

# BANK SECURITY NEWS

INSIGHTS ON CORPORATE AND INFORMATION SECURITY

WWW.ROYALMEDIA.COM

## NEWS INSIDE

### RULES & REGS page 3

Details on the tough new Canadian privacy law.

### PEOPLE SCAN page 6

William D. Langford named FinCEN senior policy advisor.

### RULES & REGS page 7

CAN-SPAM becomes law; Hong Kong regulator identifies fraudulent Swiss bank.

### RUMBLINGS page 8

Bank of England latest U.K. financial institution to get phished.

### TECH BYTES page 8

National City taps Diebold for secure ATM upgrade.

## DEPARTMENTS

Calendar page 3

Market Monitor page 4

Equities Monitor page 5

## BSN BOARD PROJECTS GREATER SECURITY SPENDING IN 2004

Managers will be banking on security in the coming year.

"We are doubling our security budget in 2004," said **Kelly Williams**, chief information officer at **First Franklin Financial Corp.**, a wholesale mortgage lending unit of Cleveland-based **National City Corp.**, during a conference call with members of the *Bank Security News* Board of Advisors on Jan. 12.

Others echoed the sentiment, and some added that institutions are beginning to break such costs out in more detail. "Before, you didn't have individual line items for employee education and identity theft," said **Erik Stein**, senior vice president and director of fraud prevention and investigation for **Countrywide Home Loans Inc.**, of Calabasas, Calif. "You'll see that more."

"I agree," chimed in **Herb Slattery**, CIO at Glen Allen, Va.-based **Saxon Mortgage**. "We are itemizing those to bring an awareness [to senior management] of what we're spending the dollars on," said Slattery, adding that Saxon, too, will double its security budget in 2004.

Executives are changing their views of security costs as well, said the group. As banks are held to increasingly higher standards by customers concerned over privacy and identity theft issues, "there is more of an awareness that security will become a customer-relationship issue," said **Catherine A. Allen**, chief executive officer of **BITS**, a Washington, D.C.-based financial services trade group that focuses on technology issues.

Indeed, **Citibank** recently introduced its **Citi Identity Theft Solutions**, a free identity support program for its credit and debit card members. The bank launched a massive advertising campaign to leverage the service — which helps cardmembers who are

## LATEST LAPTOP THEFT CEMENTS WELLS MODEL AS RESPONSE STANDARD

After a laptop with 43,000 of its consumers' contact information and Social Security numbers was stolen, **Bank Rhode Island** has adopted **Wells Fargo & Co.**'s model for responding to such a theft and proactively contacted each of the victims.

BankRI's actions firmly place the Wells Fargo approach as the preferred method among banks for addressing incidents of stolen customer information.

"Our reaction would not have been different" with regard to immediately announcing the theft, said **Jim DeRentis**, BankRI's executive vice president for retail banking and marketing. "We believe full disclosure is the right thing to do. But Wells Fargo went above and beyond what they had to do [by law], and we saw that as a very good model."

Only weeks earlier, Wells Fargo sent thousands of letters to its own customers, after a stolen computer left its customers' personal information exposed.

In this case, BankRI's customer information was housed on a laptop belonging to **Fiserv**, a third-party technology contractor. The laptop was stolen last month.

BankRI's data was password-protected, but not encrypted, according to **Fiserv**, based in Brookfield, Wis. The computer may also have contained about 80 BankRI account numbers, though not in conjunction with names or other identifying information.

Evidence at the crime scene suggested the computer was stolen for its hardware, rather than the data contained within, according to executives at **Fiserv** and **BankRI**. They declined to provide further details, including the location of the theft, to avoid potentially informing the thief that the

**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

Continued on page 2

Continued on page 3

# Outlook

## BANKSECURITYNEWS

a Royal Media Group publication

Michael Juhre  
ASSOCIATE EDITOR  
mjuhre@royalmedia.com

Mike Gibb  
SENIOR EDITOR  
mgibb@royalmedia.com

Jon Hendrix  
Adelene Lee  
Myra Patridge  
CONTRIBUTING EDITORS

Ed Jennett  
STAFF REPORTER

Jonathan S. Hornbliss  
PUBLISHER

Danielle Cattani  
AVP, CONFERENCES

Jean Gazis  
MARKETING MANAGER

Meredith Krantz  
AVP, ADVERTISING

Clarissa Carrington  
CUSTOMER SPECIALIST

*Bank Security News* is published every two weeks except in September and December, during which it is published monthly.

