



FINANCIAL SERVICES SECTOR OPEN SOURCE DIGEST

July 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

Account Takeover: The new wrinkle

July 8 – (California)

The owner of Village View Escrow Inc. of Redondo Beach, California, said her company fell prey to a “corporate account takeover” scheme after hackers were able to break into the company’s network, steal bank credentials, and send 26 consecutive wire transfers out of the country, totaling \$465,000. Dual controls were not used by the business, but an e-mail verification service offered by Professional Business Bank of Pasadena, California, was successfully disabled by the criminals. The scheme, which occurred in March, is currently under investigation, and no litigation has yet been filed. Security experts familiar with the Village View Escrow case say there are lessons to be learned by other institutions and businesses to avoid corporate account takeover via ACH and wire fraud. One area where the principals in the Village View Escrow case fell short was allowing changes to be made to online banking alerts without verifying they were legitimate. When the hackers disabled the email notification at Professional Business Bank, an alert message should have automatically been generated and sent to the area responsible for applications and systems maintenance.

BankInfo Security: [Account Takeover: The new wrinkle](#)

Newest attack on your credit card: ATM shims

July 11 – (International)

Shimming is the newest con designed to skim a person’s credit card number, PIN and other info when one swipes a card through a reader like an ATM machine. According to Diebold, “The criminal act of card skimming results in the loss of billions of dollars annually for financial institutions and card holders. Card skimming threatens consumer confidence not only in the ATM channel, but in the financial institutions that own compromised ATMs as well.” Shimming works by compromising a perfectly legitimate card reader (like an ATM) by inserting a very thin flexible circuit board through the card slot that will stick to the internal contacts that read card data. The shim is inserted using a “carrier card” that holds the shim, inserts it into the card slot and locks it into place. The carrier card is then removed. Once inserted, the shim

**SECTOR
ELEMENTS**

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

is not visible from the outside of the machine. The shim then performs a man-in-the-middle attack between an inserted credit card and the circuit board of the ATM machine. **Network World:** [Newest attack on your credit card: ATM shims](#)

Zeus baddies unleash nasty new bank Trojan

July 13 – (International)

Hackers have created a new version of the Zeus crimeware toolkit that is designed to swipe bank log-in details of Spanish, German, U.K. and U.S. banks. The malware payload, described by CA as Zeus version 3, is far more selective in the banks it targets. Previous versions targeted financial institutions around the world while the latest variant comes in two flavors: one that only target banks in Spain and Germany, and a second that only targets financial institutions in the United Kingdom and United States. In addition, the latest version of Zeus contains features that make it far harder for security researchers to figure out what the malware is doing. Zombie drones on the Zeus botnet operate on a need to know basis, CA explains. “In earlier versions, Zeus handles this configuration file in a way that security researchers can easily manage to reverse engineer and capture the actual full configuration content,” writes a senior research engineer with CA’s Internet Security Business Unit. “This is no longer the case for the latest Version 3, which is already in the wild. Command and control systems associated with the bot are “mostly hosted in Russia.”

The Register: [Zeus baddies unleash nasty new bank Trojan](#)

ZeuS Trojan attempts to exploit MasterCard, Visa security programs

July 14 – (International)

The notorious ZeuS banking Trojan is showing off a new trick: Popping up on infected computers with a fake enrollment screen for the “Verified By Visa” or “MasterCard SecureCode Security” programs. The real and legitimate Visa and MasterCard card-fraud prevention programs have cardholders use a password when making card-based purchases online as an additional means of security. The Zeus Trojan, with its ever-growing capability to steal financial information and execute unauthorized funds transfers, has recently been seen attacking banking customers on infected machines by displaying a fake “Verified by Visa” enrollment screen, or its MasterCard counterpart SecureCode, trying to lure victims into a fraudulent online enrollment action that would end up giving criminals sensitive financial data.

