

BANK SECURITY NEWS

A ROYAL MEDIA GROUP PUBLICATION • 261 FIFTH AVENUE, SUITE 412 • NEW YORK, NY 10016 • WWW.BANKNET360.COM

SHARING INFORMATION TO ENHANCE SECURITY • SEPTEMBER 2006 VOL. 4, NO. 7

NEWS INSIDE

OPERATIONS

FloridaFIRST responds to Hurricane Ernesto page 3

ENCRYPTION

Barmenia Group fortifies web site traffic page 4

COMINGS & GOINGS

Richard Stearns becomes OCC's new enforcement czar page 5

COMPLIANCE

Pitney Bowes masks data for PCI compliance page 5

DISASTER RECOVERY

Hancock Bank looks back on Hurricane Katrina page 6

ENFORCEMENT

OCC warns banks to look out for FFIEC phishing page 7

PIPELINE

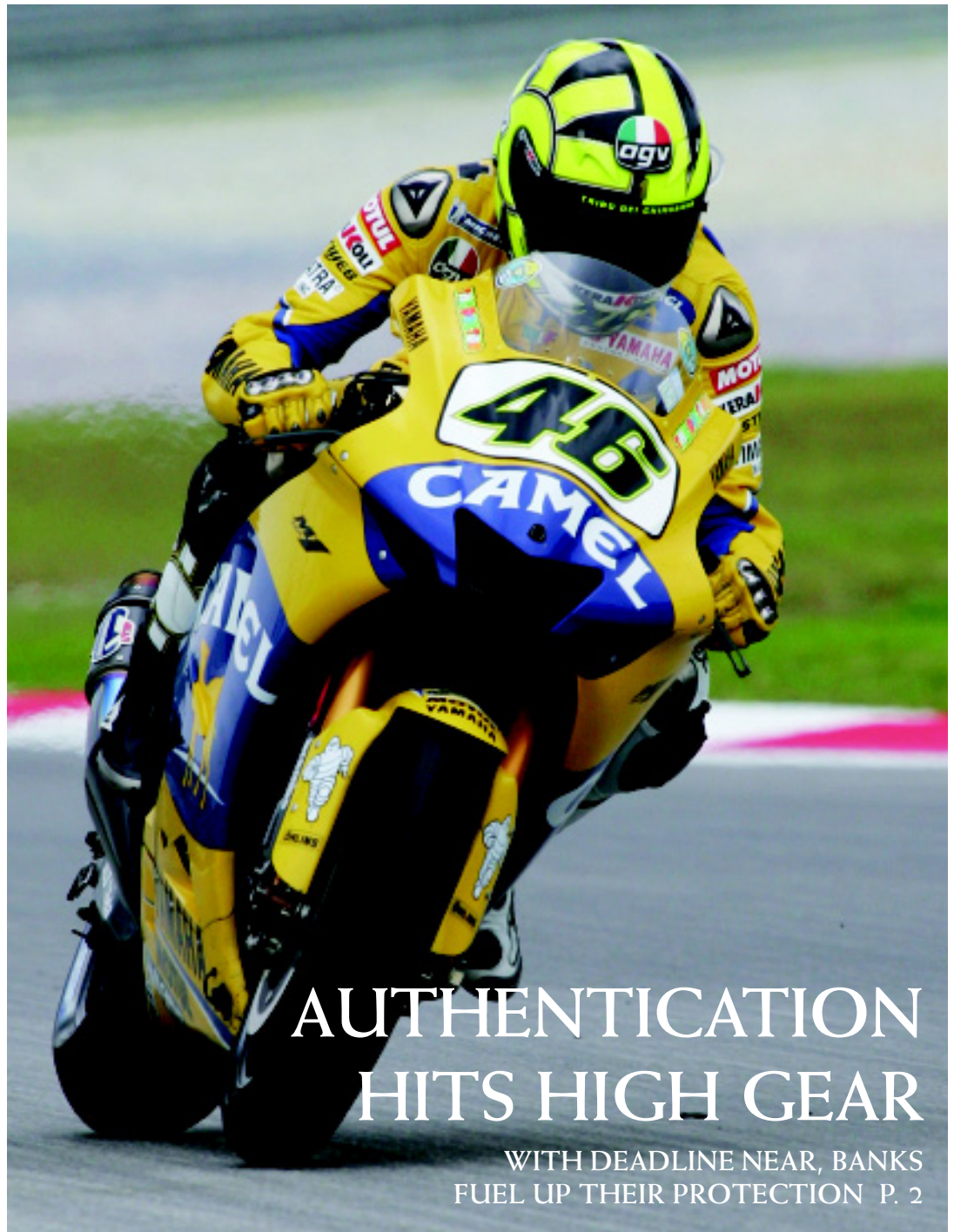
Credit Union employee charged with fraud; cross-dressing CU robber arrested; ICBA lobbies against "Red Flags" page 10

DEPARTMENTS

Tech Tracker page 8
Data Breach Monitor page 8
Industry Calendar page 8
Daily Attack Monitor page 9



2006 © Royal Media Group
All rights reserved



AUTHENTICATION HITS HIGH GEAR

WITH DEADLINE NEAR, BANKS
FUEL UP THEIR PROTECTION P. 2

RISK PROFILING GAINS TRACTION WITH BANKS

U.S. banks are accelerating their authentication technology deployments with the deadline for installing multi-factor systems fast approaching.

