Homeland Security

FINANCIAL SERVICES SECTOR OPEN SOURCE DIGEST

September 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

U.S. businesses could lose up to $1 billion in online banking fraud

September 1 – (National)

Criminals who bilk businesses' online banking accounts have gotten bolder and greedier in their heists over the past year, which could ultimately result in some $1 billion in losses for U.S. companies in 2010. So said the chairman of the Anti-Phishing Working Group and CEO of IronKey: "Trend-wise, we've been looking at reports of losses since the beginning of last year at $100,000 per incident, and as we got to the latter of last year, we saw losses in the $400,000 to $500,000 range, and now we're seeing losses in the [millions range]," he said. "The majority of successful heists in cybercrime seem to be against smaller companies that tend to bank with small- to mid-sized banks or credit unions. These banks don't have the security expertise that top banks [do] — they have the IT guy, whose also responsible for security," he said. "And many are outsourcing their banking systems to third parties, so they don't have a front-line security posture." A vice president and distinguished analyst at Gartner said $1 billion in losses from ebanking fraud for small- to-mid-sized businesses (SMBs) is possible for this year, but that figure may be more applicable to losses over the past year and a half.

DarkReading: U.S. businesses could lose up to $1 billion in online banking fraud this year

Crypto weakness leaves online banking apps open to attack

September 14 – (International)

Flaws in the way Web applications handle encrypted session cookies might leave online banking accounts open to attack. The security risk stems from a cryptographic weakness in Web applications developed using Microsoft's ASP.Net framework. ASP.Net uses the U.S. government-approved AES encryption algorithm to secure cookies generated by applications during online banking sessions. However, implementation flaws in how ASP.NET handles errors when the encrypted data in a cookie has been modified give clues to a potential attacker that would allow him to narrow down the possible range of keys used in an online banking session. Attacks based on this weakness might allow a hacker to decrypt sniffed cookies or forge authentications tickets, among other attacks. Two researchers have developed a Padding Oracle Exploit Tool to demonstrate the feasibility of the attack, an extension

SECTOR ELEMENTS

- Cyber Threat
- Physical Security
- Insider Threa
- Criminal Investigation
- Other Industr Reports

of previous research on similar flaws in JavaServer Faces and other Web frameworks.
The Register: **Crypto weakness leaves online banking apps open to attack**

Software vulnerabilities reaching 'unacceptable' levels

September 22 – (International)

Developers are failing to meet industry security standards when creating new software, according to testing firm Veracode. Data collected on 2,900 applications by the company's security verification service suggests that more than half of tested applications contain " unacceptable" levels of vulnerabilities. Financial sector applications had the lowest vulnerability levels, and mission-critical applications in general were found to be less vulnerable. Web-based applications were found to be particularly vulnerable, however. More than 80 percent of submitted Web applications contained errors listed in the Open Web Application Security Project's Top 10 risk list. The vice president of product marketing at Veracode told V3.co.uk that the high number of vulnerabilities in Web applications could be down to the skill of the developer and heightened interest in testing Web applications. She shot down the notion that data stored on site is more secure than cloud computing services, or that installed applications are inherently more secure. Instead, she suggested that companies are adopting stricter testing practices that should have been in use all along.
V3.co.uk: **Software vulnerabilities reaching 'unacceptable' levels**

Corporate ID thieves mining the store

September 23 – (Colorado; National)

Dozens of businesses in Colorado, and perhaps thousands more nationally, are victims of a new and easy form of identity theft where corporate data is hijacked and millions in phony credit purchases are made. All it takes is an Internet connection and, in some cases, as little as a $10 fee to alter the name of a corporate officer or the address of a company's registered agent on public records. Thieves then can acquire corporate credit in multiples much higher than the average consumer can get. And most companies might never know it is happening until it is too late. The nation's secretary of state offices — the agencies that usually register corporations and maintain public databases on them — have few protections to stop the Internet-based theft. In Colorado, for example, anyone can access the online databases and make changes since there is no password protection. Inaction has business owners fuming and, in turn, scratching their heads. Thieves are also relying on Dunn & Bradstreet — the business equivalent of a consumer credit reporting bureau — as unwitting accomplices. The company provides credit ratings on businesses and corroborates reported changes through secretary of state offices — where the fraud occurs in the first place. Police investigators have so far identified 48 Colorado businesses affected by the crime and expect to find dozens more.
Denver Post: **Corporate ID thieves mining the store**