Network World: [ZeuS Trojan attempts to exploit MasterCard, Visa security programs](#)

Colorado warns of major corporate ID theft scam

July 16 – (Colorado)

Colorado’s secretary of state and other officials are warning the state’s 800,000 or so registered businesses to watch out for scammers who have been forging business identities to make fraudulent purchases from several big-box retailers in recent months. So far, at least 35 businesses in the state have had their corporate identities misused to open fraudulent credit accounts at retailers such as Home Depot, Lowe’s, Office Depot, Apple, and Dell. According to the Colorado Bureau of Investigation (CBI), the scammers have made at least \$750,000 in fraudulent purchases from Home Depot alone after opening up lines of credit. Five people in California have been arrested in connection with the scam, said the CBI agent in charge of the fraud unit. It is unclear how many other businesses may have been affected. But the problem appears to be growing, with several more groups likely involved in similar scams, including one in Texas. The thefts were possible because of what appears to have been a wide open business registration system at the Colorado secretary of state’s office. Colorado, like

SECTOR ELEMENTS

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

other states, requires companies to register. In Colorado's case, however, not only does the state allow anyone to view the record — it also allows just about anyone to alter or update it. The state site requires no username or password for access to a company's registration information, which means that anyone with access to the site can make changes. The identity thieves used this hole to alter the contact and other registration information for several companies. According to the agent in charge, many of the companies targeted appear to have been smaller and medium-sized firms and, in some cases, defunct companies. Once the registration information was changed, the scammers then used the forged identity to make online applications for lines of credit with the retailers.

Computerworld: [Colorado warns of major corporate ID theft scam](#)

Russian gang uses botnets to automate check counterfeiting

July 28 – (International)

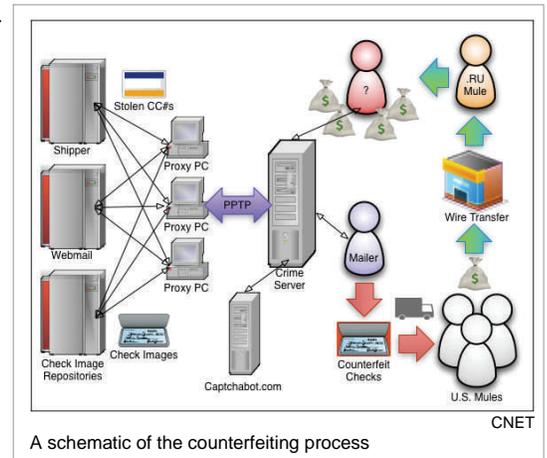
The director of malware research for Atlanta-based SecureWorks has uncovered a sophisticated check counterfeiting ring that uses compromised computers to steal and print millions of dollars worth of bogus invoices and then recruit money mules to cash them. The highly automated scheme starts by infiltrating online check archiving and verification services that store huge numbers of previously cashed checks. It then scrapes online job sites for email addresses of people looking for work and sends personalized messages offering them

positions performing financial transactions for an international company. The scammers then use stolen credit card data to ship near exact replicas of the checks to those who respond. The director was able to track the operation by infecting a lab computer and observing its interactions with command and control channels. A database file the criminals carelessly exposed showed that 3,285 checks had been printed since June of 2009 and 2,884 job seekers had responded to the employment offer. Assuming each check was written in amounts of \$2,800, a threshold sum that brings increased scrutiny to transactions, the director estimates the checks were valued at about \$9m.

The Register: [Russian gang uses botnets to automate check counterfeiting](#)

Other Cyber Threats Articles:

- *July 2 – (National) Bank Info Security:* [FDIC targeted by phishers—again](#). On July 2, the Federal Deposit Insurance Corporation (FDIC) warned consumers and financial institutions that bogus emails claiming to be from the FDIC are arriving in inboxes. This is the fourth time within a year that the federal banking regulator has issued alerts about phishing emails using its brand.
- *July 8 – (International) Associated Press:* [South Korean government websites, banks hit by suspected cyber attack](#). Suspected cyber attacks paralyzed web sites of major South Korean government agencies, banks and Internet sites in a barrage that appeared linked to similar attacks in the United States, South Korean officials said July 6. The sites of the presidential Blue House, the Defense Ministry, the National Assembly, Shinhan Bank, Korea Exchange Bank and top Internet portal



SECTOR ELEMENTS

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

Naver went down or had access problems, said a spokeswoman at Korea Information Security Agency.