Subscription: \$489 (24 issues).

Contact:  
Royal Media Group  
1359 Broadway, Suite 1512  
New York, NY 10018  
T: (212) 564-8972  
F: (212) 564-8973

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.

## SECURITY GETTING CAPITAL

*continued from page 1*

victims of identity theft halt fraudulent transactions and restore their credit standing — as a way to win over new customers.

Citibank, along with a number of banks in the United Kingdom, were hit hard last year with a new type of fraud attack known as phishing. In phishing, con artists attempt to garner recipients' personal information by sending bogus emails that appear to come from their financial institutions. It will be a big part of the 2004 battlefield for both security and customer relations, said the board.

Allen said she expected such attacks to expand in the next year beyond financial firms to retailers and other businesses.

On the legislation side, Allen said that, being an election year, Americans will hear a lot from politicians who propose new bills for security, privacy, and fraud issues, but few will be signed into law.

Compliance headaches brought on by the recently enacted CAN-SPAM email law will cause businesses to pressure their email vendors to create solutions. [See page 7 for more on CAN-SPAM.] "There is nothing out there in terms of technology that can automatically label

something as an advertisement," said Slattery, who said his biggest compliance challenge would be keeping its individual branches in line. "Microsoft, Lotus and other email software providers will have to address the issue, rather than wait around for a third-party solution."

Increased pressure by banks on their vendors to provide better and more secure computer programs across the board will be a hallmark for 2004, said Allen.

Financial companies will demand advances in patch management, also, to make that process as efficient and cost-effective as possible.

Meanwhile, banks will work harder within their organizations to communicate the importance of security, privacy, and fraud issues to employees at every level, Stein said. Williams agreed, adding, "If I had to pick a watershed priority [for First Franklin] in 2004, it is to institute an internal education and awareness effort throughout the corporation."

Finally, all agreed that Wells Fargo & Co.'s proactive crisis management and customer relation campaign taken last November after a computer theft, provided a wake-up call on the importance of consumer privacy, and a model to follow when that privacy is breached.

## 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 PINON  
Senior Vice President  
MasterCard

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

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

# Rules & Regs

## CANADIAN PRIVACY LAW CREATES OUTSOURCING CHALLENGES

A comprehensive Canadian consumer privacy law that went into Jan. 1 is forcing U.S. banks to reconfigure the way their call centers north of the border operate.

"This is a big issue," said **Michael Geist**, technology counsel to Ottawa, Ont.-based **Osler, Hoskin & Harcourt LLP**. "If [U.S.

banks] have call centers in Canada, they are subject to this law. People are trying to wrap their heads around it and determine how to comply."

Canadian banks have been adhering to the tough privacy law since 2001.

*Continued on page 5*

## BANKRI COMPUTER THEFT

*continued from page 1*

computer was worth more than the sum of its parts. They did confirm, however, that the theft did not take place in Wisconsin, nor in Rhode Island. Federal law enforcement officials, along with local police in the area in which the theft occurred, are investigating, they said.

In addition to alerting its customers by mail that their personal information was exposed, BankRI set up dedicated toll-free hotlines at the bank and at credit bureau **TransUnion** to answer consumer questions and to counsel on fraud risks.

When the personal information of thousands of Wells Fargo customers was breached in early November, the bank was bound by the California Security Act, also known as SB 1386, which mandates that companies contact in writing all California customers whose unencrypted personal information they maintain is breached as a result of negligence or theft. Wells Fargo went beyond that; it provided free credit-fraud protection through national credit bureaus.

The computer that contained the Wells Fargo customer information was later recovered and studied by law enforcement officials, who found no evidence that the data had been accessed.

Outside California, no law requires banks to inform customers when their personal information has been exposed due to theft or negligence, but BankRI's actions show that banks are taking customer privacy seriously, and are raising the bar above the regulations that govern their practices to secure it.



Les Muma  
Fiserv

"I think it would be smart [for banks] to follow SB 1386 as guidance," said **Robert Ellis Smith**, a Rhode Island attorney and publisher of the *Privacy Journal*. "Some members of Congress want to legislate this nationally, and I think we may see this national in five years."

