



FINANCIAL SERVICES SECTOR OPEN SOURCE DIGEST

August 2010

About this report: The Sector Open Source Digest (SOSD) is a sector-wide summary of events that have taken place during the past month domestically and internationally. The SOSD is primarily a compilation and reorganization of reporting drawn from the Daily Open Source Intelligence Report (OSIR). The SOSD may also contain additional reporting not originally published in the OSIR. The source materials for the OSIR and SOSD are found using open source research methodologies and include imagery; local, national, and international media reports; academia and industry sources; multimedia and blogs; and other relevant publicly available sources. The SOSD is a compilation of unclassified source material and does not provide analysis or projection. The content found within the SOSD is strictly for sector situational awareness.

SECTOR ELEMENTS

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

Cyber Threats

Botnet with 60GB of stolen data cracked wide open

August 2 – (International)

Researchers have cracked open a botnet that amassed more than 60GB of passwords and other stolen data, even as it cloaked itself using a state-of-the-art technique known as fast flux. When its command-and-control server was infiltrated, the Mumba botnet had snagged more than 55,000 PCs, according to the researchers from anti-virus provider AVG. The data-stealing operation is the work of the notorious Avalanche Group, a criminal operation that was [responsible for two-thirds](#) of all phishing attacks in the second half of 2009, according to a report earlier in 2009 from the Anti-Phishing Working Group. “These criminals are some of the most sophisticated on the Internet, and have perfected a mass-production system for deploying phishing sites and ‘crimeware,’” AVG wrote in a [report](#) issued August 2. “This means that mitigating the threat by going after the servers hosting the data using the ‘Mumba’ botnet is now much harder than before.” Most botnet command-and-control channels run on compromised Web servers or Web-hosting services designed for criminals, making it possible to dismantle the network by taking down the central server. Mumba, by contrast, makes use of fast-flux technology, in which the operations are carried out on thousands of compromised PCs. That allows the IP address and host machine to change every few minutes, a measure that frequently foils takedown attempts by researchers and law enforcement.

The Register: [Botnet with 60GB of stolen data cracked wide open](#)

Nationwide banks experience surge as phishing targets

August 2 – (National)

Since February of this year, RSA’s Anti-Fraud Command Center has seen a marked [uptick](#) in phishing attacks targeting the largest nationwide banks. From June 2009 through February 2010, larger financial institutions were targeted in the 19 to 30 percent range, depending on the month. The latest trend, however, shows that these large nationwide banks are receiving almost two-thirds of all phishing attempts in the finance sector, topping out at 68 percent in June. Infosecurity notes that the proportion of attacks targeting larger bank brands seems to come directly from the share once held by smaller regional banks. This may be a result of a recovering

**SECTOR
ELEMENTS**

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

economy and banking sector, as scammers shift their focus from smaller banks that were thought to be on more sound footing during the recent financial crisis. The report also revealed a 16 percent drop in total phishing attacks in June compared with the previous month. RSA believes one of the contributors was the dearth of activity from the Rock Phish gang (aka, Avalanche), which the company said has nearly halted its phishing activity in favor of launching malware attacks.

Infosecurity: [Nationwide banks experience surge as phishing targets](#)

Zeus botnet raid on UK bank accounts under the spotlight

August 11 – (International)

More details have emerged of how security researchers tracked down a Zeus-based botnet that raided more than \$1m from 3,000 compromised U.K. online banking accounts. The vice president of technical strategy for M86 Security said hackers [began](#) the assault by loading compromised third-party sites with a battery of exploits designed to infect visiting PCs with variants of the Zeus banking Trojan. Phase one of the attack used the Eleonore Exploit Kit and the Phoenix Exploit Kit to load Zeus onto compromised machines through a battery of browser and application-based vulnerabilities and drive-by download attacks. The main attack revolved around the use of version 3 of Zeus to steal money from online bank accounts. The use of a different strain of Zeus means the M86 researchers are sure the attack is unrelated to an otherwise similar attack involving 100,000 compromised U.K. bank accounts that was the subject of an alert by transaction security firm Trusteer the week of August 2. After noticing a pattern of possible attack, M86 researchers deliberately infected a machine in order to identify a command and control server associated with the botnet which was hosted in Moldova. They then used exploits to break into the poorly-secured system where they found logs recording the activity of compromised bank accounts. It also found that the exploit pack used to seed the attack had claimed a much larger number of victims — as many as 300,000 machines. The vast majority were Windows boxes, but 4,000 Mac machines were also hit. The logs also revealed that 3,000 online banking accounts had been victimized between July 5 and August 4.