- *July 12 – (National) Brickhouse Security: [ATM skimmer attacks now targeting bank PIN numbers](#).* Another new twist on ATM skimming uses a new tool that goes on top of the ATM's PIN pad and like the ATM skimmer, users are unable to tell that anything is out of the norm. The plastic PIN pad captures the PIN as it is typed in, and many automatically text message the stolen PINs directly to the scammer's cell phone.
- *July 13 – (International) IDG News Service: [IBM takes blame for massive bank system failure](#).* IBM took responsibility for a major IT system failure suffered by one of Singapore's largest banks July 5, saying an employee's error caused the outage.
- *July 16 – (International) Help Net Security: [Bank of America phishing scam](#).* ScanSafe reports a new phishing scam on the Bank of America Web site where the link provided for signing in to online banking points to a gramsbbq.org/bain (a Web site belonging to a barbecue establishment in California), which in turn automatically redirects tusers to a phishing page hosted on chasingarcadia.com – another legitimate, but compromised, site belonging to a Canadian band.
- *July 19 – (National) Bank Info Security: [BP aftermath: Fear of fraud](#).* Financial institutions in states along the Gulf of Mexico are taking action to prepare for the long-term financial impact of the BP oil spill — including fraud attempts against customers. One Alabama bank recently reported a phishing scheme that enticed customers to click fraudulent links, using BP relief and recovery funds as a guise. All Alabama Bankers Association (ABA) banks have been warned of this scheme, according to the ABA's CEO.
- *July 23 – (National) Bank Info Security: [FDIC: Top 5 fraud threats](#).* The chief of the FDIC Cyber Fraud and Financial Crimes Section recently released his top five list of fraud threats of concern to: 1. Malware and Botnets; 2. Phishing; 3. Data Breaches; 4. Counterfeit Checks; 5. Mortgage Fraud.
- *July 27 – (International) eWeek: [Citi, Apple disclose iPhone app security flaw](#).* Banking giant Citigroup and iPhone maker Apple are encouraging users who downloaded Citi's banking application for the smartphone to upgrade to a new version after a security flaw was discovered in the application. The flaw accidentally saves personal information, including access codes, bill payment information and even bank account numbers, onto the iPhone or any computer with it has been synchronized with.

Physical Security

Police: Man drove car bomb into a bank

July 17 – (Illinois)

A man is in custody on charges of felony arson after allegedly driving a car bomb into a Lockport, Illinois bank July 16. The 48-year-old suspect, of Blue Island, Illinois, was arrested after witnesses at the scene identified him, the Lockport Police Department said. He drove his car into the front entrance of a PNC bank, police said. The car exploded as the suspect walked away, police said, adding that he used the same material found in fireworks. No injuries were reported because the



SUN TIMES
The Cook County bomb squad at the PNC bank.

SECTOR ELEMENTS

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

bank was closed and unoccupied, authorities said. The suspect is being held on charges of felony arson and felony criminal damage to property with an incendiary device. His motive is unknown, according to police.

CNN: Police: [Man drove car bomb into a bank](#)

Gunman makes terror threat, robs downtown office

July 22 – (Illinois)

According to police, a gunman threatened to detonate a car bomb and claimed links to al-Qaeda while robbing an American Express office on the Magnificent Mile in Chicago July 21. A man approached an employee in the American Express travel service office at 605 N. Michigan Ave. at first trying to buy euros and then showing her a gun in his waistband as he demanded money, said the Near North District captain. The man told the woman he was a member of al-Qaeda, pointed to a vehicle across the street, and claimed there was a bomb in the car and that he could detonate it with his cell phone. The man, described as 6-foot tall, 200 pounds and possibly of Middle Eastern descent, went on to instruct all the office employees they had three minutes to hand over all the money they had. Police believed the robber made off with 15,000 euros in addition to other currency. He fled the scene on foot, heading south on St. Clair Street, according to the police captain. No one was hurt. When police arrived, the vehicle carrying the alleged bomb was gone. The man had spent several hours in the office July 20, employees told police. He had tried to obtain euros but was unable to because the office did not have a sufficient amount, the spokesman said. The man told the employees that they had better have plenty of euros on hand when he returned.