In late August, **Wells Fargo & Co.** announced that it had begun to deploy a real-time, risk-analysis tool developed by Santa Clara, Calif.-based **Bharosa Inc.** This month **National City Corp.** also installed Bharosa technology. And **M&T Bank Corp.** decided to protect its online commercial and individual accountholders with software from **Corillian Corp.** that takes a behavioral approach to user verification based on "access signatures."

The Bharosa technology, part of the vendor's "Tracker" product line, allows San Francisco-based Wells Fargo to determine whether a customer is logging onto its web site from a pre-established internet protocol address and location. If the bank does not recognize the user's computer "fingerprint," it can apply additional layers of authentication, such as challenge questions, to ensure that the person attempting to log in is who he claims to be.

The risk-analysis feature complements Wells Fargo's layered approach to security, Executive Vice President of Internet Banking Products **Jim Smith** said in a statement. "No one solution can solve the problem of online security," he said.

Similar aims prompted **SVB Silicon Valley Bank**, a subsidiary of Santa Clara, Calif.-based **SVB Financial Group**, to roll out Bharosa's computer forensics technology alongside its virtual authentication devices, which are part of a product suite called "Authenticator."

A commercial bank that caters to

technology, life sciences, and private equity firms, SVB wanted an authentication solution that its clients could customize according to their business needs.

The bank began shopping for vendors last fall, when the **Federal Financial Institutions Examination Council** mandated that financial institutions implement stronger forms of authentication to safeguard online accounts.

"We wanted to simplify the process and make sure that our clients had the appropriate level of security and confidentiality associated with their accounts," said **David Webb**, SVB's chief information officer.

Last month marked the six-month anniversary of SVB's simultaneous deployment of the Bharosa Authenticator and Tracker suites.

Authenticator provides several web-based interfaces through which customers can access their accounts. The interfaces, which are hardware- and software-independent, can be customized with pictures so customers know they are visiting a legitimate site.

Username and password data is entered via mouse clicks and encrypted at the point of entry and as it is transmitted.

At the backend, Tracker allows SVB to assess the risk of each transaction based on the bank's familiarity with a user's IP address, computer browser and processor speeds, and geo-locations. The technology also allows banks to place a cookie on a user's computer during each login.

"It's always a one-time experience, so if the cookie is hijacked, the fraudster doesn't have the ability to assume the user's computer," said **Jon Fisher**, Bharosa's chief executive.

In late July, Phoenix-based **Desert Schools Federal Credit Union** also announced that it would implement both Authenticator and Tracker.

"We recognize that significant threats are out there," said **Ron Amstutz**, the credit union's chief information officer. "This particular solution offers the broadest security available."

The credit union plans to roll out the technology in stages during the next six months, said **Gary Laieski**, senior director of technology.

Even online banks are getting into the multi-factor authentication race.

ING Direct, the Wilmington, Del.-based savings bank, last month rolled out a new login process using **RSA Security Inc.**'s risk-based and site-to-user authentication solutions.

Users attempting to access their ING Direct accounts are verified by their computer's internet protocol address and by the personal identification number they enter with mouse clicks into a graphical interface that resembles the PIN pads on automated teller machines.



David Webb
SVB Silicon Valley Bank

The RSA solution requires each user to select a secret image and five challenge questions. The image appears during each login to confirm the web site's validity, and the challenge questions are issued when ING does not recognize a user's IP address.

"RSA Security's powerful authentication solution provides us with a full set of tools designed to help protect our customers, and to monitor and reduce fraud," ING Chief Information Officer **Rudy Wolfs** said in a statement.

Those tools include RSA's behind-the-scenes technology that scores transactions in real-time according

Continued on page 3

Continued from page 2

to perceived levels of risk and adds security measures, such as an automated phone call, when necessary.

The bank is also enrolled in the Bedford, Mass.-based company's round-the-clock anti-phishing service, which detects and blocks attacks, and its eFraudNetwork, a worldwide community that includes thousands of financial institutions that collate intelligence to give each other a heads-up about the latest threats.

It is not just U.S. banks that are getting serious about authentication.