BankRI is handling the matter well, said Ellis, but he added that with the rising instances of identity theft, banks could best secure their customers' accounts by discontinuing the practice of using Social Security numbers to verify accounts. "It's superfluous and dangerous to have Social Security numbers floating around. They should not be part of a data file of a person's account," he said. "They should not be used for any verification reason outside filing taxes."

**Les Muma**, chief executive of Fiserv, agreed.

"There is a move toward that in business in general — certainly in banking, and in the insurance business," said Muma, who added that the presence of client information on a laptop was a violation of company policy, and that the individual responsible had been reprimanded. "I think the lesson learned is to monitor policies more tightly and communicate them more strongly," he said.

The bank is also stepping up its internal controls. BankRI is installing fraud-detection software on all of its computers, and encryption programs on all laptops. The bank's laptop computers already include tracking systems that allow the bank or law enforcement to pinpoint their physical location.

## CALENDAR

**Jan. 26-31**

SANS Cyber Defense Initiative West, Sheraton San Diego Hotel and Marina. 301-654-SANS or [www.sans.org](http://www.sans.org)

**Feb. 2-3**

Strategic Research Institute's Email Security Summit, Westin Grand, Washington, D.C. 800-599-4950 or [www.srinstitute.com](http://www.srinstitute.com)

**Feb. 4-6**

Alert Media's International Money Laundering Conference, Fontainebleau Hilton Resort, Miami. [www.moneylaunderingconference.com](http://www.moneylaunderingconference.com)

**Feb. 23-27**

RSA Annual Conference, Moscone Center, San Francisco. [www.rsaconference.com](http://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](http://www.misti.com)

**March. 24-26**

American Bankers Association/Foreword Financial Bank Technology Convention, Renaissance Orlando Resort at Seaworld. [www.aba.com](http://www.aba.com)

**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. SDGT's added between Dec. 5, 2003, and Jan. 15, 2004:

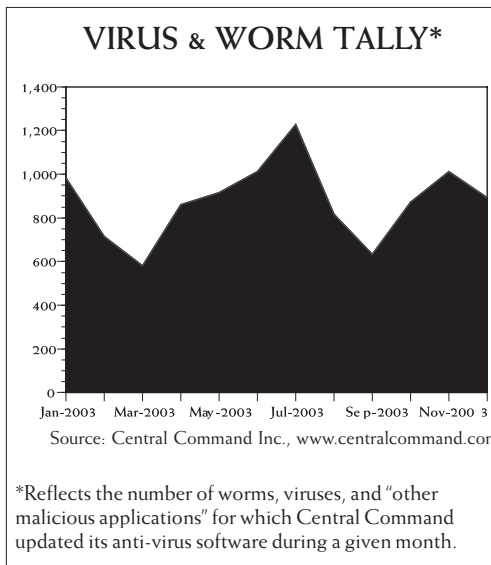
Durugut, Safet (a.k.a. "Abu-Sumaya"); DOB 10 May 1967; POB Orahovac, Kosovo;

Hochberg, AG (f.k.a. Ba Taqwa For Commerce and Real Estate Company Limited), Vaduz, Liechtenstein; formerly c/o Asat Trust reg., Vaduz, Liechtenstein

Kongra-Gel (a.k.a. Freedom and Democracy Congress of Kurdistan; a.k.a. Halu Mesru Savunma Kuveti (HSK); a.k.a. Kadek; a.k.a. Kurdistan Freedom and Democracy Congress; a.k.a. Kurdistan People's Congress (KHK); a.k.a. Kurdistan Workers' Party; a.k.a. Partiya Karkeran Kurdista; a.k.a. People's Congress OF Kurdista; a.k.a. PKK; a.k.a. The People's Defense Force)

Al Mansooran (a.k.a. Al Mansoorian; a.k.a. Army of the Pure; a.k.a. Army of the Pure and Righteous; a.k.a. Army of the Righteous; a.k.a. Lashkar E-Tayyiba; a.k.a. Lashkar E-Toiba; a.k.a. Lashkar E-Taiba, Pakistan Defense

