



# FINANCIAL SERVICES SECTOR OPEN SOURCE DIGEST

November 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

### Phishing scam targets military families

*November 2 – (National)*

A new phishing scam is taking aim at members of the U.S. military and their families, using unsolicited e-mails purportedly from [United States Automobile Association](#) (USAA), one of the nations largest financial services and insurance companies, to trick people into divulging their personal information to identity thieves. USAA and the [Navy Federal Credit Union](#) in May were hit by a similar phishing scam that also attempted to extract Social Security numbers, credit card numbers, birth dates and other information used to either pilfer bank accounts or steal unsuspecting users' identities. This time around, according to an advisory on security software maker AppRiver's Web site, the con artists are sending a slew of unsolicited e-mails with subject titles, such as "USAA Notification" or "Urgent Message for USAA customer" in the hope of getting just a small fraction of a percentage of recipients to click on a link embedded in the missive. **eSecurity Planet:** [Phishing scam targets military families](#)

### Firm finds security holes in mobile bank apps

*November 4 – (National)*

A security firm disclosed holes November 4 in mobile apps from Bank of America, USAA, Chase, Wells Fargo, and TD Ameritrade, prompting a scramble by most of the companies to update the apps. "Since Monday [November 1], we have been communicating and coordinating with the financial institutions to eliminate the flaws," research firm viaForensics wrote in a post on its site. "The findings we published reflect testing completed on November 3. Since that time, several of the institutions have released new versions and we will post updated findings shortly." The company had reported its findings to the Wall Street Journal earlier in the day. On November 3, viaForensics went public with problems in PayPal's iPhone app, spurring the online payment provider to action. Specifically, viaForensics concluded that: the USAA's Android app stored copies of Web pages a user visited on the phone; TD Ameritrade's iPhone and Android apps were storing the user name in plain text on the phone; Wells Fargo's Android app stored user name, password, and account data in plain text on the phone; Bank of America's Android app saves a security question (used if a user was accessing the site from an unrecognized device) in plain text on the phone; and Chase's

**SECTOR  
ELEMENTS**

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

iPhone app stores the username on a phone if the user chose that option.

**Network World:** [Firm finds security holes in mobile bank apps](#)

## New, improved Trojans target banks

*November 8 – (National)*

Security researchers are warning financial institutions about the Qakbot Trojan, a rare kind of malware that is allegedly infiltrating large banks and other global financial institutions. It is unlike other types of malware because it has the ability to spread like a worm, but still infect users like a Trojan. Named for its primary executable file, \_qakbot.dll, the Trojan is not new, but its qualities and difference in attack set it head and shoulders above other more well-known Trojans, such as Zeus, in that it can infect multiple computers at a time. It is the only Trojan known to exclusively target U.S. banks, said an RSA security researcher. The more well-known Trojans and their variants, Zeus and Spyeeye, are all available for sale on the black market, said the researcher who is head of new technologies, consumer identity protection at RSA, the security division of EMC. First discovered by Symantec in 2007, Qakbot is likely being run by one group. It is likely an organized crime group developed it, focusing on their own specific methods, and tailored the Trojan to a specific segment -- large banks and their commercial customers.

**Bank Info Security:** [New, improved Trojans target banks](#)

## Russian banks probed for involvement in U.S. hacker attacks

*November 16 – (International)*

Russia's financial watchdog is looking into the activities of its banks and other financial institutions for possible involvement in hacker attacks in the United States, the head of the agency said November 16. "We are working together with the Americans. The question we are looking at is whether our Russian financial institutions could have been involved in these [money laundering and hacking] operations," the head of the Russian financial monitoring service said at a meeting with the Russian prime minister.

In mid-October, a U.S. court found two Russians guilty of staging a cyber attack on banks and stealing money. The two Russians were members of the group behind a scam to penetrate companies' computer networks, steal bank details, and siphon off cash. Their partners in crime have yet to be identified.

**RIA Novosti:** [Russian banks probed for involvement in U.S. hacker attacks](#)



RIA NOVOSTI  
Russian banks are being probed for involvement in U.S. hacker attacks.