Turkey's **Garanti Bank** has decided to secure its mobile banking customers with **Vasco Data Security International's** Digipass phone-authentication tool.

The Brussels-based vendor's software can be downloaded onto any Java-enabled cell phone, so that the bank can enable digital signatures via cell phones and text its customers one-time passwords for verification purposes.

In other words, it's slightly more important than a **Britney Spears'** ring tone.

—GEOFF MOSHER

OPERATIONS

FLORIDAFIRST PASSES HURRICANE ERNESTO TEST

Disaster-recovery coalition **FloridaFIRST** has come a long way since it was formally introduced last December.

Grown to 29 members from five, the non-profit association, established by the U.S. Treasury Department, expanded to Tampa in July. It will soon have a Jacksonville presence, as well.

The group's mission: to make sure that smaller members get a helping hand from larger ones whenever catastrophic storms barrage the Sunshine State.

So while Tropical Storm Ernesto was bearing

down on southern Florida in late August, **J.P. Morgan Chase & Co.** Global Operations Resiliency Manager **Libby Lester** was on the phone with FloridaFIRST Chairman **Robert Otero** offering the use of the New York-based giant's two training centers in Tampa should other banks' facilities be incapacitated by the storm.

"That really won over my confidence — when a big member bank offered to help the little banks, if they were devastated," said Otero, senior vice president and director of corporate security at Coral Gables-based **BankUnited**.

By cataloguing the resources that member banks have available to others in the event of a disaster, FloridaFIRST's executive board can quickly dispense aid, especially to the community banks with just one or two branches.

Other offerings ranged from ice and water to generators, armored cars, and eight mobile ATMs from Brandenton-based **Coast Bank of Florida**.

"Cash is the No. 1 thing needed in an emergency event," said Lester, a FloridaFIRST board member and chairman of the Tampa Bay region. "In the Tampa Bay area, we don't have a cash operation, but we do have back-office operations, so that's where we can help fill some of the needs."

Ernesto introduced FloridaFIRST members to how the system works in a real-life situation.

"When we got to the [hurricane-] watch stage, we started sending weather bulletins throughout the day and sharing information about which banks in which areas were closing, and when they were sending employees home," Otero said. "The **Treasury [Department]** gave us the information they had from the **Federal Emergency Management Agency** and **National Oceanic & Atmospheric Administration**, and then let us know how they were going to support us by having funds together. In my book, [the Treasury Department] really put its money where its mouth is and backed up its commitments."

Continued on page 4



Ron Amstutz
SVB Silicon Valley Bank

STAFF BANKSECURITYNEWS

EXECUTIVE EDITOR
& PUBLISHER
JJ Hornblass
hornblass@royalmedia.com

ASSOCIATE EDITOR
Geoff Mosher
gmosher@royalmedia.com

MANAGING EDITOR
Vincent Ryan
vryan@royalmedia.com

SENIOR EDITORS
Marcie Belles
mdblles@royalmedia.com
Mike Gibb
mgibb@royalmedia.com

CONTRIBUTING EDITORS
J.J. Andrews
Stephen Bernard

STAFF REPORTERS
Aaron Johnson
Oksana Poltavets

ASSOCIATE REPORTER
Jillian Ryan

PRODUCTION EDITOR
Ethan Byun
ebyun@royalmedia.com

ADVERTISING SALES
Meredith Krantz
mkrantz@royalmedia.com
Helena Panahbarhagh
helenap@royalmedia.com
Adam Rosen
arosen@royalmedia.com

MARKETING DIRECTOR
Nancy Rand

EVENTS
Molly Devine

IT DIRECTOR
Edward Song

Bank Security News is published monthly. Annual subscription: \$439 (12 issues).

Tax ID #13-3852425. For more information, contact Royal Media Group 261 Fifth Avenue, Suite 412 New York, NY 10016 T: (212) 564-8972 F: (212) 564-8973 E: connect@royalmedia.com www.royalmedia.com

2006 © 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

But Florida is not the only state where the concept of a disaster-recover coalition among financial institutions is gaining popularity.

Since FloridaFIRST's inception, similar organizations have sprouted up in Los Angeles and San Francisco while Houston, Atlanta, and Birmingham, Ala. are in the process of developing theirs.

ChicagoFIRST, founded in 2003, was the initial FIRST program.

"Ernesto highlights one of the great reasons to do this," said **Scott Parsons**, deputy assistant secretary of the Treasury Department's **Office of Critical Infrastructure Protection and Compliance Policy**. "We've been doing a series of outreach meetings across the country, and the industry is beginning to take note as to how effective and meaningful the regional coalition effort has been, and they're saying, 'This is a good idea, and we need to do this.'"