Accounts raided in global bank hack

October 1 – (International)

More than 100 people have been arrested or charged in the U.S. and in the U.K. as part of an alleged global cybercrime ring using computer viruses to steal bank account information and loot money from unsuspecting victims. At least $3 million was stolen from U.S. accounts from about May of 2009 to the September of 2010, federal and state prosecutors said in New York September 30 as they unveiled indictments. The investigation is in its early stages and could result in law-enforcement actions in other countries, authorities said. In an action American officials say is related, 19 people were arrested September 28 in London as part of an investigation of a group alleged to have

SECTOR ELEMENTS

- Cyber Threats
- Physical Security
- Insider Threat
- Criminal Investigation
- Other Industry Reports

stolen at least $9.5 million from U.K. bank accounts. Police announced a 20th arrest September 30. Those arrested in the U.K. included men and women from Ukraine, Latvia, Estonia, Belarus and Georgia. Nine people have been arrested in the New York area, while one person has been taken into custody elsewhere in the United States, the FBI's New York office confirmed September 30. Many of those arrested in the New York area are money mules who are used to funnel money to the cybercrime group.
Wall Street Journal: **Accounts raided in global hack**
See also, Wall Street Journal: **U.K. arrests 19 for major bank hack**

Other Cyber Threats Articles:

- *September 6 – (International)* **Help Net Security:** **Every week 57,000 fake Web addresses try to infect users.** Every week, hackers are creating 57,000 new Web addresses, which they position and index on leading search engines in the hope that unwary users will click them by mistake.
- *September 9 – (National)* **Computerworld:** **Hotel operator warns of data breach.** HEI Hospitality, owner and operator of upscale hotels operating under the Marriott, Sheraton, Westin, and other monikers, has sent letters informing 3,400 customers that their credit card data may have been compromised. The warning stems from an intrusion into point of sale systems at several HEI properties earlier this year.
- *September 15 – (International)* **TrendLabs Malware Blog:** **One server, multiple botnets.** During a recent investigation into a server hosting SpyEye, TrendLabs noticed there were several open directories that led to other control panels. The investigation led to the discovery of what seems to be three botnets running on one server, which appears to be operated by at least two remote users.
- *September 16 – (International)* **SC Magazine UK:** **Emails containing Zeus malware detected, as removal tool announced.** Warnings have been made of a new wave of malicious e-mail messages that carry a Zeus payload. According to Websense Security Labs, the campaign is related to pharmaceutical spam messages, except it combines an HTML or ZIP attachment with a social engineering technique.
- *September 17 – (International)* **Krebs on Security:** **SpyEye botnet's bogus billing feature.** Miscreants who control large groupings of hacked PCs or "botnets" are looking for ways to better monetize their crime machines, and competition among rival bot developers is leading to devious innovations. The SpyEye botnet kit, for example, now not only allows botnet owners to automate the extraction of credit card and other financial data from infected systems, but it also can be configured to use those credentials to generate bogus sales at online stores set up by the botmaster.
- *September 21 – (International)* **Help Net Security:** **Phishers still favor spam over social networking sites.** SpamTitan Technologies announced the findings of its latest survey of small and medium businesses on the continued danger of phishing attacks, and it shows that despite media reports about the rise in phishing on social networking sites, its perceived threat to businesses is marginal when compared with traditional spam techniques.
- *September 27 – (International)* **The Register:** **ZeuS attacks mobiles in bank SMS bypass scam.** Security researchers have warned that cybercrooks might be able to compromise online bank accounts even in cases where banks use SMS messages to authorize transactions. The approach relies on first compromising a targeted user's computer using a variant of the ZeuS banking Trojan before infecting the same user's smartphone.
- *September 28 – (International)* **SC Magazine UK:** **Email spam campaigns continue to rise as LinkedIn users targeted.** A significant e-mail spam campaign

SECTOR ELEMENTS

- Cyber Threats
- Physical Security
- Insider Threats
- Criminal Investigation
- Other Industry Reports

was detected September 27 which targeted the LinkedIn social media community. Targets were e-mailed an alert link with a fictitious social media contact request and after clicking the link, victims were taken to a Web page that said "please waiting ..... 4 seconds," which redirected them to the Google homepage. According to Cisco, during those 4 seconds, the victim's PC was infected with the Zeus data theft malware by a drive-by download.