Chicago Tribune: [Gunman makes terror threat, robs downtown office](#)

‘Ho Hum Bandit’ hits 9th SoCal bank

July 27 – (California)

The “Ho Hum Bandit” latest robbery was reported at 9:22 a.m. July 24 at 310 Genneyre Street, according to the Laguna Beach Police department. This is the ninth robbery attributed to the suspect. The “Ho Hum Bandit,” named for his unassuming manner, is described as Caucasian in his 30s, 5-foot 9-inches tall with a medium build. He walked up to a teller and handed her a note demanding money, according to police. The “Ho Hum Bandit” is believed to be responsible for five robberies in San Diego and four in Orange County. He robbed the same Orange County Citibank on East Coast Highway in Newport Beach July 22 and June 11 according to FBI officials. In all of the robberies, the suspect hands the teller a note and demands money. He has already escaped with thousands of dollars in cash, although no specific amount has been released by the FBI.

KTLA 5 Los Angeles: [‘Ho Hum Bandit’ hits 9th SoCal bank](#)

**Other Physical Security Articles:**

- *July 1 – (Oregon)* **KPTV 12 Portland:** [Bomb threat made at Sandy bank.](#) A man who robbed a U.S. Bank branch in Sandy, Oregon, threatened employees with a gun and made a bomb threat as he left the bank, police said. The man escaped with an unknown amount of money and told bank employees he was going to blow up the

SECTOR ELEMENTS

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

bank, according to a representative with the Sandy Police Department. He left behind a paper bag which he claimed was a bomb.

- *July 16 – (Tennessee) Chattanooga Times Free Press: [Bomb threats force evacuations at Home Depot, Bank of America](#).* Telephoned bomb threats July 16 forced the evacuation of two businesses near Northgate Mall in Chattanooga, Tennessee, a Chattanooga Police Department spokeswoman said. Both the Home Depot at 1944 Northpoint Blvd. and the Bank of America branch at 1945 Northpoint Blvd. were searched and no explosive devices were found. Workers and customers returned to the buildings after about 45 minutes. Police are working to locate the caller or callers.
- *July 26 – (New York) Long Island Press: [Man armed with fake bomb robs West Babylon bank](#).* A man wearing what appeared to be an explosive device strapped to his body walked into a Chase Bank branch in West Babylon, New York, early July 26 and demanded cash. The robber was given cash and fled through the back door. The robber discarded the device behind the shopping center where the bank is located. Emergency service section officers responded and determined the device was not a real bomb.

Insider Threats**41% of IT pros admit to snooping on confidential information**

July 7 – (International)

The results of a Cyber-Ark global survey show that 35 percent of respondents believe their company's highly-sensitive information has been handed over to competitors. Thirty-seven percent of the IT professionals surveyed cited ex-employees as the most likely source of this abuse of trust. 28 percent suspected "human error" as the next most likely cause, followed by falling victim to an external hack or loss of a mobile device/laptop, each at 10 percent. The most popular information shared with competitors was the customer database (26 percent) and R&D plans (13 percent). To address vulnerabilities related to human error that could expose a proprietary database or financial information, organizations must employ additional layers of control such as the ability to grant privileges to sensitive data and systems on-demand. This limits "innocent" mistakes by allowing access to information only when users need it to perform a particular task or query. The research also confirmed that snooping continues to rise within organizations both in the United Kingdom and the United States. Forty-one percent of respondents confessed to abusing administrative passwords to snoop on sensitive or confidential information – an increase from 33 percent in both 2008 and 2009.

Help Net Security: [41 % of IT pros admit to snooping on confidential information](#)

Other Insider Threat Articles:

- *July 20 – (South Carolina) Associated Press: [2 plead guilty in SC bank fraud case](#).* Two former bank officials in South Carolina have pleaded guilty to fraud charges. Multiple media outlets reported that the 58-year-old and 44-year-old suspects pleaded guilty to conspiracy to commit bank fraud in federal court in Florence July 19. The two admitted falsifying information on loan applications so Myrtle Beach banks would approve mortgages that wound up in foreclosure.
- *July 20 – (Oklahoma) Oklahoman: [Employee among 3 arrested in Shawnee bank robbery](#).* Three men arrested July 16 and 17 face federal bank robbery charges, as they are accused of robbing a Shawnee, Oklahoma bank July 8,

SECTOR ELEMENTS

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

according to the FBI. All three men live in Pottawatomie County. Investigators searched homes in Shawnee and Tecumseh before the arrests. The special agent said one of the suspects was employed at the bank, but could not comment further. First United Bank was robbed July 8 by a masked robber who fled in a small black car with a driver.