The Register: [Zeus botnet raid on UK bank accounts under the spotlight](#)

See also; The Register: [Botnet that pawned 100,000 UK PCs taken out](#)

Top phishing gang turns to malware

August 19 – (International)

An Internet security [report](#) released August 20 said phishing attacks dropped 10 percent from April to June 2010 year-over-year. While reassuring at first glance, the report states cybercriminals have shifted their schemes from old-school phishing e-mail attacks — which are designed to trick users into revealing personal information — to distributing Zeus malware, a more insidious form of cybercrime. Phishing attacks by Avalanche, one of the most prolific cybercriminal gangs (responsible for two-thirds of the world's phishing attacks in the second half of 2009), have disappeared, but other criminals have moved in to take its place, according to Internet Identity (IID). Phishing targets have shifted from banks to gaming, e-commerce and social networking sites, aiming to steal log-in information. However, Avalanche and others have turned to distributing Zeus malware which is capable of hijacking computers, then stealing banking, social networking and e-mail account logins, and making that information available as part of a criminal network. Once the malware has entered the user's computer, the identity theft is automatic — eliminating the need for the unsuspecting user to supply personal information in response to a fraudulent e-mail.

Tech Daily News: [Top phishing gang turns to malware](#)

**SECTOR
ELEMENTS**

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

Other Cyber Threats Articles:

- *August 2 – (Texas) Krebs on Security: [Texas firm blames bank for \\$50,000 cyber heist](#).* Dallas-based Hi-Line Supply Inc. is trying to force its bank, Community Bank, Inc. of Rockwall, Texas, into a settlement over an attack by organized cyber thieves in 2010 that cost the company \$50,000.
- *August 4 – (International) The Register: [Scotland Yard arrests six over multi-million phishing scam](#).* Six suspected fraudsters have been arrested in the U.K. and Ireland over their alleged involvement in a bank and credit card phishing scam that affected tens of thousands of victims and resulted in losses of millions of pounds.
- *August 5 – (National) IDG News Service: [Hackers find a new target in payroll processing](#).* Criminals recently hacked into a desktop computer belonging to Regeneron Pharmaceuticals and tried to steal money by redirecting funds using Regeneron's account on the company's third-party payroll system, operated by Ceridian. The attack did not work, but it shows that criminals, who have been making millions of dollars by hacking into computers and initiating fraudulent bank transfers, may have found a new target.
- *August 12 – (International) The H Security: [Macs not vulnerable to Eleonore online banking trojan](#).* Macs are not being infected with the Zeus botnet said M86 Security, after reports August 12 by a number of news sources that Macs, PlayStation 3's and Nintendo Wii's had joined Windows systems as part of a banking targeted botnet.
- *August 16 – (International) The New New Internet: [Credit card clearing house hacked says security researchers](#).* An underground credit-card clearing house has been hacked, according to Trend Micro security researchers. Leaked data from the hack include employee e-mails and recorded phone calls.
- *August 18 – (International) The New New Internet: [Zeus Trojan spreading through zip files](#).* The Zeus Trojan is back again, looking to spread through zip files. Zeus, which is one of the most commonly found pieces of malware, is believed to be one of the most prevalent on the Internet has infected millions of users.
- *August 23 – (National) Help Net Security: [U.S. military personnel targeted by malware](#).* U.S. military personnel are again targeted by malware-peddling cybercriminals. Fake e-mail purportedly coming from Bank of America is asking holders of Military Bank accounts to update them by following a given link.
- *August 23 – (International) IDG News Service: [Apple can't stop ongoing iTunes charge scam](#).* Users of Apple's iTunes services should keep a close eye on PayPal and credit card statements for fraudulent iTunes charges. For more than a year, scammers have been racking up unauthorized charges on iTunes accounts, leaving Apple's customers to clean up the mess.