Physical Security

Fla. bank robbers strap bomb to abducted teller

September 24 – (Florida)

MIAMI HERALD

Safe escape: Police escort a bank teller from the bank. He is handcuffed and shirtless because the alleged bomb was cut from his clothes.

A bank teller was kidnapped September 24 from his home by robbers who strapped a suspected bomb to his chest and used him to steal money from a Bank of America branch near the University of Miami in Coral Gables, Florida, according to the FBI. The suspected explosive device was safely removed, and the teller was brought out of the bank shortly before noon. The device remained in the bank at midday, and authorities were working to detonate it, said a lieutenant in the Coral Gables Police Department. A major South Florida road, U.S. 1, was closed for hours in both directions at the height of rush hour. Three local schools were on lockdown as a precaution, and the University of Miami sent out a campus-wide alert. The incident began with a home invasion at an apartment complex in Kendall, where the bank teller lived. Three suspects later took the teller to the Coral Gables bank, used him to steal an undetermined amount of cash, and then made a getaway in a stolen red Ford Mustang.
Associated Press: Fla. bank robbers strap bomb to abducted teller

Other Physical Security Articles:

- *September 15 – (International)* **Agence France-Presse: N. Ireland dissidents threaten to attack bankers.** The Real IRA, a dissident republican terror group in Northern Ireland, threatened September 15 to target banks and bankers as it seeks to destabilize the peace process.
- *September 25 – (Arizona)* **KTVK 3 Phoenix: Device detonated at bank near Anthem following robbery.** Workers at a Bank of America near Anthem, Arizona, witnessed a robbery and a bomb scare just before closing September 24. Maricopa County deputies found a small device left on the front door of the bank when they arrived at the scene. The bomb squad detonated the device.
- *September 30 – (International)* **Associated Press: Failed bank heist in Baghdad leaves 3 dead.** A gang using bombs and automatic weapons tried to storm a bank in southwestern Baghdad, Iraq, in a failed robbery September 30 that officials said left three people dead, including two policemen. Police said the assault began with four bombs exploding near the state-run Al-Rafidain bank. Two robbers were captured.

SECTOR ELEMENTS

- Cyber Threats
- Physical Security
- Insider Threats
- Criminal Investigation
- Other Industry Reports

Insider Threats

Hancock Bank employee indicted on fraud charge

September 14 – (Mississippi)

A third Hancock Bank employee has been indicted on federal charges of bank fraud for scheming to defraud the bank of an undisclosed amount of money from the branch in Petal, Mississippi, according to federal court records. The suspect was indicted in January, though all of the details in the original indictment remain under seal. In the redacted indictment, she is accused of stealing from the bank between July 31, 2006, and June 24, 2009. She has pleaded guilty. The suspect was a financial services associate. She has been fired and is free on a $25,000 unsecured bond. Her sentencing, initially set for July 15, was postponed after the government filed a motion saying Hancock officials have since discovered what appears to be "additional fraud" involving the suspect. She is now the third former Hancock employee indicted on fraud charges. In an unrelated case, the former branch operations manager at Hancock's Ocean Springs main branch, and a former bank teller there, have pleaded guilty in a scheme to steal more than $2 million over more than 20 years, ending in July 2009. The thefts in that case started around 1982, when the pair started working side-by-side as tellers. The two, along with two other co-conspirators, reportedly stole money from the accounts of elderly people they had befriended. An independent audit showed $2,386,451.84 stolen from customer accounts between 1995 and July 2009. There were no records before 1995, so the amount embezzled from early 1980 to 1995 is unknown. All 44 of the victims were between the ages of 71 and 102.