Vazir (a.k.a. Al-Haramain; a.k.a. Al-Haramain Foundation; a.k.a. Al-Haramain Humanitarian Foundation; a.k.a. Al-Haramain Islamic Foundation; a.k.a. Al-Haramayn; a.k.a. Al-Haramayn Foundation; a.k.a. Al-Haramayn



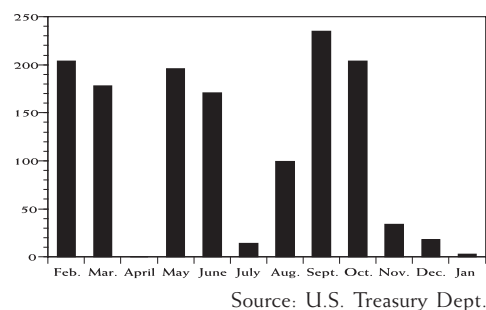
**THE 10 MOST COMMON VIRUSES**

Worm/Gibe.C	21.4	—
Worm/Klez.E (& G)	14.7	18.2
Worm/MiMail.I	12.8	—
Worm/MiMail.J	5.98	—
Worm/BugBear.B	5.2	24.8
Worm/MiMail.K	5.1	—
Worm/MiMail.A	3.7	—
Worm/Sober.C	1.9	—
Worm/Nachi.A	1.6	—
Worm/MiMail.C	1.6	—

Humanitarian Foundation; a.k.a. Al-Haramayn Islamic Foundation; a.k.a. Al-Haramein; a.k.a. Al-Haramein Foundation; a.k.a. Al-Haramein Humanitarian Foundation; a.k.a. Al-Haramein Islamic Foundation; a.k.a. Alharamain; a.k.a. Alharamain Foundation; a.k.a. Alharamain Humanitarian Foundation; a.k.a. Alharamain Islamic Foundation; a.k.a. Alharamayn; a.k.a. Alharamayn Foundation; a.k.a. Alharamayn Humanitarian Foundation; a.k.a. Alharamayn Islamic Foundation; a.k.a. Alharamein; a.k.a. Alharamein Foundation; a.k.a. Alharamein Humanitarian Foundation; a.k.a. Alharamein Islamic Foundation; a.k.a. Mu'Assasat Al-Haramain AL-Khayriyya; a.k.a. Mu'Assasat Al-Haramayn AL-Khayriyya; a.k.a. Mu'Assasat Al-Haramein AL-Khayriyya; a.k.a. Vezir), 64 Poturmahala, Travnik, Bosnia-Herzegovina; Somalia

**SDNS 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 Jan. 12.



**RECENT CIVIL PENALTIES IMPOSED BY TREASURY**

These penalties were imposed by the U.S. Department of Treasury's Office of Foreign Assets and Control and made public between Dec. 5, 2003, and Jan. 2, 2004.

Company	Summary of Violation	Year(s) Occurred	Voluntary Disclosure	\$Settlement
Arab Banking Corp.	Funds Transfer: Kosovo	2000	Yes	5,500
Bank of China	Funds Transfer: Cuba	1996	No	10,00
Eastern Financial Florida Credit Union	Funds Transfer: Cuba	2002	No	4,000
J.P. Morgan Chase & Co.	Funds Transfers: Libya, Cuba, Sudan	2001-03	Yes	17,304
J.P. Morgan Chase & Co.	Funds Transfers and Letter of Credit: Libya, Cuba, Sudan	2000-02	No	73,281