Physical Security**Gunmen storm Baghdad money exchange, kill 3***August 5 – (International)*

Gunmen stormed a Baghdad, Iraq money exchange and killed three people August 5, the latest in recent brash daylight attacks on banks, financial, and trade centers in the Iraqi capital, many of which have been blamed on insurgents. Police officials did not immediately know how much money was stolen in the 2 p.m. heist in the southeastern New Baghdad neighborhood. Fleeing the scene, the gunmen also threw flash bombs into a crowd of people responding to the shooting. Hospital officials confirmed three people were killed, including the owner of the money exchange. Five passers-by were

SECTOR ELEMENTS

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

wounded. Insurgents, suspected of trying to steal funding for their operations, have increasingly been blamed for heists of banks and financial centers.

Associated Press: [Gunmen storm Baghdad money exchange, kill 3](#)

Young girl among those hurt by acid in letters

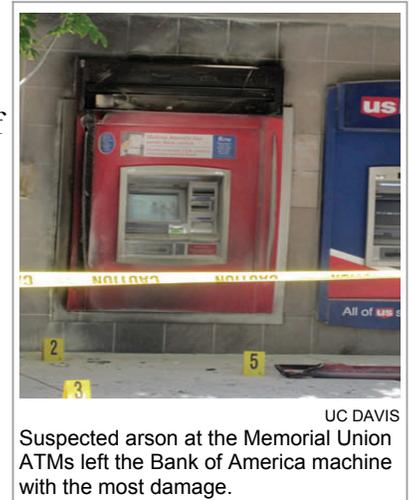
August 26 – (International)

An 8-year-old girl was among those injured by letters containing acid that were sent to the families of Geneva, Switzerland bank executives in recent days, the magistrate investigating the case said August 26. The girl was taken by ambulance to a hospital after she opened a box inside one of the letters and her hands were burned by concentrated sulfuric acid, the magistrate said by telephone from Geneva. Two adults were also injured, but apparently less seriously, by the letters, which targeted Geneva private bankers and their families, he said. The magistrate said that a total of eight letters containing acid were mailed to eight different addresses, in several cases the wives of executives at Geneva private banks. The letters were mailed from within Switzerland, but were routed through a central post office so it was not possible to say from where. The letters were sent August 22, the Swiss newspaper Tribune de Geneve reported. The motivation for sending the letters is not yet clear.

New York Times: [Young girl among those hurt by acid in letters](#)

Other Physical Security Articles:

- *August 2 – (California) KCRA 3 Sacramento:* [Bank of America ATM torched at UC Davis.](#) A Molotov cocktail might have been used to torch an automated teller machine (ATM) at the University of California, Davis (UC Davis) August 2, a university representative said.
- *August 12 – (New York) Watertown Daily News:* [Potsdam bomb call shuts two bank sites.](#) A bomb threat August 11 closed for several hours the Community Bank branches on Market Street and the drive-through on May Road in Potsdam, New York. The police chief said a man called the police station at 10:02 a.m. reporting the bomb threat.
- *August 19 – (California) KGTV 10 San Diego:* [Man claiming to have bomb in bank robbery arrested.](#) A suspected bank robber who claimed to have a bomb while robbing a bank in San Diego, California, was arrested August 19. No bomb or threatening device was found, police said.
- *August 20 – (Oregon) BNO News:* [Bomb threat at Aloha, Oregon bank closes highway.](#) A bomb threat at a bank in Aloha, Oregon forced the closure of a busy highway for nearly 2 hours August 19, authorities said. No suspicious device was found.



UC DAVIS
Suspected arson at the Memorial Union ATMs left the Bank of America machine with the most damage.

Insider Threats**US Grand Jury indicts two women on \$2.4 million credit-union fraud**

August 4 – (West Virginia)

A federal grand jury has indicted two women in a \$2.4 million credit-union fraud scheme case. A former employee of the N&W Poca Division Federal Credit Union located in southern West Virginia was charged with taking money from the union from

SECTOR ELEMENTS

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

2003 to August 2008 by creating fake deposits into her own account and those of family members. She also wrote official credit union checks made payable to family members and to third parties to pay for her personal expenses, according to the charges. The indictment, returned by a federal grand jury in Beckley also alleges a former co-worker aided in the schemes. If convicted, each defendant could receive 30 years in prison, a fine of \$4.8 million and an order of restitution.