## Cleveland Federal Reserve hacked

*November 19 – (National)*

A 32-year-old Malaysian man was arrested shortly after his arrival last month at John F. Kennedy International Airport in New York City. Authorities said he hacked into the Cleveland Federal Reserve Bank and several other computer systems, including a defense contractor. The Malaysian national faces a four-count indictment that charges him with hacking into computer systems, stealing more than 400,000 credit and debit card numbers. "Cybercriminals continue to use their sophistication and skill as hackers to attack our financial and national security sectors," said the U.S. Attorney for the Eastern District of New York. The suspect's arrest comes just 1 month after authorities arrested a big cyber crime gang in the United States and Europe for similar crimes. When the suspect arrived in New York October 21, he was arrested hours later by Secret Service agents. The suspect, who is being held in pre-trial detention, "made a career of

**SECTOR ELEMENTS**

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

compromising computer servers belonging to financial institutions, defense contractors and major corporations, among others, and selling or trading the information,” said the U.S. Attorney for the Eastern District of New York.

**Bank Info Security:** [Cleveland Federal Reserve hacked](#)

**For more information; see also Straits Times:** [M’sian hacker ‘not alone’](#)

**Other Cyber Threats Articles:**

- *November 4 – (National)* **Wisconsin State Journal:** [International sting nabs two men in Wisconsin for alleged computer virus scheme](#). Two Moldovan men who allegedly took part in a complex scheme to siphon millions of dollars out of American bank accounts were arrested November 3 in Wisconsin, and are to be shipped to New York to face charges. The two suspects appeared November 4 in U.S. District Court in Madison where they agreed to be sent back to New York City to face charges stemming from the use of computer viruses to raid bank accounts through the Internet.
- *November 8 – (National)* **InformationWeek:** [Financial data at risk in development: A call for data masking](#). An Informatica sponsored study conducted by the Ponemon Institute surveyed 437 senior IT professionals in the financial services industry whose firms have been engaged in application testing and development in order to better understand if the risk of using real data in development is being addressed. An overlooked privacy risk is the vulnerability of personal and business information used for testing and application development. During the test and development phase of new software, real data — including financial records, transactional records, and other personally identifiable information (PII) — is being used by as many as 80 percent of organizations.
- *November 16 – (National)* **Insurance Journal:** [Cyber crime reaches milestone](#). Complaints about Internet crimes have reached a milestone. On November 9, the Internet Crime Complaint Center (IC3) logged its 2 millionth consumer complaint alleging online criminal activity. The IC3, a partnership between the FBI and the National White Collar Crime Center, became operational in May 2000 and received its 1 millionth complaint 7 years later, on June 11, 2007. It took half that time to receive the 2 millionth complaint.
- *November 19 – (National)* **KOMO 4 Seattle:** [Secret Service: Seattle cyber attack larger than first thought](#) **Complaints**. Federal agents now say the Seattle, Washington, cyber attack was a much bigger crime than first thought. A U.S. Secret Service spokesman said more than 1,000 accounts may have been compromised. The scheme appears to involve the sale or distribution of stolen account information to numerous individuals across the country, as well as foreign countries. Those individuals used the information to make purchases.

**Physical Security****Robbers caught in hail of gunfire**

*November 3 – (Illinois)*

On November 2, a 23-year-old woman and a 36-year-old man, both wearing stocking masks and armed with automatic handguns, burst into a US Bank branch in Chicago, Illinois, and demanded cash, police and the FBI said. But a quick-thinking customer who ran from the bank as the heist began dialed 911, and Homewood and Hazel Crest police officers were waiting for the robbers when they left moments later. In “an exchange of gunfire” with the officers, the female bank robber hastily abandoned a blue backpack

**SECTOR  
ELEMENTS**

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

stuffed with thousands of dollars in cash and was shot in the shoulder as she attempted to flee, and she and the man were arrested. A third suspect, the male getaway driver, was on the run. None of the 10 customers and bank were hurt.

**Chicago Sun-Times:** [Robbers caught in hail of gunfire](#)

**FBI rookie helps nab swine flu bandit**

*November 12 – (Illinois)*

A rookie FBI agent with 1 week on the job is being credited with helping to nab the serial bank robber dubbed the “Swine Flu Bandit” at a Chicago, Illinois bank. The rookie and a senior agent, members of the FBI’s Violent Crimes Task Force, were inside a First American Bank branch at 1241 Wabash Avenue November 10 working the case when lucky timing and good police work collided.