## RECENT PERFORMANCE OF PUBLICLY TRADED INFORMATION SECURITY COMPANIES

Company	Ticker	Price 1/15	Price 12/18	4-wk ch(%)	P/E	52-wk Hi	52-wk Lo	Shrs.Out.*	MarketCap*	Avg Volume
Alanco Technologies Inc	ALAN	0.80	0.78	2.56	N/A	1.29	0.23	15,262	12,210	206,040
Blue Coat Systems	BCSI	24.40	19.71	23.80	N/A	25.60	4.13	10,459	255,200	115,954
Brink's Co.	BCO	24.41	22.01	10.90	119.7	24.02	12.36	54,253	1,324,316	219,590
CompuDyne Corp.	CDCY	11.11	9.20	20.76	29.3	12.44	4.80	7,929	88,091	71,545
Checkpoint Systems Inc.	CKP	20.95	19.08	9.80	21.9	22.45	8.66	32,889	689,025	259,331
Diversified Security Solutions	DVS	5.92	5.75	2.96	N/A	7.70	5.26	5,068	30,003	7,534
Entrust Inc.	ENTU	4.75	4.09	16.14	N/A	5.70	2.25	63,327	300,803	133,868
Honeywell International Inc.	HON	36.48	31.57	15.55	N/A	36.24	20.20	862,051	31,447,620	3,884,636
ICTS International NV	ICTS	3.22	2.52	27.78	41.3	6.24	2.40	6,513	20,972	13,129
International Electronics Inc.	IEIB	3.30	3.50	-5.71	N/A	4.10	2.15	1,629	5,376	1,409
Invision Technologies Inc.	INVN	32.47	32.47	0.00	5.7	31.41	19.82	16,919	549,360	391,772
Internet Security Systems	ISSX	18.32	18.10	1.22	310.5	24.20	9.85	49,787	912,098	188,181
Kroll Inc.	KROL	27.00	25.35	6.51	27.2	27.25	26.66	41,791	1,128,357	486,046
Lojack Corp.	LOJN	8.00	7.66	4.44	19.7	9.90	4.49	14,856	118,848	30,484
Magal Security Systems	MAGS	7.90	8.26	-4.36	29.32	9.97	4.60	7,697	60,806	17,136
Markland Technologies Inc.	MRKL.OB	1.80	2.35	-23.40	N/A	5.00	1.65	N/A	N/A	192,613
Napco Security Systems Inc.	NSSCE	7.27	7.80	-6.79	20.1	10.20	7.01	3,198	23,249	5,818
Network Associates Inc.	NET	16.20	14.66	10.50	42.4	20.70	10.42	161,439	2,615,312	2,155,196
Protection One Inc.	POIX.OB	0.31	0.30	3.33	N/A	1.65	0.15	98,283	30,468	74,590
Rainbow Technologies Inc.	RNBO	13.00	11.3	15.04	448.3	13.22	6.00	26,660	346,580	208,500
RSA Security	RSAS	17.10	14.26	19.92	N/A	17.60	4.79	60,184	1,029,146	786,181
Safenet Inc.	SFNT	35.04	30.40	15.26	N/A	44.50	15.60	13,273	465,086	324,136
Silent Witness Enterprises Ltd.	UGHO.OB	0.18	0.12	50.00	63.0	4.00	0.09	N/A	N/A	223,681
Universal Guardian Holdings	VRSN	19.37	15.85	22.21	N/A	20.17	6.55	241,504	4,677,932	2,708,708

\* in thousands

**CANADA LAW A CONCERN***continued from page 3*

As of Jan. 1, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs the manner in which any firm operating in Canada may collect, use, store, or disclose an individual's personal information.

Among other requirements, firms must get permission from customers, employees, and sales prospects before sharing their personal information with any unaffiliated organizations or using the information to market products or services to the person from whom it was collected.

Companies must also disclose, upon an individual's request, any information they maintain on that person. This is a great challenge for smaller firms, Geist said.

"Now, any institution that collects information on me — I can ask what they have, and they have to respond within 30 days," said Geist. "It's not that organizations are unwilling to comply, but many have not set up their data systems to handle those requests."

Companies that operate only in Quebec are exempt, as that province's own privacy law was accepted by Canada's Federal Privacy Commission.

**Dina Palozzi**, chief privacy officer for **BMO Financial Group**, in Toronto, has used her years of experience with PIPEDA compliance to hone the company's internal control policies as well as those of its outside contractors.

Banks, she said, should carefully outline in their contracts the minimum measures their service providers must take to ensure the security of personal data. "You can't outsource your liability," warned Palozzi. Banks should then audit their contractors. "It's one thing to tell them what you expect, it's another thing to make sure they do it," she said.

### WILLIAM D. LANGFORD JOINS FINCEN

**William D. Langford** has been named senior policy advisor to the Financial Crimes Enforcement Network (FinCEN), the Treasury Department's lead agency in the fight against money laundering.

Langford will serve as senior advisor to FinCEN Director **William J. Fox** on the development and administration of regulations involving the Bank Secrecy Act.