Dow Jones Newswire: [US Grand Jury indicts two women on \\$2.4 million credit-union fraud](#)

Other Insider Threat Articles:

- *August 5 – (California)* **San Francisco Chronicle:** [Ex-bank manager pleads guilty in fraud](#). A former San Jose bank manager is expected to spend 6 years in state prison after pleading guilty to embezzling more than \$550,000, primarily from elderly clients, police said.
- *August 10 – (Michigan)* **Grand Rapids Press:** [Details of how Fifth Third Bank worker concealed \\$1 million ATM scheme revealed at sentencing](#). A 27-year-old suspect who concealed an embezzlement scheme in Kalamazoo for 5 years totaling \$950,000 was sentenced to serve 41 months in prison for thievery.
- *August 25 – (Utah)* **Salt Lake Tribune: Prosecutors:** [Mortgage worker got drunk, shot computer server](#). A Salt Lake City, Utah mortgage company employee allegedly got drunk, opened fire on his firm's \$100,000 computer server with a .45-caliber automatic, and then told police someone had stolen his gun and caused the damage.

Criminal Investigation**2 charged in first-of-its-kind credit fraud case**

August 4 – (National)

Federal prosecutors have charged a California woman and Florida man with helping at least three people build false credit histories that allowed them to obtain millions of dollars in mortgage loans. A U.S. attorney said August 5 it is the first time the Department of Justice has charged people with supplying customers with false credit histories. The two were charged with conspiracy to defraud the U.S. government and interstate transportation of funds obtained through fraud. According to the indictment, the two sold false Social Security numbers to a man of Anaheim, California in late 2004 or early 2005. The man then bought numbers for himself and helped at least two Kansas City-area men to obtain others. Prosecutors said the Tampa Bay man increased the credit scores attached to the Social Security numbers by using his companies, South Florida Management Group and Consumer Financial Group, to report false account and payment information to credit bureaus. The men from Anaheim then used the false numbers and credit information to purchase six new homes worth more than \$2.7 million. All three were sentenced earlier this year for their roles in a \$12.6 million mortgage scheme in the Kansas City suburb of Lee's Summit. They were among 18 people who have pleaded guilty to participating in the scheme, which involved 25 upscale homes. Investigators said children are prime targets because most will not use their Social Security numbers to get credit for several years, which means fraudsters can use their numbers for long periods of time undetected.

Associated Press: [2 charged in first-of-its-kind credit fraud case](#)

See also: Associated Press: [New ID theft targets kids' SS numbers](#)

**SECTOR
ELEMENTS**

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

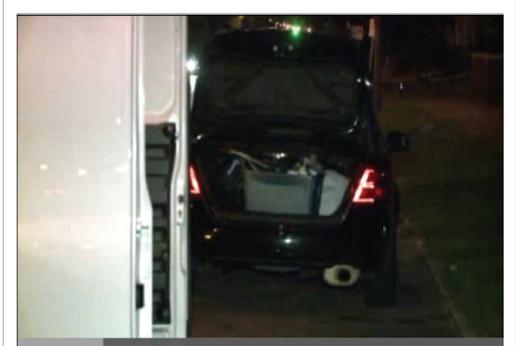
Another car, more cash found in ATM solutions heist*August 6 – (Missouri)*

Just before midnight August 6, FBI agents found a car they have been looking for as well as cash in the trunk. The car was towed from a storage facility near 270 and Lilac in North County. It was taken to the crime lab. Agents and St. Louis, Missouri police were also back at a home on Page Avenue August 5, where they arrested a suspect August 4 and found \$1.5 million in the trunk of his car. He is believed to be one of four men who stole millions from ATM Solutions. The Four armed bandits were clad from head to toe in black

when they overpowered two workers at an ATM-servicing business in St. Louis, August 2, then used an armored vehicle to haul millions of dollars in the well-orchestrated heist.

KTVI 2 St. Louis: [Another car, more cash found in ATM solutions heist](#)

See also; Associate Press: [Masked robbers steal millions in St. Louis heist](#)



KTVI 2 ST LOUIS
The FBI has found another car they believe was involved in the ATM Solutions armed robbery.

Police: Sovereign citizen busted with \$302 billion in fake bonds*August 25 – (Georgia)*

Prosecutors say a \$1 million brick home that a family moved into in DeKalb County, Georgia, is one of at least 19 properties that have been taken over by a sect of anti-government extremists involved in criminal behavior. They call themselves “sovereign citizens” and believe they are immune to state and federal laws. They assert, among other things, that banks cannot own land and that any home owned by a bank — including the thousands throughout Georgia — is free for the taking. The FBI has listed them on the domestic terrorist list, saying their crime of choice is paper terrorism and attempting to disrupt the U.S. economy. Prosecutors said the local sovereign citizens are consistent with other anarchist movements, filing lawsuits and liens on police, government officials and anyone who questions them. They are all born in the United States, but create their own drivers’ licenses, complete with seals for fictitious nations. Many of the suspects have multiple names and a history of not paying taxes.