—AARON JOHNSON

ENCRYPTION

BARMENIA GROUP PLUGS GAPS IN SSL TRAFFIC

The technology financial services institutions use to encrypt web traffic is an indispensable security feature, yet many firms are defenseless against harmful content lurking in Secure Socket Layer transmissions.

But one of Germany's largest independent insurance providers, **Barmenia Group**, has closed this SSL "blank spot" by implementing software developed by San Jose, Calif.-based **Secure Computing Corp.**, **Dirk Hörner**, the insurer's web services and intranet manager, said during a web cast last month.

SSL protocol relies on cryptography to secure private data transmitted via the internet. While the protocol, which is compatible with most browsers, shields sensitive information like credit card numbers, it can also contain viruses and malware that are

not captured by URL filters and anti-spyware and anti-virus software.

To fortify its SSL traffic, the Wuppertal, Germany-based company has rolled out Secure Computing's Webwasher Secure Content Management Suite, Hörner said.

The software decrypts SSL content as it travels from a client's browser to the company's web site, while it is still in the corporate network. This strategy allows Barmenia to apply additional security features to block spam, spyware, viruses, Trojans, and worms.

Barmenia also uses a URL filter to prevent its more than 3,500 employees from accessing inappropriate, malicious, or distracting web content in accordance with its acceptable use policy.

"This innovative approach allows us to reliably enforce our corporate standards to http traffic, as well as our encrypted web traffic, without a chance of being circumvented,"

Continued on page 5



BANK SECURITY NEWS

ARE YOU QUALIFIED?

Apply for a complimentary subscription to *Bank Security News: Sharing Information to Enhance Security* — full of relevant, insightful market intelligence — that everyone is talking about.

Qualified readers may be eligible to receive a complimentary subscription to *Bank Security News*.

Applying for a complimentary subscription is easy, please go to www.royalmedia.com

Continued from page 4

Hörner said.

Webwasher applies dozens of checks to ensure that all web site certificates are valid, which takes the decision out of the hands of employees, Hörner said.

"Most employees don't have the knowledge or the background to decide whether a certificate is OK or not," he said. "Most of the time they will click 'yes' or 'accept.'"

—G.M.

COMINGS & GOINGS

STEARNS TAPPED TO HEAD OCC ENFORCEMENT

The Office of the Comptroller of the Currency has tapped a former counselor at the Office to Thrift Supervision to head its enforcement arm.

On July 31, **Richard C. Stearns** was named the OCC's new director for enforcement and compliance.

In this role, Stearns, 57, oversees the regulatory agency's Law Department Division, which investigates, recommends, and litigates enforcement actions.

Stearns replaces **Brian C. McCormally**, who left the agency this spring to join Washington, D.C.-based law firm **Arnold & Porter LLP**. In his new role, Stearns reports to **Daniel P. Stipano**, the OCC's deputy chief counsel.

Since 1993, Stearns has served as the deputy chief counsel for enforcement at the Office of Thrift Supervision. Prior to that, he was the agency's deputy chief counsel for regional enforcement and assistant chief counsel for enforcement. From 1985 to 1991, he was an assistant

director and a senior trial attorney at the **Department of Justice's Civil Division**.

"Rick brings impressive enforcement and litigation skills and experience to his new responsibilities," **Julie L. Williams**, the OCC's first senior deputy comptroller and chief counsel said in a statement.

During his career, Stearns served as a Senior Trial Attorney with the **Department of Housing and Urban Development**, an associate with the law firm of **Kirkpatrick & Lockhart**, and as a Lieutenant in the U.S. Navy Judge Advocate General Corps.

Stearns holds a law degree from the **University of Virginia** and a bachelor's in political science from the **University of North Carolina**. —G.M.

COMPLIANCE

HOW PITNEY BOWES HANDLES ITS PAYMENT COMPLIANCE EFFORTS

Just as biologists tag organisms to learn more about an ecosystem, security officers at companies that process, store, and transmit credit card information are monitoring data as it migrates through their enterprises.

Companies that handle such sensitive cardholder data are bound by the Payment Card Industry security standards advanced last June by **Visa International**, **MasterCard Inc.**, **American Express Co.**, and other credit card companies.

The private security standard, which was broadened in late July to include more merchants, requires companies to follow 12 steps to protect the data, including installing and maintaining firewalls, encrypting

transmissions across public networks, and restricting access.

"What it all boils down to is you have to take the PCI requirements in the context of your business and as part of an overall security program," said **Trevor Odell**, a security administration manager with **Pitney Bowes Inc.**, a manufacturer of postage meters, mailing systems, and other equipment.

The Stamford, Conn.-based company operates its own bank in Utah through which its customers deposit money that is used to finance the postage meters they use. The firm also processes credit card payments through its small business division.