Criminal Investigation

Six indicted in Colorado on bank fraud charges

July 12 – (National)

A national, bank-fraud ring, originally based in California, has been broken up in Colorado after a state grand jury indicted six of the members, the Colorado attorney general announced July 12. According to the indictment, the six individuals scammed thousands of dollars from Colorado banks and businesses. Also hit were banks and firms in Utah, Nebraska, North Dakota, Illinois, and Wisconsin. The indictment alleges the ring made fake credit cards and obtained 1-800 numbers, printed on the back of cards. When cashiers at the bank or sales people at the stores were unable to authenticate the fake credit cards, they would call the 800 number, which rang to other members of the ring, according to the indictment. The attorney general said ring members answering the phones would convince bank and store employees that the cards were legitimate, thus allowing for purchases and cash advances. Among the businesses hit were Enterprise Rent-a-Car in Aurora, Colorado and Revolution 2, a clothing store in Aurora. Among the Colorado banks targeted were the Dolores State Bank, Cortez; the Montrose Bank, Montrose; Valley Bank & Trust, Brighton; and the Colorado Community Bank in Castle Rock. The attorney general said losses exceeded \$65,000.

Denver Post: [Six indicted in Colorado on bank fraud charges](#)

Fla. man indicted in \$880M Ponzi scheme

July 14 – (National)

A Florida man was indicted July 14 in an alleged \$880 million Ponzi scheme tied to a phantom grocery-distribution business, authorities in New Jersey said. The 41-year-old suspect of Miami Beach, who is the former owner and chief executive officer of Capitol Investments USA Inc., is accused of soliciting hundreds of millions of dollars from people in New Jersey and elsewhere who thought they were investing in his wholesale grocery-distribution enterprise. Federal authorities allege Capitol had no active wholesale grocery business at the time, and from 2005 to 2009 the suspect used new investor funds to make principal and interest payments to earlier investors. He allegedly siphoned off \$35 million to underwrite his lavish lifestyle. The July 14 indictment is a follow-up to a criminal complaint that led him to surrender to FBI and Internal Revenue Service agents April 21. He is now charged with securities fraud, money laundering and conspiracy to commit securities and wire fraud.

UPI: [Fla. man indicted in \\$880M Ponzi scheme](#)

Other Criminal Investigation Articles:

- *July 14 – (Florida)* **Miami Herald:** [Six arrested in another South Florida mortgage fraud scam](#). Six South Floridians were arrested July 14 on charges of grand degree theft for their involvement in a mortgage scam that netted more than \$2 million in fraudulent mortgages, the state department of financial services division of insurance fraud said.

**SECTOR
ELEMENTS**

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

- *July 21 – (New York) Associated Press: [NY ex-bank computer tech gets prison in \\$1M scam](#).* A computer technician who used a three-month job at a New York bank as a launching pad for almost a decade of theft from charities has been sentenced to 5 to 15 years in prison. The suspect told a judge July 21 he felt “shame, guilt and remorse” for his scheme. He admitted last month to stealing 2,000 bank employees’ identities in 2001.
- *July 22 – (Illinois) Chicago Southtown Star: [Feds crack \\$35M mortgage fraud scheme](#).* A south Chicago man is among seven people indicted July 22 in an alleged \$35-million mortgage fraud scheme involving more than 120 residential properties. The suspect allegedly bought and sold homes, recruiting others to act as purchasers, costing lenders and financial institutions at least \$16 million in losses on mortgage loans that were not repaid or fully recovered through foreclosure, according to a release from the U.S. Attorney’s office.
- *July 23 – (National) WIVB 4 Buffalo: [Five indicted for bank fraud conspiracy](#)* Five people have been indicted for bank fraud conspiracy that spanned from July 2009 until December 2009. A federal grand jury in Buffalo, New York has returned a four-count indictment charging the five suspects, all residing in New York or Florida, with conspiracy to commit bank fraud. The five are also charged with production and use of counterfeit-access devices, possession of device-making equipment and aggravated identity theft. The charges carry a mandatory minimum penalty of two years in prison and a maximum of 30 years, a fine of \$1 million or both.