Investigators in Georgia have tied the sovereign citizens to at least 19 property thefts in DeKalb, Fulton, Gwinnett, Henry, Spalding, Newton and Richmond counties. Police have charged six suspects with violating the Racketeer Influenced and Corruption Organizations Act. Warrants have been issued for another five suspects. The banks that owned the homes were unaware of the deed changes. Another “sovereign citizen” was arrested when he was found to not have a current tag, registration or insurance for his Chevy Avalanche. A search of the truck found \$108,000 hidden under the cup holders. Then officers located several envelopes containing 12 fake surety bonds. The monetary total for all 12 fake bonds was \$302.7 billion, police said.

WSBTV 2 Duluth: [Police: Sovereign citizen busted with \\$302 billion in fake bonds](#)

See also; Atlanta Journal-Constitution: [DA: Paper terrorists stealing homes](#)

Brazen Bandit Bank Robber Arrested in Florida*August 26 – (Florida)*

The FBI in conjunction with Florida state and local law enforcement arrested the Brazen Bandit without incident on August 25. The bandit was charged with bank robbery and with the use of a firearm in the commission of each bank robbery. The FBI had announced a \$25,000 reward for information leading to the arrest of the “Brazen

SECTOR ELEMENTS

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

Bandit,” who shot a Deerfield Beach, Florida bank customer August 18, and was also being sought for a bank heist in Boca Raton August 13. The victim was shot in the neck at the AmTrust Bank at 3600 W. Hillsboro Blvd., at 3:30 p.m. August 18. The gunman, who eluded a police dragnet, was dubbed the Brazen Bandit because of his bold behavior. He jumped a bank counter and snatched money from several drawers, putting it in a black backpack, then shot at the customer. Shortly after shooting the victim, he left the bank, firing several more shots, shattering the window of a nearby tax office. On August 13, the same robber struck PNC Bank’s southeast Mizner branch at 520 S. Federal Highway in Boca Raton.



Federal Bureau of Investigation: [Brazen Bandit Bank Robber Arrested in Florida](#)
See also; South Florida Sun Sentinel: [FBI offers \\$25,000 in case of ‘Brazen Bandit’ bank robberies in Deerfield Beach, Boca Raton](#)

Other Criminal Investigation Articles:

- *August 3 – (Arizona) NACS Online:* [Arizona reports 30 cases of skimmers at gasoline stations](#). During the last 6 months, the Arizona Department of Weights and Measures have reported at least 30 cases of illegal credit-card readers found attached to legitimate card readers at gasoline pumps across the state
- *August 6 – (National) Insurance and Financial Advisor:* [Pa., other securities regulators seeing fraud scheme ‘mutations’](#). Securities regulators in Pennsylvania and other states are warning investors to keep an eye out for “mutations of old schemes and themes” as con artists seek to profit from new federal financial reform legislation.
- *August 9 – (National) LoanSafe.org:* [Minnesota man charged with \\$80 million bank Ponzi scheme](#). A 40-year-old Lakeville man was charged August 9 in federal court in the district of Minnesota with operating a Ponzi scheme that resulted in a total estimated loss of \$79.5 million for 17 lenders.
- *August 11 – (National) AC-360/CNN:* [FBI: ‘Grandad Bandit’ caught](#). A suspected serial bank robber dubbed the “granddad bandit” was arrested August 11 in Baton Rouge, Louisiana, authorities said.
- *August 16 – (Michigan) Tucson Citizen:* [BBB warns of another advance fee loan scam](#). The Better Business Bureau (BBB) has received several complaints over the last few weeks, from consumers across the country, inquiring about a company identified as First National Financial Corp., allegedly located on Grand River Avenue in Brighton, Michigan. The Michigan Office of Financial & Insurance Services has informed BBB that First National Financial Corp. is not an active Michigan corporation and that it does not have a valid license to provide lending and financial services.