Biloxi-Gulfport Sun Herald: **Hancock Bank employee indicted on fraud charge**

Snyder woman admits felony wire fraud

September 17 – (National)

A Snyder, New York, woman who worked at a Florida-based mortgage company pleaded guilty to a felony wire fraud charge in connection with a mortgage fraud scheme that cost nine banks a total of $24 million. She pleaded guilty before a U.S. District Judge the week of September 13, admitting to wire fraud affecting a financial institution. As an employee at Federal Guaranty Mortgage Co., she was responsible for preparing loan packages and forwarding the documents to financial institutions, according to an Assistant U.S. Attorney. The suspect admitted that she would sometimes sign several fraudulent mortgage applications for the same piece of property. Multiple mortgages would be obtained for the same property purchase, and the proceeds for the fraudulent mortgages would be wired to the account of a company associated with the company for which she worked.

Buffalo News: **Snyder woman admits felony wire fraud**

6 tips for guarding against rogue sys admins

September 27 – (National)

The vice president of the fraud program at the BITS Financial Services Roundtable said there has been an increase in insider incidents among U.S. financial services firms. "You have intentional breaches like theft of financial or propriety information and placement of logic bombs and malware, but you also have the unintentional breaches caused by insiders such as employees accidentally opening an infected file, installing unauthorized software or threats from social media," the vice president said. "We've seen an increase in the intentional and the unintentional" insider-related security breaches. Network World spoke with CISOs and IT security experts about what practical steps IT departments can take to minimize the insider threat. Their advice is:

SECTOR ELEMENTS

- Cyber Threats
- Physical Security
- Insider Threats
- Criminal Investigation
- Other Industry Reports

Restrict and monitor users with special privileges; Keep user access and privileges current, particularly during times of job changes or layoffs; Monitor employees found guilty of minor online misconduct; Use software to analyze log files and to alert when anomalies occur; Consider deploying data-loss prevention technology; and educate employees about the insider threat.
Network World: 6 tips for guarding against rogue sys admins

Mortgage broker and loan officer charged in fraud scheme

September 28 – (Pennsylvania)

An indictment was filed September 28 in Philadelphia, Pennsylvania, against a mortgage broker, loan officer, and an associate for engaging in schemes to defraud Wilmington Trust Federal Savings Bank and Malvern Federal Savings Bank involving properties valued at more than $35.5 million, a U.S. Attorney announced. The broker intentionally misrepresented material facts to Wilmington Trust about borrowers' income and assets, the potential rental income, and accurate appraisals of properties. The loan officer with Wilmington Trust allegedly worked in conjunction with her to approve mortgage loans for borrowers who did not meet Wilmington Trust's criteria for income, assets, and credit scores. The mortgage broker and an associate are charged with engaging in a scheme to defraud Malvern Federal. She allegedly altered borrowers' income tax returns prior to submitting them to Malvern Federal.
Federal Bureau of Investigation: Mortgage broker and loan officer charged in fraud scheme

Other Insider Threat Articles:

- *September 10 – (National)* **7th Space Interactive:** **Bank employee pleads guilty to role in bid-rigging and fraud conspiracies.** A former employee of a national bank pled guilty to participating in bid-rigging and fraud conspiracies related to contracts for the investment of municipal bond proceeds and other municipal finance contracts, the Department of Justice announced September 10.
- *September 18 – (California)* **San Francisco Appeal:** **Man sentenced in $1.3 million bank fraud scam.** One man was sentenced to prison September 15 for participating in a scheme with three others that defrauded banks of more than $1.3 million, according to the U.S. Justice Department.
- *September 20 – (New Jersey)* **Loansafe.org:** **Former Chase employee charged in $1.8 Million bank fraud scheme.** An indictment was unsealed September 20 against a suspect accused of charging a multi-year bank fraud scheme that netted him over $1.8 million between the summer of 2005 and the summer of 2009, a U.S. attorney announced.
- *September 24 – (Mississippi; Tennessee)* **Memphis Commercial Appeal:** **Southaven couple plead guilty to fraud charges.** A Southaven, Mississippi, couple has pleaded guilty to federal wire and mail fraud charges stemming from a scam involving insurance checks totaling nearly $700,000. They admitted to siphoning money from the woman's employer, Direct General Insurance Corp. of Memphis, Tennessee, by creating fraudulent checks on insurance claims.
- *September 27 – (South Carolina)* **Beaufort County Island Packet:** **Ex-loan officer to plead guilty in fraud scheme.** A former mortgage loan officer at Carolina First Bank on Hilton Head Island in South Carolina pleaded guilty September 27 to one count of conspiracy to commit bank fraud in connection with a scheme that cost banks as much as $7 million, according to a U.S. attorney. Prosecutors said the former mortgage loan officer used inflated appraisals to fraudulently arrange residential mortgages for "straw purchasers," and then used the difference between