In February 2005 — about five months before the PCI standards were unveiled — Pitney Bowes installed software from San Francisco-based **Vontu Inc.** to prevent data "at rest" and "at flight" from being compromised, Odell said during an August web conference.

Pitney employs "Vontu Monitor" to keep tabs on all data that passes through its computer network, assess risks associated with the information flow, and detect policy violations. At the same time, the company uses "Vontu Protect" to quarantine sensitive files and enforce access control and encryption policies, Odell said.

The company, he said, has compliance managers in various divisions whose job it is to ensure that electronic communications containing information that would violate PCI does not leave the company. If one of Pitney's more than 35,000 employees unknowingly attempts to send out such information, the company turns the opportunity into an educational experience, Odell said.

"They are learning that there is not only company policy to prevent this information [from leaking out], but this is why it's a bad thing to do,"

Continued on page 6



Daniel P. Stipano
Office of the Comptroller of
the Currency

Continued from page 5

he said. "We've found that to be extremely valuable."

Companies must perform quarterly network-vulnerability scans to prove that they are PCI-compliant. Failure to meet the standard can result in forfeiture of business with Visa and MasterCard and fines of up to \$500,000.

After PCI was released, Pitney decided to tag cardholder data to track its path through the company's computer network. The test uncovered 51 applications and databases that were then encrypted, Odell said.

His advice to other companies as a result: "Only encrypt what you need to."

"Encrypting an entire database can have a horrendous performance impact," he said.

The most common PCI failure today is management's inability to understand which data is being accessed and stored throughout the enterprise, and the risks associated with those uses, said **Gary Clayton**, a principal at the Dallas, Tex.-based **Privacy Compliance Group**, which provides data-protection solutions to Fortune 500 companies.

"Companies simply have not understood how data flows throughout the organization," Clayton said. "They don't know where the data is and, as a result, they don't mitigate risks."

Clayton favors an enterprise-wide approach to securing credit card information. Data security and privacy efforts, he said, should be integrated into an overall security program that includes administrative, physical, and technical safeguards.

Such steps, he said, are becoming increasingly important as the PCI standard's impact grows.

"It's just a matter of time before courts begin to uphold those standards, or something similar, required for all businesses that are

handling sensitive data, including credit card data," he said. —G.M.

DISASTER RECOVERY

HANCOCK BANK TRIUMPHS OVER HURRICANE KATRINA

When executives from Gulfport, Miss.-based **Hancock Holding Co.** opened the **Nasdaq** stock market on Aug. 29, they became symbols of the Gulf Coast region's rebound from Hurricane Katrina.

The bell-ringing ceremony, which coincided with the storm's one-year anniversary, was an acknowledgement of the bank's leadership in helping the region bounce back.

Hancock Bank's post-Katrina performance, dubbed "nothing short of phenomenal" by Mississippi Gov. **Haley Barbour**, would not have been possible without extensive pre-planning, a determined workforce, and flexible information technology.

The 104-branch bank, which serves southern Louisiana, Mississippi, and Florida, followed a disaster-recovery plan its hurricane-tested executives drafted years ago to protect critical data.

The Friday before Katrina touched down with 140-mile-an-hour winds, the bank shipped more than 200 backup tapes containing all of its records to Chicago and uploaded them onto secure servers, said **Michael Croal**, a former director of corporate loan operations.

The bank's primary data center in Gulfport, which would later have to be rebuilt, was backed up on servers located in Baton Rouge. Those servers were also linked to the

Chicago facility, which houses the bank's check-cashing images, said **Croal**, now a senior director at **Cornerstone Advisors Inc.**, a Scottsdale, Ariz.-based financial services consulting firm.

The Category 4 storm knocked out more than 75% of Hancock's branches, rendered its automated teller machines useless, and pummeled the lobby and parking lot of its 15-story headquarters in Gulfport, about a quarter of a mile inland from the Gulf of Mexico.

Executives ran the bank using borrowed offices, cell phones, and four large white boards. The corporate headquarters were temporarily relocated to the bank's offices in Baton Rouge, La.

About 110 of Hancock's 1,200 employees lost their homes, **Croal** said. The bank rented apartments for employees who had to abandon their homes.



Hancock Bank executives open the Nasdaq stock Market on Aug. 29, a year after Katrina.

A day after the storm, several branches re-opened, including the one in Ocean Springs, Miss., where employees cashed checks from a folding table at a make-shift outdoor teller window.

"People needed to know that there was something normal in a world of chaos," said **K. André Pires**, a loan operations analyst at the bank.

On Aug. 31, 2005, the bank's chief executive, **George A. Schloegel**, convinced **Federal Reserve** officers in Alabama to send more than \$15 million in cash in an armored truck to cover payroll for the many public- and private-sector employees who were crucial to the recovery effort.