Other Industry Reports**Bank Failures: 2010 Pace Exceeds 2009***July 6 – (National)*

Although there were no bank failures to report on the Fourth of July, midway through 2010, there have been more than twice the number of failed banks and credit unions as was seen at this same point in 2009. There have been 96 failures — 86 banks and 10 credit unions — so far in 2010. At the end of June 2009, there were 45 failures en route to a total of 171 failed institutions for the year. Of the 86 banks to fail so far in 2010, the largest is Westernbank Puerto Rico, which closed in April and had approximately \$11.94 billion in total assets. Of 10 credit unions to be closed, acquired or placed into conservatorship, the largest is Arrowhead Central Credit Union of San Bernardino, California. This full service credit union was placed into conservatorship in June, with assets of \$876 million. Florida leads the nation with 14 failures. Next on the list are: 12 failures in Illinois, nine in Georgia and California, seven in Washington State, and six in Minnesota. Meanwhile, with slightly fewer than 800 financial institutions now on the Federal Deposit Insurance Corporation’s “troubled banks” list — up from 90 in 2008 — the likelihood of further bank closings is very real.

Bank Info Security: [Bank Failures: 2010 Pace Exceeds 2009](#)**Europe votes to send secret bank data to U.S. authorities***July 8 – (International)*

The European Parliament July 8 gave its consent to the controversial Swift agreement that will allow the bulk transfer of European citizens’ financial data to U.S. authorities as part of the Terrorist Finance Tracking Program (TFTP). The Parliament originally rejected the agreement in February over concerns about civil liberties. But after both the European Commission and the European Council approved the plan, Parliament came under increased pressure to allow the agreement to go ahead. The commission revised

SECTOR ELEMENTS

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

the original proposal with concessions to Parliament and its members voted to approve the revised proposal by 484 to 109. There were 12 abstentions. In exchange for Parliament's support, the new agreement acknowledges the ambition for the European Union to establish a system equivalent to the TFTP, which could allow for data extraction to take place on EU soil. The United States has committed to providing assistance in setting up such a system.

IDG News Services: [Europe votes to send secret bank data to U.S. authorities](#)

FDIC regains backup authority

July 14 – (International)

In a move seen as strengthening its oversight powers, the FDIC board voted recently to restore the agency's backup supervisory authority. This means that the FDIC can now step in and examine large banks currently under the supervision of other banking regulators, including the Office of the Comptroller of the Currency and the Office of Thrift Supervision. The agency had been given this power back in 1983, following some costly failures of banks that the FDIC had little or no prior knowledge of, said a former FDIC chairman. This power remained in place until 1993, when the board tempered the FDIC's backup supervisory program by requiring prior board approval before FDIC examiners could exam a national bank or thrift. The revised Memorandum of Understanding gives the FDIC backup supervision authority under an expanded list of circumstances.

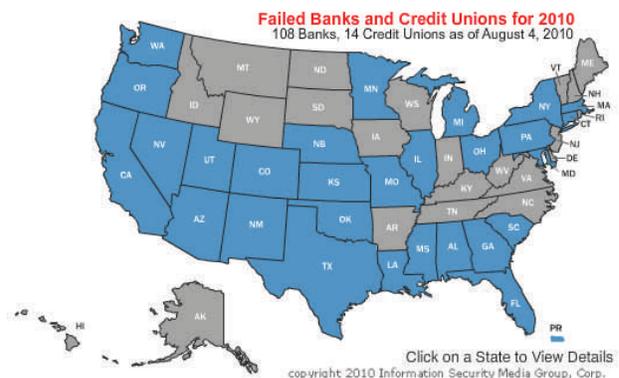
Bank Info Security: [FDIC regains backup authority](#)

Featured Incidents: Bank and Credit Union Closings, July 2010

As of August 4, 2010 there have been 108 Bank and 14 Credit Union closings. 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 July, please click on one of the following links.

For information on bank and credit union failures, see Bank Info Security:

[Four banks closed on July 9, 6 banks closed on July 16, and 5 banks, 2 credit unions fail July 30.](#)



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