SECTOR ELEMENTS

- Cyber Threats
- Physical Security
- Insider Threats
- Criminal Investigation
- Other Industry Reports

the inflated mortgage proceeds and the actual value of the property to pay the straw purchasers, himself, and others.

Criminal Investigation

Fraud probe at UK money printing factory

September 7 – (International)

One of the world's biggest money printing factories is being probed by fraud investigators over dud banknote paper. De La Rue — which employs 600 people at its Overton factory in Hampshire, United Kingdom — has sent a file on some workers to the Serious Fraud Office. The probe will center on allegations staff faked certificates that verified the quality of banknote paper. The company has reported its findings to the relevant law enforcement agencies. The company said "appropriate disciplinary action" was being taken. The company is the world's biggest supplier of banknotes, and paper to print it on, and has customers in 150 countries.

Sky News: Fraud probe at UK money printing factory

New vishing spree strikes U.S.

September 7 – (National)

In July, two phone-based phishing, or vishing attacks, hit residents in Provo, Utah. In August, 10 additional attacks were reported, incorporating a combination of vishing and text-message-based smishing scams, aimed at various communities scattered throughout the United States. The common factor: perpetrators targeting customers of community banking institutions. Recently, these campaigns have been seen popping up in small towns hitting markets where consumers might not be so savvy or prepared for a socially engineered attack. Vishing and smishing have replaced the traditional e-mail phishing attacks that were more prevalent 3 years ago. Since January, the number of traditional e-mail or phishing attacks has significantly dropped. "What's replacing them are these new waves of text and person-to-person scams and they're not being tracked," said the client relations specialist for FICO's Card Alert Service. August's vishing and smishing schemes hit residents in Elgin, Illinois; Long Island, New York; Binghamton, New York; New York's Chautauqua and Cattaraugus counties; Bend, Oregon; Arkansas City, Arkansas; Rocky Mount and Henry County, Virginia; Auburn, Alabama; Texarkana, Texas; and Central Falls, Rhode Island. Rather than being generic, in most cases, the calls and texts identified specific institutions by name.

Bank Info Security: New vishing spree strikes U.S.

7 charged in Richmond in insurance-fraud case

September 10 – (International)

More than 800 investors in the United States and Canada allegedly were swindled out of at least $100 million in a scheme involving life-insurance settlements. "This case involved elderly retirees and others who gave most — and in some cases, all — of their life savings and have seen it all disappear," a U.S. Attorney said at a news conference in Richmond, Virginia. This marks the first national financial fraud case coordinated by the Virginia Financial and Securities Fraud Task Force, a partnership formed in May between federal and state investigators and regulators. The U.S. attorney's office in Richmond charged and arrested three executives of A&O Resource Management in Houston, Texas. It also charged four others in connection with the fraud, including one who solicited investors in the Richmond area. All of the suspects are from the Houston area, and each was charged in federal court with one count of conspiracy to commit mail fraud, six counts of mail fraud, one count of conspiracy to commit money laundering,

SECTOR ELEMENTS

- Cyber Threats
- Physical Security
- Insider Threats
- Criminal Investigation
- Other Industry Reports

six counts of money laundering, and four counts of securities fraud.
Richmond Times-Dispatch: 7 charged in Richmond in insurance-fraud case

FBI arrests dozens in raid on massive N.J. bank-fraud ring

September 16 – (National)

THE STAR-LEDGER
FBI agents walk one of 50 suspects taken into custody in an early morning raid that swept across New Jersey.