Other Industry Reports**PCI updates unveiled**

August 12 – (International)

The long-anticipated new version of the Payment Card Industry Data Security Standard (PCI DSS) includes no new requirements — just clarifications and new guidance on existing components. This is the headline news from the PCI Security Standards Council, which has just released a summary of the expected changes to PCI DSS and the Payment Application Data Security Standard (PA DSS.) A more detailed summary of

SECTOR ELEMENTS

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

the proposed versions 2.0 of PCI DSS and PA DSS will be released in September, prior to the council's community meetings. The final version of the amended standards is expected to be released October 28, then go into effect January 11, 2011.

Bank Info Security: [PCI updates unveiled](#)

SEC charges New Jersey with securities fraud

August 18 – (New Jersey)

U.S. regulators said August 18 they charged the state of New Jersey with securities fraud for not disclosing to municipal bond investors it was underfunding pensions. New Jersey, the first state ever hit with securities fraud charges by the Securities and Exchange Commission (SEC), agreed to settle the case without admitting or denying the findings. The state was not required to pay any civil fines or penalties, but ordered to cease and desist from future violations. New Jersey offered and sold more than \$26 billion of municipal bonds in 79 deals between August 2001 and April 2007, according to the SEC. The offering documents "created the false impression that the Teachers' Pension and Annuity Fund (TPAF) and the Public Employees' Retirement System (PERS) were being adequately funded, masking the fact New Jersey was unable to make contributions without raising taxes, cutting other services or otherwise affecting its budget," the SEC said. "The state of New Jersey didn't give its municipal investors a fair shake, withholding and misrepresenting pertinent information about its financial situation," the director of the SEC's Division of Enforcement said.

Reuters: [SEC charges New Jersey with securities fraud](#)

U.K. fines Zurich Insurance for losing customer data

August 18 – (International)

Britain's financial regulator August 24 imposed a record fine of \$3.5 million on Zurich Insurance PLC for losing confidential data on 46,000 customers. The Financial Services Authority (FSA) said the security breach — which included the loss of identity information and in some cases details of bank accounts, credit cards and insured assets — could have exposed customers to significant losses although there is no evidence the data was misused. The FSA said Zurich Insurance, part of Switzerland's Zurich Financial Services Group, outsourced some data work to the company's South African unit, which lost an unencrypted back-up tape in August 2008. The FSA said the loss was not discovered until 1 year later. "Zurich U.K. let its customers down badly," said the FSA's director of enforcement and financial crime. She said the company failed to oversee the outsourcing arrangement effectively and did not have full control over the data being processed. "To make matters worse, Zurich U.K. was oblivious to the data loss incident until a year later," she said. The fine was the largest ever imposed by the FSA on a single company for a data loss, even though Zurich Insurance got a 30 percent discount from the maximum because it cooperated with the investigation.

Associated Press: [U.K. fines Zurich Insurance for losing customer data](#)

ACH fraud: action plan in Oct.

August 26 – (National)

A working group created by the Financial Services Information Sharing and Analysis Center is honed in on developing best practices for institutions and their customers to help fight corporate account takeover. These incidents, resulting from ACH and wire fraud against business accounts, have been the focus of industry experts for 1 year now. The FBI said that at least one or two incidents of corporate account takeover are being reported each week, resulting in financial losses for businesses and lawsuits against banks. An information security professional at a worldwide bank is leading FS-ISAC's

SECTOR ELEMENTS

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

Corporate Account Takeover Working Group. This is, he says, a 45-member entity dedicated to bringing education and change. Since the formation of the task force in May, 31 financial services companies, including banking institutions, have joined the group. Five industry associations have also joined the task force's working groups, including the American Banking Association, the Independent Community Bankers Association, the Financial Services Roundtable technology arm BITS, NACHA and SWACHA. Eight government and law enforcement agencies have also joined to help in the fight. The working group's short term goals are a September 22 presentation at an FS-ISAC meeting recommendations for advisories and best practices that will be presented during the National Cyber Security Alliance's cyber awareness month in October. The area's being covered are protection, detection, response, and law enforcement involvement.