While talking to bank personnel and getting security video because they believed the bandit had previously cased the bank, the junior agent saw a man outside who matched the robber’s description, an FBI spokesman said. The agents

walked outside and arrested the man who, fitting the size of the Swine Flu Bandit and wearing the same clothes and hat worn in the most recent stick-ups, was also found to be carrying a 9mm semi-automatic handgun in his pocket. It is believed the 28-year-old suspect was preparing to hold up the bank when he was arrested.

**WMAQ 5 Chicago:** [FBI rookie helps nab swine flu bandit](#)

See also, **WLS 890 AM Chicago:** [Feds: ‘Swine Flu’ bank robber was B of A employee](#)

**Geezer Bandit strikes again**

*November 16 – (California)*

A serial bank robber responsible for 10 bank robberies in California in San Diego County and one in Temecula, has apparently struck for the 12th time, this time in Kern County, the FBI said. The “Geezer Bandit” is believed to have held up a Bank of America branch office in Bakersfield November 12, an FBI Special Agent said. Authorities dubbed the serial thief the Geezer Bandit because he appears to be a man in his 70s or 80s. However, authorities have said it was possible the bandit was actually a younger person disguised by a realistic Hollywood-style mask and rubber hand coverings. He first appeared in August 2009 and has been the subject of several Facebook fan pages. November 12’s robbery in Bakersfield marks the Geezer Bandit’s first robbery since June 24, when he held up a bank in Temecula.

**Bay City News Service:** [Geezer Bandit strikes again](#)

**Cleveland man suspected of robbing four banks**

*November 18 – (Ohio)*

Authorities are looking for a man they believe has robbed four Cleveland, Ohio-area banks since October. The 34-year-old male, who hails from Cleveland, is wanted on federal bank robbery charges. The FBI said the suspect is a suspect in the robbery of the Huntington Bank on Coventry Road in Cleveland Heights, November 17, according to the FBI. Authorities said the suspect is also suspected of robbing a PNC Bank in North Randall, a US Bank in Warrensville Heights, and a Charter One Bank in Maple Heights. All of the robberies occurred over the last few weeks. The suspect is a black male and is about 6-foot-2, and weighs between 180 and 200 pounds. He was last seen wearing a dark brown hat, beige jacket, and dark green shirt.

**WEWS 5 Cleveland:** [Cleveland man suspected of robbing four banks](#)

**SECTOR  
ELEMENTS**

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

## Escondido bomb maker had largest stash of home-made explosives ever found in U.S.; suspect also accused of bank robberies

*November 22 – (California)*

A 54-year-old male from Escondido, California pleaded not guilty to 28 criminal counts November 22. He is accused of possessing destructive explosive devices and the ingredients to make them, as well as robbing two local banks. The deputy district attorney told the judge that the suspect's home was "a bomb factory" containing "the largest quantity of these types of homemade explosives at one place in the United States." Those materials pose "a huge danger to officers and the public," she said. In addition to bombs and explosive materials, authorities found multiple detonators, grenades, and shrapnel.

**East County Magazine:** [Escondido bomb maker had largest stash of home-made explosives ever found in U.S.; suspect also accused of bank robberies](#)

### Other Physical Security Articles:

- *November 5 – (Colorado)* **Denver Post:** [Bank robber's bomb threat bogus](#). A well-dressed robber left what he claimed was a bomb on the counter of an Edgewater, Colorado bank November 4. The metal box, however, contained nothing dangerous, the Jefferson County bomb squad determined.
- *November 9 – (Illinois)* **Chicago SouthtownStar:** [Acid threat used in bank heist](#). Police said the November 6 robbery of a TCF Bank in Chicago, Illinois where a robber threatened a bank teller with acid follows a rash of similar crimes against the bank chain. The robbery occurred about 10:30 a.m at a TCF branch at 3220 Chicago Road, police said. According to officials, a man walked up to a teller and claimed he had a container of acid inside his coat. He said he wanted only \$100 bills and threatened to toss the acid on the teller if she sounded any alarm, police said. No one saw a container with acid.
- *November 10 – (Kansas)* **Kansas City Star:** [Teller found tied to chair after being kidnapped, forced to open bank](#). A teller at an Overland Park, Kansas, bank told authorities he was kidnapped November 10 and driven to the bank so his kidnapper could rob it. A co-worker called police about 7:20 a.m. after finding the teller tied to a chair inside the U.S. Bank branch, a Kansas City FBI spokeswoman said. The co-worker was going through normal opening procedures when the teller was found, she said. The kidnapping victim told authorities a man kidnapped him about 1 or 1:30 a.m. and drove him around for a while before taking him to the bank at 10100 W. 119th St. The victim suffered minor injuries. The bank robber was described as a white male, about 5 feet 8 or 10 inches tall and weighing 180 pounds.