Federal authorities in New Jersey charged 53 people September 16 with participating in a massive bank-fraud ring that authorities said hijacked identities of overseas workers to bilk millions from financial institutions. More than 270 local and federal agents — including from the FBI, IRS, and Immigration and Customs Enforcement — fanned out across Bergen and Essex counties in New Jersey, and Manhattan in New York City to arrest 43 suspects. Stretching from New Jersey to California to the South Pacific, the alleged scheme used Social Security numbers from Asian immigrants who worked in American territories, including Guam, to apply for driver's licenses under fake names, which they then utilized to secure credit cards and bank loans. The suspects used those credit cards to buy luxury cars, designer shoes, aged whiskey and other finery, authorities said. Or, members of the ring swiped the cards at their own businesses or shell companies to trick banks into transmitting them money directly, authorities said. When time came to pay the credit-card bills, the banks were left with the name of someone on the other side of the globe, authorities said.
Newark Star-Ledger: FBI arrests dozens in raid on massive N.J. bank-fraud ring

Other Criminal Investigation Articles:

- *September 2 – (California)* **San Jose Mercury News:** **Thief suspected in string of bank robberies strikes Bank of the West in San Jose.** A San Jose, California, bank robbery September 1 is believed to be the latest heist by a buttoned-down thief identified in nine similar crimes in the last 3 months.
- *September 4 – (Ohio)* **Columbus Dispatch:** **Couple accused of $25M stock swindle.** A Gahanna, Ohio, man with a criminal past and his wife were in court September 3, accused of stealing at least $25 million from 50 people in a stock-investment scheme.
- *September 7 – (California)* **Los Angeles Times:** **FBI increases reward for information about 'Geezer Bandit'.** Absence has increased the FBI's desire to arrest the bank robber known as the "Geezer Bandit," who is accused of 11 holdups in San Diego and Riverside counties. The Geezer Bandit has not hit a bank since June 24 — the longest hiatus since he began his spree 1 year ago.
- *September 8 – (Maine)* **Seacoastonline.com:** **State police seize more than $1 million from truck on Interstate 95 in York.** State police are not ready to say why a truck stopped for a routine inspection September 3 in York, Maine, was transporting more than $1 million in $20 bills neatly bundled and placed in orange plastic buckets. On September 7, an FBI official in the Portsmouth, New Hampshire, office classified the case as an immigration and customs enforcement issue.

SECTOR ELEMENTS

- Cyber Threats
- Physical Security
- Insider Threats
- Criminal Investigation
- Other Industry Reports

SURVIELLENCE STILL
Police are looking for the wig-wearing bank robbers.

- *September 8 – (Georgia)* **Atlanta Journal-Constitution: Bank robbery duo strikes again.** Bank robbers known to wear straggly, black wigs struck again September 8 in Gwinnett County, Georgia. The two armed men wearing masks entered a Wachovia branch in the 3000 block of Centerville Highway. Those in the bank were forced to the floor and a single gunshot was fired into the ceiling.
- *September 10 – (North Carolina)* **WBTV 3 Charlotte: ATM "skimmers" scam ring hitting Charlotte area hard.** Authorities say a sophisticated ring of scam artists based in Florida is targeting the Charlotte, North Carolina, area, stealing local victims' ATM numbers along with thousands of dollars from their accounts.
- *September 17 – (Texas)* **KWTX 10 Waco: FBI seeks public's help in finding I-35 bandit.** The FBI asked for the public's help September 17 in locating the man dubbed the I-35 Bandit who has robbed 15 Texas banks between Wichita Falls and San Antonio since January 2004.
- *September 17 – (National)* **U.S. Security and Exchange Commission: Lambros D. Ballas sanctioned.** A suspect, of Huntington, New York, was barred from association with any broker or dealer by the U.S. Securities and Exchange Commission. He arranged for the distribution of phony press releases involving major public companies, such as Google, Microsoft, and Walt Disney, and then posed as an investor on Yahoo! Inc. Internet message boards providing links to the bogus releases he had created and disseminated.
- *September 22 – (National)* **United Press International: FBI: 'Massive frauds' uncovered.** An FBI official told the U.S. Senate Judiciary Committee September 22 the bureau has uncovered "massive frauds" in its ongoing effort to fight financial crime. The assistant director who heads the criminal investigative division said the agency has continued to find fraud, including newly identified Ponzi schemes.