Within two weeks, the bank opened temporary branches in converted RVs

Continued on page 7

Continued from page 6

in Pass Christian and Waveland, Miss., two hard-hit coastal communities. For months, employees fanned out across the coast on buses to serve customers. Meanwhile, incoming phone calls were rerouted to backup call centers in Denham Springs, La., and Tallahassee, Fla., Croal said.

While Katrina did a number on its physical infrastructure, the hurricane kicked one of Hancock Bank's IT projects into high gear.

The week before the storm hit, the bank had just decided to roll out **Hyland Software Inc.'s** "OnBase" document-management solution to reduce costs and generate efficiencies.

The storm forced the bank to relocate more than 126,000 crucial paper files from its vault in Gulfport, which housed 8.7 million documents, to a remote location 75 miles away in Purvis, Miss. That, in turn, prompted the bank to shrink its timeframe for deploying the Westlake, Ohio-based company's software from years to months, said Pires, who headed the effort.

In less than six months, Hancock Bank digitized 500,000 consumer lending and commercial credit files. The bank now scans 10,000 documents per day, and converts incoming files upon closing. These documents can be accessed by employees in multiple locations for file reviews and audits. Documents that must remain in hard copy form, such as titles, are stored in the vault, while others are shredded after conversion.

The solution has reduced loan-processing times, improved document organization, and eliminated the risk of the Gulfport center becoming a single point of failure. It has also



George A. Schloegel
Hancock Holding Co.

helped the bank automate and scale its lending operations in response to the post-Katrina reconstruction boom.

In late September 2005, Hancock Bank became the first financial institution to reopen in downtown Gulfport, just as it did after Hurricane Camille in 1969. The bank established dedicated loan centers and extended hours, including Saturday.

In October 2005, the bank unveiled a \$35 million restoration project for the headquarters. More than 1,000 new missile-impact-resistant windows were installed in the building, which is slated to reopen

late next month.

Four months after Katrina, the bank grew \$1.6 billion in assets despite suffering a \$32.4 million pre-tax hit last year as a result of the storm. —G.M.

ENFORCEMENT

FFIEC GUIDANCE COULD SPARK PHISHING WAVE: OCC

Hackers may attempt to exploit a December deadline for stronger authentication by luring customers to cough up their account details, the **Office of the Comptroller of the Currency** said in an alert sent to banks this month.

The OCC warning forecast a spike in phishing attacks that use the **Federal Financial Institutions Examination Council's** October 2005 online authentication guidance as a pretext for fraud.

"Sophisticated schemes may employ multiple methods to 'convince' the customer of their legitimacy," the statement said.

The FFIEC logo might even be used in phishing emails, the OCC warned.

Financial institutions are required by

yearend to implement additional factors of authentication beyond username and password to reduce the threat of identity theft and fraud.

The OCC recommends institutions inform their customers "well in advance" of their plans and of possible fraudulent activity citing the new methods of online identification.

MULTI-FACTOR FAQs ADDRESSED

Customers who are content to use only a login name and password must adopt the stronger forms of authentication implemented by their financial institutions, according to a document the FFIEC released last month.

The interagency body released the seven-page document to answer some of the common questions it has received from banks and technology providers during the past 11 months. The document, which is posted online, contains answers to 35 queries.

Banks, the FAQ says, should not forgo a risk assessment by immediately implementing additional authentication controls.

Each institution's stronger authentication solution should involve live testing, according to **Rick De Lotto**, an analyst with **Gartner Inc.**, a Stamford, Conn.-based consultancy.

"You must find your individual problems and fix them," De Lotto said. "You must demonstrate from your risk assessment that this is appropriate."

Banks that offer brokerage services and are chartered by an FFIEC agency must provide stronger authentication to customers that access those services.

"If customers come into a portal and then access those services, they must be covered," said **Edward Regan**, vice president of information technology risk management at New York-based **J.P. Morgan Chase & Co.**

The FFIEC is not considering any "general extension of the timing associated with this guidance," the document states. —G.M.

NEW PRODUCTS AND SERVICES

| Price | Company | Product/Services | Description | Web Site |
|----------|------------------------------------|---------------------------|--|------------------------|
| Sept. 18 | StillSecure | Safe Access v5.0 | Enterprise network access control software | www.stillsecure.com |
| Sept. 6 | Diebold Inc. | Diebold identiCenter | Fingerprint reader for bank branches | www.diebold.com |
| Sept. 6 | New Boundary Technologies | PCI Compliance Solution | Compliance automation software | www.newboundary.com |
| Sept. 5 | id-Confirm Inc. | SecureLink System | End-to-end biometric authentication | www.id-confirm.com |
| Aug. 28 | Oakley Networks Inc. | CoreView | Insider threat detection and prevention solution | www.oakleynetworks.com |
| Aug. 23 | IRIS AG | riskpro v2.6 | Risk analysis infrastructure | www.iris.ch |
| Aug. 16 | Mimosa Systems | NearPoint V2.0 | Information management platform | www.mimosasystems.com |
| Aug. 8 | FundsXpress Financial Network Inc. | fxCommunicator | Integrated web communication platform | www.fundsexpress.com |
| Aug. 7 | Edge Dynamics | Edge Dynamics v3.5 | SOX automation software | www.edgedynamics.com |
| Aug. 4 | Edentify Inc. | IDSscreen, Closed Account | Joint identity risk mgmt solution | www.edentify.com |