### Insider Threats

#### Bank insiders charged in Zeus cybercrime smackdown

*November 8 – (International)*

Six corrupt bank insiders turned Zeus money mule suspects have been arrested in Moldova. All half dozen of the suspects worked in local banks in the east European country. Investigators believe the suspects specialized in laundering Western Union and MoneyGram payments received from co-conspirators in Western nations that can ultimately be traced back to compromised corporate and personal bank accounts. The arrests in Moldova follow charges against alleged members of a massive cybercrime ring estimated to have raked in up to \$70 million by using the Zeus banking Trojan to steal online banking log-in credentials and loot accounts. Further arrests may follow in

**SECTOR  
ELEMENTS**

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

## ***Criminal Investigations***

### **Hedge-fund manager Mueller pleads guilty in \$70 million Ponzi scheme**

*November 2 – (Colorado)*

A Cherry Hills Village, Colorado hedge-fund manager faces up to 40 years in prison for running a \$70 million Ponzi scheme that lured wealthy Denver-area investors. The suspect pleaded guilty November 1 to the scam that ensnared about 65 people who invested funds since 2001 with Mueller Capital Management. The manager had less than \$9.5 million in cash and investments in April, and liabilities to investors of \$45 million. Some investors may have made withdrawals, officials said. He attracted investors with a strategy of day trading that he claimed earned regular returns of 12-15 percent per year. Police took him into custody April 22 after he sent apologetic messages to investors and threatened to jump off an RTD parking garage in Greenwood Village. The hedge-fund manager was hospitalized and later released. The state eventually shut down his funds and seized his assets.

**Denver Post:** [Hedge-fund manager Mueller pleads guilty in \\$70 million Ponzi scheme](#)

### **Principal of A&O Entities pleads guilty to his role in \$100 million fraud scheme involving life settlements**

*November 15 – (International)*

A 36-year-old male, of Houston, Texas, pleaded guilty November 15 in U.S. District Court in Richmond, Virginia, to conspiracy charges in connection with his role as a principal of the A&O entities, a group of businesses that acquired and marketed over \$100 million of investments in life settlements to more than 800 victims across the United States and Canada, announced the U.S. Attorney of the Eastern District of Virginia and the assistant attorney general of the criminal division. The suspect pleaded guilty to a two-count criminal information alleging conspiracy to commit mail fraud and conspiracy to commit money laundering involving losses to investors of more than \$50 million. At sentencing, he faces a maximum penalty of 5 years in prison and a \$250,000 fine on each count.

**Media Newswire:** [Principal of A&O Entities pleads guilty to his role in \\$100 million fraud scheme involving life settlements](#)

### **Classified documents stolen from Bank of Canada Governor Mark Carney's car**

*November 17 – (International)*

The Bank of Canada is dealing with a serious security breach after a thief smashed the window of the Central Bank Governor's unattended car in Montreal, Quebec, Canada, and made off with a travel bag containing classified documents. Confirming the theft November 16, a Bank of Canada spokesman said the stolen documents had differing levels of security classification, and included staff reports and briefing notes that would not affect markets. None of the documents were related to sensitive policy areas such as the direction of interest rates.

**Toronto Globe and Mail:** [Classified documents stolen from Bank of Canada Governor Mark Carney's car](#)

### **FBI raids three hedge funds in insider trading case**

*November 23 – (National)*

The FBI raided three hedge funds as part of a widening probe into suspected insider trading in the \$1.7 trillion hedge fund industry. The November 22 raids come as federal prosecutors prepare to unveil a series of new insider trading cases as soon as this year

**SECTOR ELEMENTS**

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

Moldova and elsewhere, a Washington Post staffer turned security blogger reports.

**The Register:** [Bank insiders charged in ZeuS cybercrime smackdown](#)

### Reward offered in bank fraud investigation

*November 12 – (Oregon)*

The FBI and Wells Fargo bank are offering a reward to help track down a former bank manager in Coos Bay, Oregon accused of taking up to \$1.2 million from customers. They are offering a \$10,000 reward for information leading to the arrest of a female suspect. FBI agents and police raided her home in October as part of an investigation into allegations she stole from accounts at a Wells Fargo branch. The FBI said the suspect worked for the bank from August 2006 to August 2010. She was fired when Wells Fargo discovered she had opened bank accounts for customers without their knowledge to get commissions for the new accounts. A federal judge issued an arrest warrant for the suspect October 27 based on charges of identity theft, aggravated identity theft, credit card fraud, wire fraud, bank fraud, and money laundering. Investigators have asked for the public's assistance in locating her.