Previously, Langford was a senior advisor to the general counsel at the Department of Treasury where, since Sept. 11, 2001, he focused on implementing the anti-terrorism and anti-money laundering provisions of the U.S.A. Patriot Act.

In his new role, Langford aims to help increase FinCEN's partnership with industry in drafting regulation as well as

garner feedback after any is implemented. "In order to have a successful regime in the nature of money laundering, you must have feedback from those affected by the regulations and from law enforcement, and find out what their needs are," he said.

Langford is interested in studying policies governing currency transaction reports (CTRs) and suspicious activity reports (SARs).

A financial institution must file a CTR with its primary regulator anytime it facilitates a currency transaction in excess of \$10,000. It must file an SAR on any transaction worth \$5,000 or more, in which the institution believes the funds may have come from illegal activities.

In recent years, banks have filed more CTRs and SARs than ever before, as

America's war on terror highlights the need to curb terrorist financing, and increased regulation has pressured them from a compliance standpoint. There were 21,337 SARs filed as of June 30, 2003, 29% more than during the same period in 2002, according to FinCEN.



William Langford  
FinCEN

Scrutinizing the ever-increasing number of such reports can be taxing. Langford plans to examine ways to file and screen such reports more effectively.

"We want to increase the utility of these documents for law enforcement and regulators, but also to make sure they are useful," he told *Bank Security News*.

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](http://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

---

# Rules & Regs

## MUCH CRITICIZED CAN-SPAM ACT BECOMES LAW

Despite being roundly criticized, the controversial CAN-SPAM Act of 2003 went into effect on Jan. 1, just two weeks after it was signed by President George W. Bush.

Among other things, the law requires unsolicited commercial email messages be labeled as advertisements, though it does not specify a standard method for doing so. CAN-SPAM, short for Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, also requires a functioning return-email address, the inclusion of opt-out instructions — which must be honored within 10 days — and the sender's physical address.

The most important issue for banks is that the Federal Trade Commission has been empowered, though not required, to establish a "Do Not Email" registry. If created, the registry would most likely be

similar to the FTC's "Do Not Call" registry, which allows consumers to opt out of receiving telemarketing calls.

"I think that is something that credit issuers need to keep an eye on," said **Melanie Brody**, a partner in the Washington, D.C., office of law firm Kirkpatrick & Lockhart. The FTC will submit a report to Congress — within the next six months — that sets forth a plan and a timetable for a "Do Not Email" registry and addresses any concerns that the agency would have with the plan. "I think banks are already concerned about the registry," said **Lorretta Salzano**, a partner at law firm **Franzen & Salzano**, adding that the creation of a registry is likely to occur.

CAN-SPAM also prohibits the sending of emails in which the name used in the message's "From" header is misleading, or

the subject headings are deceptive.

Even with such restrictions, the law is not likely to have a significant impact on lenders' operations.

"I don't think that legitimate businesses will change in a significant way," said Brody. "Legitimate businesses have already been in compliance with this."

Added Salzano, "It seems like a common sense thing not to be deceptive. If they hadn't been doing deceptive marketing, that shouldn't have much impact on them."

Violators face both civil and criminal penalties, which could include fines and, in some extreme cases, imprisonment. CAN-SPAM preempts all state laws or rules regulating spam, except any laws or rules that prohibit falsity or deception in a commercial electronic message.

---

## BANK OF SWISSCREDIT IS A FRAUD, HONG KONG MONETARY AUTHORITY SAYS

A web site using the domain name "www.swisscreditbank.com" is suspected of attempting to defraud credit card customers worldwide, warned the **Hong Kong Monetary Authority** in an alert published on Dec. 31.

Visitors to the web site are asked to "activate your account with credit card (sic)...minimum deposit \$5,000," providing a form for use with MasterCard, Visa, or American Express cards.

The web site purports to belong to "Bank of Swisscredit," claiming it has offices in Zurich, Hong Kong, and Canada. The HKMA advised that no such entity is authorized to provide banking services or take deposits in Hong Kong, and that the

Swiss Federal Banking Commission has no entry for Swisscredit.



The web site lists no phone number for the alleged Swiss headquarters, and telephone calls to the listed Hong

Kong branch went unanswered. The domain name swisscreditbank.com is registered to **Ultimate Search**, according to the Hong Kong Internet domain name registry, and lists only a Hong Kong post office box as an address. Calls made to the phone number listed with the registry led to recordings indicating the call could not be completed as dialed.