BREACH MONITOR

DATA BREACHES

| Date reported | Organization | Incident Description | Information Compromised | Accounts Affected |
|---------------|-------------------------|-------------------------------|--------------------------------------|---------------------|
| Sept. 1 | Wells Fargo & Co. | Stolen laptop, data disc | Employee health data | Unknown |
| Aug. 31 | Diebold Inc. | Stolen laptop | Employee financial data | Unknown |
| Aug. 29 | AT&T Corp. | Computer hacking | Customer financial data | Fewer than 19,000 |
| Aug. 25 | Sovereign Bancorp Inc. | Stolen laptops | Customer personal data | "Thousands" |
| Aug. 22 | Aflac Inc. | Stolen laptop | Customer personal data | 612 |
| Aug. 8 | America Online Inc. | Search records exposed online | Customer financial and personal data | 650,000 |
| Aug. 1 | U.S. Bancorp | Stolen briefcase | Customer personal data | "Very small number" |
| July 29 | Sentry Insurance | Insider theft | Customer personal data | 112,198 |
| July 28 | Matrix Bancorp Inc. | Stolen laptops | Customer financial data | Unknown |
| July 25 | Old Mutual Capital Inc. | Stolen laptop | Customer financial and personal data | 6,500 |

Source: Privacy Rights Clearinghouse

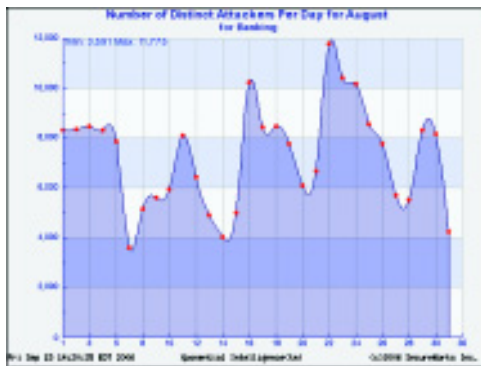
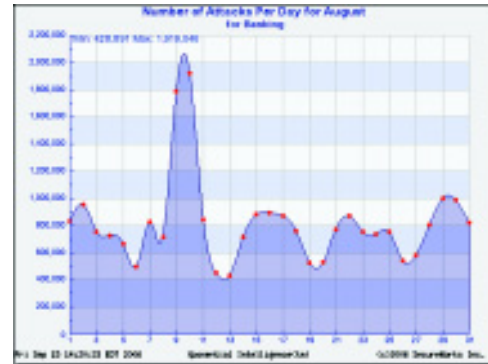
INDUSTRY CALENDAR

| Date | Event | Producer | Location | Web Site |
|-------------|---|-------------------------------|------------------|------------------------------|
| Sept. 25-26 | ABA Identity Theft & Fraud Symposium | American Bankers Association | San Francisco | www.sourcemedia.com |
| Sept. 25-27 | IT Security World Conference & Expo 2006 | MIS Training Institute | San Francisco | www.misti.com |
| Oct. 5 | ID Management Forum | Financial Services Roundtable | Washington, D.C. | www.bitsinfo.org |
| Oct. 8-10 | ABA Money Laundering Enforcement Conference | American Bankers Association | Washington, D.C. | www.aba.com |
| Nov. 2 | Transformation Summit | Royal Media Group | New York | www.transformationsummit.com |

To have your event listed in the calendar, contact Geoff Mosher at (212) 564-8972 x103 or gmosher@royalmedia.com.

DAILY NUMBER OF DISTINCT ATTACKERS

The number of IP addresses that attacked SecureWorks Inc.'s 600 banking clients in August crested on August 10, with more than 2 million attackers, doubling July's record daily high of 1 million.



DAILY NUMBER OF ATTACK TYPES

The greatest number of distinct attack types — 11,775 — occurred on August 22, up from July's record daily high of 9,539.



DAILY NUMBER OF ATTACKS

On August 24, there were 712 internet-based attacks, compared to July's high of 697.