**KPTV 12 Portland:** [Reward offered In bank fraud investigation](#)



FOX 12 ORGEGON  
The suspect in the Wells Fargo insider fraud case.

### Former Park Bank official indicted for embezzling \$227,764

*November 19 – (Wisconsin)*

The former assistant manager of Park Bank's Sun Prairie, Wisconsin branch was indicted November 18 on accusations the embezzled \$227,764 from the bank last year. The 26-year-old male, of Sun Prairie, who left the bank for unrelated reasons in June, appeared November 18 in U.S. District Court in Madison, where the U.S. Magistrate Judge ordered him jailed until an arraignment is held at a later date. According to a one-paragraph indictment unsealed November 18, the suspect took the money from the bank on or about August 27, 2009. If convicted, the suspect faces up to 30 years in prison. The case is being investigated by the FBI. An agency spokesman said he could not provide any further information. The Park Bank's vice president of marketing said the suspect worked for Park Bank for more than 4 and a half years.

**Madison Capital Times:** [Former Park Bank official indicted for embezzling \\$227,764](#)

### Most employees will steal company secrets if fired

*November 23 – (National)*

Insider threats are mainly comprised of normal, mainstream employees. Most strikingly, the Imperva survey found that 70% of respondents had clear plans to take something with them upon actually leaving their job. The most popular data is intellectual property (27%) and customer records (17%). Moreover, about half of respondents claimed to have personal ownership of the data - 59% in the case that they were about to change jobs, and 53% if they knew they were about to be dismissed. "This survey refutes the conventional wisdom that insiders are corporate spies or revenge-seeking employees," explained Imperva CTO Amichai Shulman. "It seems most employees have no deliberate intention to cause the company any damage. Rather, this survey indicates that most individuals leaving their jobs suddenly believe that they had rightful ownership to that data just by virtue of their corporate tenure."

**Help Net Security:** [Most employees will steal company secrets if fired](#)

**SECTOR ELEMENTS**

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

against hedge fund traders, consultants and Wall Street bankers. Two of the raided funds are Diamondback Capital Management LLC and Level Global Investors LP, each based in Connecticut and run by former managers of SAC Capital Advisors, one of the best-known U.S. hedge funds. A Boston, Massachusetts-based firm, Loch Capital Management, was also raided, a person familiar with the matter said. Loch has close ties with a witness who pleaded guilty in an insider trading probe centered on hedge fund Galleon Group.

**FBI:** [FBI raids three hedge funds in insider trading case](#)

**Other Criminal Investigations Articles:**

- *November 15 – (California) Central Valley Business Times:* [Arrest in \\$11 million Ponzi scheme](#). A 43-year-old of Sacramento has been arrested on a complaint charging him with wire fraud stemming from a Ponzi scheme that bilked investors out of \$11 million, according to an U.S. district attorney. The complaint alleged that between 2005 and 2009, the suspect, using the corporate name Genesis Innovations, recruited people to invest in real estate, promising investors a 14 percent annual rate of return.
- *November 18 – (Illinois) LoanSafe.org:* [Sunrise Equities: Owners accused of cheating investors in \\$43 million Ponzi and bank fraud scheme](#). Three owners of a bankrupt Chicago, Illinois real estate development firm that purported to adhere to Islamic law in handling investments from individuals in the Chicago area and nationwide actually operated a Ponzi-scheme that defrauded hundreds of victims and three banks of more than \$43 million, according to a federal indictment made public November 18. The defendants, who owned Sunrise Equities, Inc., allegedly fraudulently obtained more than \$40 million from more than 300 investors through the sale of promissory notes, and fraudulently obtained more than \$29 million in loans from three area banks.
- *November 19 – (New York) FBI:* [Societe Generale trader convicted of stealing high-frequency trading system code](#). The United States Attorney for the Southern District of New York, announced that a male suspect, a former trader at Societe Generale (SocGen) was found guilty November 20 of theft of trade secrets and interstate transportation of stolen property for stealing the proprietary computer code used in SocGen's high-frequency trading system. The suspect was found guilty by a federal jury after an 8-day trial before a United States district judge.
- *November 29 – (Virginia) LoanSafe.org:* [Virginia woman indicted in multi-million dollar mortgage elimination scam](#). On November 29, a federal grand jury indicted a 51-year-old Manassas, Virginia woman for her alleged involvement in a "mortgage elimination" scheme that caused more than \$10 million in losses. The U.S. Attorney for the Eastern District of Virginia, and the Assistant Director in Charge of the FBI's Washington D.C. Field Office, made the announcement November 29. The indictment alleged the woman defrauded more than 150 homeowners of \$10 million.