"We are not aware of any members of the public that have had any dealing with this entity, and we have urged anyone who has to contact police,"

said **Jasmin Fung**, a spokeswoman for the HKMA.

The web site also states that Swisscredit is a member of the U.S. Federal Deposit Insurance Corporation. That claim is fraudulent, according to a statement issued by FDIC.

The case is under investigation by the Hong Kong Police Force, and the HKMA has alerted the Swiss bank regulator.

*The Commercial Crime Bureau of the Hong Kong Police Force asks anyone with information on this possible fraud to call (852) 2860-5012. Information may also be forwarded to the FDIC's Special Activities Section by email to alert@fdic.gov.*

---

# Rumblings

## BANK OF ENGLAND PHISHING INCIDENT HIGHLIGHTS INCREASING MENACE

Thousands of companies and individuals in the United Kingdom received last month fraudulent emails disguised as coming from **The Bank of England**, the country's central bank announced Dec. 30.

The email originated from "admin@bankofengland.co.uk," a phantom address, according to the bank, and instructed recipients to download an attached program it claimed would help secure their personal financial information. The program was, in fact, a virus.

The bank advised anyone who receives such an email to delete it immediately.

"We're not aware if anyone actually downloaded the attachment," said a spokeswoman for the bank. "It was definitely a virus, but that's about all we've got so far. The national police and

the National Hi-Tech Crime Unit are looking at the problem."

The incident underscores the escalating problem of "phishing," in which fraudsters employ an email that appears to come from a well-known bank or company as a ruse to garner a victim's personal financial information. At least 51 phishing scams hit major banks and e-commerce portals based in the U.S., Canada, the U.K., Spain, and Australia in 2003, according to a study by London-based consultancy **mi2g**. British banks, including **Barclays**, **Lloyds TSB**, and **NatWest**, were especially targeted in the last two months of the year.

Some bankers at a cyber-security summit held in London in mid-December suggested the international community create a new ".bank" internet domain name for financial services

companies. Since only accredited financial firms would be permitted to register domain names using the ".bank" extension, criminals would have a harder time mocking up banks' email addresses.

The attack on The Bank of England, however, shows that phishing fraudsters are becoming more sophisticated, making their emails appear to have come from just about any domain name. The methods banks must develop to address this rising threat remain open for discussion.

"We see phishing as just the toe in the water," a security expert for one of the U.K.'s largest banks told *Reuters* on Dec. 16, on the condition of anonymity, at the Inaugural European Forum on Cyber Security in the Financial Services summit. "It's like credit card fraud. Phishing is not big yet. But it will be," he said.

---

## NATIONAL CITY TAPS DIEBOLD FOR SECURE ATM MACHINES

**National City Corp.** has chosen North Canton, Ohio-based **Diebold Inc.** to replace its network of automatic teller machines in a deal worth \$30 million, the companies announced Jan. 7.

Over a 30-month period Diebold will upgrade the Cleveland-based bank's 1,580 ATMs across six states to its new Opteva model.

The new ATMs, which feature consumer-convenience enhancements, such as touch-screen operation, also provide a higher level of encryption for securing a customer's personal identification number (PIN) than past models.

"Behind the scenes, the keypad is taking advantage of the triple-DES [data encryption standard] as you enter your PIN," said **Matt Burns**, National City's senior vice president for elec-

tronic banking. "In today's world, your PIN is encrypted once [when you enter it] and then unencrypted for verification [in the financial institution's database]. These machines actually encrypt it three times."

As well, a simple mirror system gives users the ability to monitor onlookers who may attempt to see them enter their PIN, something the old machines did not.

The keypad itself is "recessed in a way that, unless you are literally standing on top of someone you can't see what a customer is keying in," said Burns.

In one of the model's most celebrated features, visually impaired customers can plug any standard headset into the new ATM to receive an audio version of the on-screen instruction as

well as the customer's own key entries. "The only thing that is not audible, is we don't echo back their PIN," Burns added.

[www.diebold.com](http://www.diebold.com)



### IN THE NEXT ISSUE

The security implications of J.P. Morgan Chase's acquisition of Bank One Corp.