Other Industry Reports

Under piles of paperwork, a foreclosure system in chaos

September 23 – (National)

The nation's overburdened foreclosure system is riddled with faked documents, forged signatures and lenders who take shortcuts, according to court documents and interviews with attorneys, housing advocates and company officials. The problems, which are so widespread some judges approving foreclosures ignore them, came to light after Ally Financial, the fourth-biggest U.S. mortgage lender, halted home evictions in 23 states. During the housing boom, millions of homeowners got mortgages with little proof of income or background. Now, as millions are being pushed out of homes they can't afford, the foreclosure process is producing more paperwork than anyone can read, making it vulnerable to fraud. Ally is double-checking to ensure all documents are in order after lawsuits showed a single employee of its GMAC mortgage unit signed off on 10,000 foreclosure papers per month without checking if the data justified an eviction. Many homeowners in fact, might have been in default and some may have been unfairly targeted. But the flawed process is creating an opening for borrowers to contest some of the more than 2 million foreclosures that have taken place since the real crisis began.

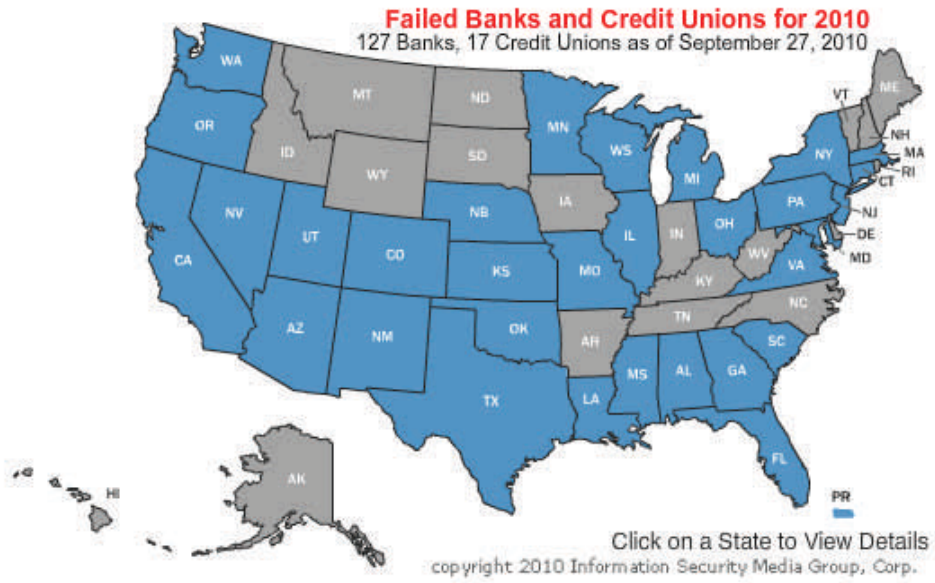
Washington Post: Under piles of paperwork, a foreclosure system in chaos

SECTOR ELEMENTS

Other Industry Reports Articles:

- *September 22 – (International)* **Help Net Security: Breakdown of security weaknesses by industry and organization size.** WhiteHat Security released the tenth installment of its Security Website Security Statistics Report, providing a first-time breakdown of the state of Web site security by industry and company size. Compiled using data from 2,000 sites across 350 organizations, this issue shines a light on the need for organizations to focus on improve remediation of vulnerabilities to reduce risk and improve the effectiveness of the SDLC over time.
- *September 25 – (National)* **Wall Street Journal: Credit unions bailed out.** Regulators September 24 issued a rescue and revamp of the U.S. wholesale credit union system, underpinned by a federal guarantee valued at $30 billion or more.
- *September 26 – (International)* **China Post: Norwegian central bank sues Citigroup for fraud .** Norway's central bank has sued New York-based Citigroup for allegedly providing false financial statements that led to losses of $835 million, a Citi official said September 24. Norges Bank complained Citigroup repeatedly issued "untrue statements and non-disclosure of material information to investors," which led it to purchase Citi securities at inflated prices between 2007 and 2009.

Featured Incidents: Bank and Credit Union Closings, September 2010



For more information on bank and credit union failures, see:
Fla. bank closed
6 Banks closed on Sept. 17
Two banks closed on Sept. 24

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: CIKRISEaccess@DHS.gov.