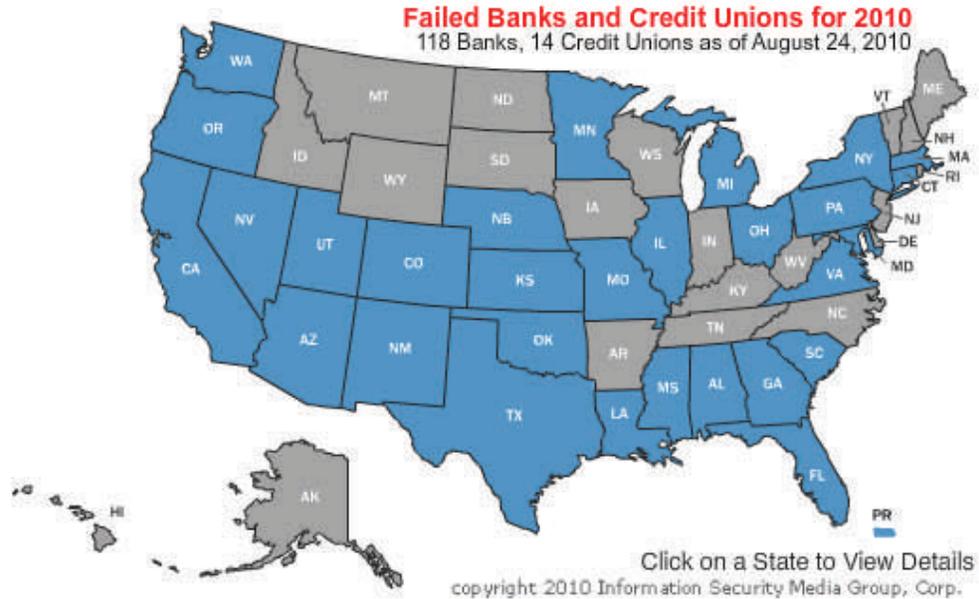
Bank Info Security: [ACH fraud: action plan in Oct.](#)

Other Industry Reports Articles:

- *August 2 – (International)* **Bank Info Security:** [GPS: The future of authentication](#). A new report published by Gartner Research places emphasis on another use for mobile technology in the financial transaction chain — as a security layer for user authentication via global positioning.
- *August 18 – (International)* **DarkReading:** [ITRC Study: Loss of credit card information and merchant data breach cited as priority concerns to consumers](#). The Identity Theft Resource Center (ITRC) announced August 18 that 87 percent of consumers who have made a purchase or bank transaction online in the past month are concerned about the safety of the personal identifying and financial information they transmit. The findings are part of the ITRC's 2010 national survey to monitor trends in "Consumer Concerns about Internet Transactions."
- *August 23 – (National)* **Washington Post:** [Last phase of credit card reform law in place, taking aim at penalty fees](#). The sweeping reform of the credit card industry was completed August 22 as the last pieces of the landmark federal law designed to stop unfair or deceptive practices took effect.
- *August 23 – (National)* **Associated Press:** [Judge approves Countrywide ID theft settlement](#). A federal judge August 23 granted final approval to a settlement between Countrywide Financial Corp. and millions of customers left at high risk for identity theft because of a security breach. Countrywide, now owned by Bank of America, will provide free credit monitoring for up to 17 million people whose financial information was exposed, according to the settlement.
- *August 25 – (International)* **Computerworld:** [Visa offers new guidance on securing payment applications](#). Visa August 24 announced a set of security best practices for vendors of payment applications, and for the systems integrators and resellers responsible for implementing and managing them. The guidelines are designed to address continuing vulnerabilities in the payment chain stemming from insecure implementations of applications that are used in credit and debit card transactions, according to Visa's head of global payment system security.

**SECTOR
ELEMENTS**

- [Cyber Threats](#)
- [Physical Security](#)
- [Insider Threats](#)
- [Criminal Investigation](#)
- [Other Industry Reports](#)

Featured Incidents: Bank and Credit Union Closings, August 2010

No banks or credit unions were closed on August 27 keeping the number of failed institutions to 132 so far in 2010. Click on the following picture to open to an interactive map of the United States for more information on state by state bank and credit union closings. For more information on all bank closures for the month of August, please click on one of the following links.

For more information on bank and credit union failures, see:

[One bank fails on Aug. 6](#)

[One bank fails on Friday, Aug. 13](#)

[Eight banks closed on Aug. 20](#)

Your comments and suggestions are highly valued. Please send us feedback at:
cikr.productfeedback@hq.dhs.gov

This report is posted regularly to the [Homeland Security Information Network Critical Sectors](#) portal. If you would like to become a HSIN-CS member, please contact:
CIKRISAccess@DHS.gov.