**Other Industry Reports****U.S. bars advance fees to loan modification companies**

*November 19 – (National)*

Foreclosure rescue companies and loan modification firms, many of which have been accused of taking money from desperate homeowners and doing little for them, will no longer be allowed to require payment in advance, the Federal Trade Commission (FTC)

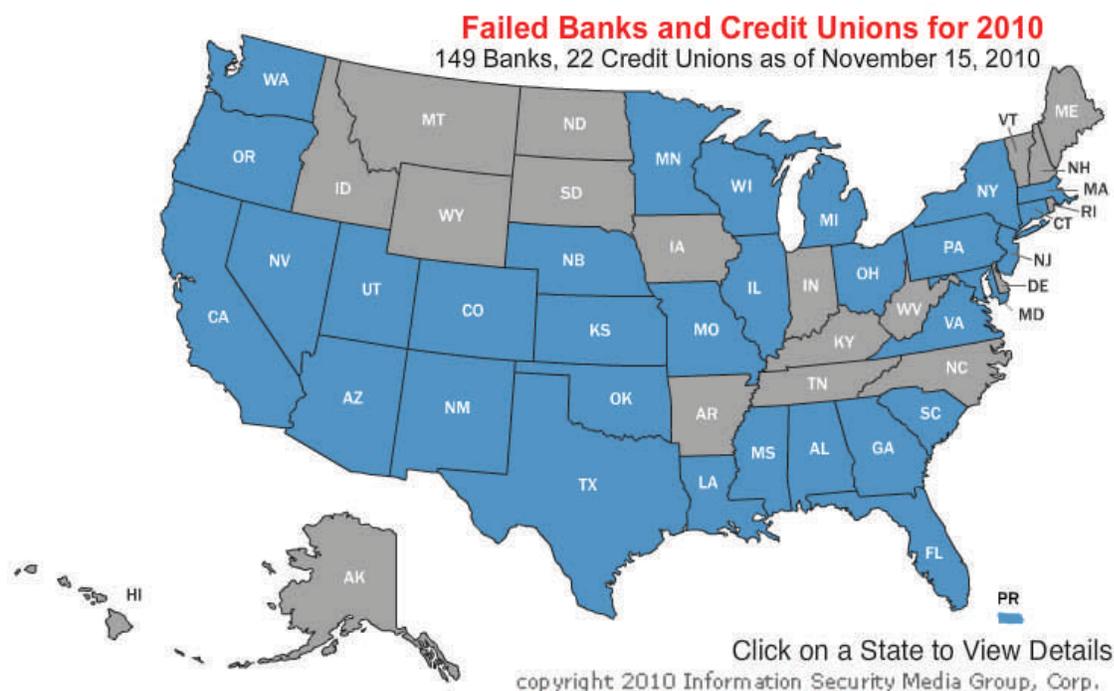
**SECTOR ELEMENTS**

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

said November 19. The firms will be barred from asking for payment until home owners receive a written offer from a lender or other mortgage servicer that they decide to accept, the agency said. The agency has brought more than 30 cases against the companies, which often promise to negotiate with lenders on the homeowners' behalf and then fail to deliver. A report by the Government Accountability Office completed in July 2010 found home owners were often scammed out of several thousand dollars.

Reuters: [U.S. bars advance fees to loan modification companies](#)

**For information on national bank closings up to November 15, 2010, see: [Failed Banks and Credit Unions for 2010](#)**



Your comments and suggestions are highly valued. Please send us feedback at:  
[cikr.productfeedback@hq.dhs.gov](mailto: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](mailto:CIKRISAccess@DHS.gov)

To receive the monthly *Sector Open Source Digest Highlights* newsletter, subscribe [here](#) at HSIN-CS.