of the association of **Certified Anti-Money Laundering Specialists (CAMS)**. "But one of the things we learned going through the CIP process was that we were in pretty good shape already."

BofA, Soto said, is currently undergoing a CIP examination by the **Office of the Comptroller of the Currency**, its primary regulator. "We have learned that the regulators don't only want to hear from us in the compliance area on how we're doing," said Soto, a former bank examiner for the **Federal Deposit Insurance Corp.** "They also want to talk to our lines of business, because ultimately they are the ones who have to answer the questions on how they are

implementing these procedures. But so far we've found their questions very reasonable."

John Byrne, director of regulatory compliance for the **American Bankers Association**, agreed with Galli, saying that he has never received so many questions from compliance officers about a specific issue in his 20 years in the industry. Most questions, Byrne said, deal with the minutiae of banks' written CIP procedures, especially over the wording in Section 326 that require them to "verify" their customers.

"It is not an authentication requirement," said Byrne, referring to the verification clause. Financial institutions, he said, are not required to validate the authenticity of passports, drivers licenses, or other documents provided by new customers opening accounts.

Rather, banks must only require that customers provide reasonable evidence of their identities.

"Don't make [your CIP] out to be more complicated than it needs to be," said Byrne, who, as an ABA lobbyist, worked with legislators when they drafted the Patriot Act.

Congress, he said, intended the rule to simply reflect practices most U.S. banks already undertake: having written account-opening procedures that diligently attempt to ensure that customers are who they say they are, and the source of their funds reasonably accounted for, Byrne said.

But, while banks can breathe a sigh of relief with such news, Byrne stressed that the 326 CIP provisions do not replace the KYC procedures, required in the Bank Secrecy Act long before it was amended under the Patriot Act in response to the events of Sept. 11.

Those procedures include identifying the

sources of income for their account-holders, and recognizing deposits or withdrawals outside the normal pattern for those customers.

"If you come up with some information that suggests identity theft, bank fraud, or some other way [the customer is using] information for illegal purposes, you can't ignore that simply because it's not a 326 requirement, said Byrne. You still have to deal with suspicious-activity reporting; you still have to deal with due diligence, just not under the rubric of 326."



John Byrne
American Bankers
Association

More importantly, said **Izzidin Hussein Razem**, a management

consultant and former compliance officer for Jordan-based **Arab Bank Plc**, as cross-border commerce increases in the emerging global economy, banks need to know more than just their customers.

"We started with 'know your customer,'" said Razem. "But we have to go beyond that. Know-your-staff, know-your-correspondent bank, know your customers' customers. Now, we're talking about know-your-'X' actually," with 'X' representing any person or entity that comes in contact with your organization.

Most large, international banks are beginning to mirror this in their policies not just in the U.S., but across all their operating units worldwide. Citigroup, for instance, enforces the CIP program it designed as required under the Patriot Act to all of its subsidiaries and operating units.

"KYC rules do not apply necessarily to a banks operations outside the United States," said Citigroup's Galli. "But I think there is an expectation from the regulators on a safety and soundness perspective, that large organizations are willing to apply consistent standards globally."



Daniel D. Soto
Bank of America