PIPELINE

MARYLAND CU EMPLOYEE NABBED FOR COOKING BOOKS

Richard William Shives Jr., assistant manager of City, County, and State of Allegany County Federal Credit Union, was indicted by a federal grand jury Sept. 20 for making false statements to the National Credit Union Administration.

Shives, who was in charge of loan and collection officers, also allegedly concealed customers' loan delinquen-

cies and outstanding balances by making false entries in Cumberland, Md.-based CCSAC's books between 1999 and 2003.

According to the indictment, Shives prevented customers from receiving quarterly loan statements and delinquency notices, caused collection officers not to call delinquent customers, and understated the number and amount of delinquent loans on quarterly NCUA reports.

CROSS-DRESSING CU ROBBER SNAGGED IN BUNGLED HEIST

Three men accused of robbing Bright Star Credit Union in Hollywood, Fla. — one while dressed in drag — were arrested Sept. 19.

Upon entering the credit union, Esli Joseph, 20, wearing a dress, fired a shot and then proceeded to stuff \$140,000 from a vault into, ironically enough, a customer's purse.

Continued on page 10

Continued from page 9

Joseph was accompanied by **Rashad Joseph**, 21.

After exiting the building, the "couple" dropped the purse and fled when their getaway driver, **Jimmy Reny Fernetus**, 19, sped off without them at the sight of approaching police cruisers.

Fernetus was apprehended after crashing into another car, and the other two suspects were nabbed a couple blocks away. The money was also recovered.

In other news, chivalry is dead.

AMERICA'S COMMUNITY BANKERS WANTS "RED FLAGS" PROPOSAL RESCINDED

America's Community Bankers this month went a step further than the **Independent Community Bankers of America** and demanded that the proposed new rules on identity theft be rescinded.

In a Sept. 15 letter to six regulatory agencies, the ACB said the proposal from federal banking and thrift regulators, which details procedures and processes for identity theft fraud prevention and risk management, is duplicative of existing regulatory

requirements and would force small banks to expend significantly more resources "with only a disproportionately small benefit."

Under the "red flags" proposal, a bank's identity theft program would have to include steps for verifying information from people opening accounts, measures to detect red flags that indicate identity theft, steps to assess the instance of a red flag, steps for mitigating the risk of identity theft, staff training, and oversight of service providers.

The ICBA's letter to regulators included similar comments on the "Identity Theft Red Flags and Address Discrepancies" proposal, but that community banking advocacy group stopped short of recommending that the entire proposal be thrown out.

TYPOSQUATTERS TARGET CUS

One of the largest ever bulk registrations of credit union-like domain names occurred the weekend of Sept. 9, according to the **Credit Union Information Security Professionals Association**.

The CUISPA recorded more than 450 domain names that include "fcu.com" or "creditunion.com" over the weekend.

The registrants, known as "typosquatters," create domain names that resemble the names of legitimate web sites, sometimes containing an intentional typo or two, with the objective of attracting traffic that mistypes the intended domain name. The practice is not illegal, but is considered unethical and misleading.

BANK OF IRELAND COVERS PHISHING LOSSES

The Bank of Ireland announced early this month that it had reimbursed at least nine customers who had their accounts cleaned out by fraudsters.

The Dublin-based bank's decision to pay the customers — who were duped in a phishing attack — a total of \$205,064 caused a stir in the Irish banking community. Bankers have claimed the reward will spur attackers to strike again.

The payment is reportedly the first of its kind by an Irish bank.

For the latest news on bank security, visit www.banknet360.com, Royal Media Group's daily banking news web service.

BOARD OF ADVISORS

CATHERINE A. ALLEN
Chief Executive Officer
BITS

RICH CARALLI
Senior Member Technical Staff
Carnegie Mellon Software Engineering
Institute

JAMES COWING
Senior Director
Digital Resources Group

ERWIN MARTINEZ
Chief Information Officer
Tamalpais Bank

JIM MORRELL
VP Information Systems
iQ Credit Union

SERGIO PIÑON
Senior Vice President
MasterCard

GARY REYNOLDS
SVP, Financial & Electronic Crime
Investigations
Wells Fargo & Co.

PAT RUCKH
Executive Vice President and
Chief Technology Officer
First Tennessee

JAY SCHULMAN
Senior Manager Advisory, Information
Protection
KPMG

The Board of Advisors for *Bank Security News* provides insights and advice that help shape the scope and coverage of each issue. The opinions expressed in *Bank Security News* are not necessarily shared by the board members nor their employers.

MATTHEW SPEARE
Corporate Information Security Officer
M&T Bank

ERIK STEIN
Director, Fraud Prevention
and Investigation
Countrywide Home Loans

JEFF WEINSEIN
EVP & Chief Information Officer
WMC Mortgage

MAUREEN YOUNG
Partner
Bingham McCutchen