



# FINANCIAL SERVICES SECTOR OPEN SOURCE DIGEST

June 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**

### **Facebook used to find money mules**

*June 1 – (International)*

Phishers are looking into different ways of reaching new recruits of cyber criminals by casting their nets onto social networking sites, creating special Facebook groups for their work-at-home scams, according to Kaspersky Lab. Far from a novel idea, phishers have been using social networks for years to find new recruits. Now, the scammers have created Facebook groups specifically dedicated to the work-at-home scams that often serve as recruitment schemes for money mules. One such group has almost 225,000 members on Facebook, according to Kaspersky researchers. The criminals promise high earnings for minimal efforts: \$6,000 per month for only 18 hours of work per week. Job responsibilities often involve accepting deposits and wire transfers of thousands of dollars a day, then transferring the money to other accounts designated by the phishing gang. Although money mules can make fast cash relatively easy, it is usually they who are most likely to be discovered, arrested and prosecuted.

**The New New Internet:** [Facebook used to find money mules](#)

### **Latvians to be deported for role in Davidson Companies extortion plot**

*June 11 – (Montana)*

Three men who aided an extortion plot on Davidson Companies will be deported after receiving their sentence June 10 in Helena, Montana. The three suspects, all of Latvia, previously pleaded guilty to a federal charge of receipt of extortion proceeds. A senior U.S. district judge sentenced the men to time served, as they have been in the custody of Dutch and U.S. officials since February 2008. Davidson's computer system was hacked into some time between December 20, 2007, and January 11, 2008, by a man identified in court documents as "John Doe, aka [real name]." The hacker has not been arrested and remains at large. Thousands of customers' personal and/or financial account information was accessed as part of the computer attack. The hacker demanded \$80,000 from Davidson in exchange for revealing security vulnerabilities and destroying any confidential information he had obtained, court documents state.

**SECTOR  
ELEMENTS**

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

**Great Falls Tribune:** [Latvians to be deported for role in Davidson Companies extortion plot](#)

## **Belgian pump and dump botnet**

*June 18 – (International)*

According to a report in Belgian newspaper De Tijd, malware has been used to compromise the online portfolios of Belgian investors. The botnet was then used to influence stock prices, making the criminals more than 100,000 Euros. The investigation remained secret until June 18. The federal prosecutor and the computer crimes unit of the national police in Belgium were looking into events that took place in 2007. Between April and May 2007, criminals infected the PCs of customers of the banks Dexia, KBC and Argenta with a bot (the exact nature of the bot is unspecified) which stole the usernames and passwords for online share-trading platforms. The article goes on to detail what appears to be a highly targeted, custom-written attack that was able to automate stock trades across the botnet. With a push of a button, the botmaster instructs all the computers to buy or sell the same shares at the same time. The criminals behind the enterprise went on to profit from the sharp changes in stock price of the penny stocks that were being manipulated by buying and selling their own shares at exactly the right moments in classic pump-and-dump tactics.

**Trend Micro:** [Belgian pump and dump botnet](#)

## **FBI releases information on the latest telephone scam**

*June 24 – (International)*

Telephone scams have been around for decades but scammers are still finding new twists to trick consumers. On June 21, the FBI released information on the latest phone scheme targeting consumers. The “telephone denial-of-service” scam ends with the consumer receiving an exorbitant amount of phone calls ranging from recorded messages to dead air. What consumers do not know is that while they are receiving the phone calls, scammers are hard at work. Scammers find out the victim’s personal information months before they set up these phone calls. They find out account numbers and passwords, and then use the phone calls to divert the victim’s attention and prevent any other phone calls from coming in. While the phone lines are busy, the scammer either drains the victim’s bank account through fraudulent transactions or they pretend to actually be the victim using the account information they previously collected.

**Better Business Bureau:** [FBI releases information on the latest telephone scam](#)

## **FTC says scammers stole millions, using virtual companies**

*June 27 – (International)*

The Federal Trade Commission (FTC) has disrupted a long-running online scam that allowed offshore fraudsters to steal millions of dollars from U.S. consumers - often by taking just pennies at a time. The scam, which had been run for about four years, according to the FTC, provides a case lesson in how many of the online services used to lubricate business in the 21st century can equally be misused for fraud. The FTC has not identified those responsible for the fraud, but in March, it quietly filed a civil lawsuit in U.S. District Court in Illinois. This has frozen the gang's U.S. assets and also allowed the FTC to shut down merchant accounts and 14 "money mules" - U.S. residents recruited by the criminals to move money offshore to countries such as Bulgaria, Cyprus, and Estonia. The scammers found loopholes in the credit-card processing system that allowed them to set up fake U.S. companies that then ran more than one million phony, credit-card transactions through legitimate credit-card processing companies. The scammers stayed under the radar from investigators for so long by charging very small amounts -- typically between 25 cents and \$9 per card - and by

**SECTOR  
ELEMENTS**

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

setting up more than 100 bogus companies to process the transactions.

**IDG News Service:** [FTC says scammers stole millions, using virtual companies](#)

**Other Cyber Threats Articles:**

- *June 1 – (Maine) Bank Info Security:* [ACH fraud sparks another suit](#). In another round of bank vs. customer, a Maine business has [sued its bank](#), alleging that the institution, Ocean Bank of Portsmouth, failed to prevent fraudulent ACH transactions totaling more than \$500,000.
- *June 3 – (National) Wall Street Journal:* [Dark side arises for phone apps](#). As smartphones and the applications that run on them take off, businesses and consumers are beginning to confront a budding potential security concerns. Concerns are growing among security researchers and government officials that efforts to keep out malicious software aren't keeping up with the apps craze.
- *June 4 – (International) Techworld:* [HSBC browser plugin attacked by Trojan](#). A popular anti-keylogging tool used by online banks such as HSBC, Trusteer's Rapport, has come under direct attack by malware writers trying to bypass its protection settings.
- *June 11 – (National) Reuters:* [SEC eyes confluence of events as flash crash cause](#). U.S. regulators will most likely find that a confluence of events caused the unprecedented stock market "flash crash" in early May, the Securities and Exchange Commission (SEC) chairman said June 10.
- *June 14 – (National) Better Business Bureau:* [New tab napping scam targets your bank information](#). Tab napping is more sophisticated than phishing scams and doesn't rely on persuading a user to click on a link to a scammer's Web page. Instead, it targets Internet users who open lots of tabs on their browser at the same time. It works by replacing an inactive browser tab with a fake page set up specifically to obtain personal data without the user even realizing it has happened.
- *June 15 – (International) Reuters:* [Police arrest 178 in global credit card scam](#). Police arrested 178 people in Europe and the United States suspected of cloning credit cards in an international scam worth over 20 million Euros, Spanish police said June 15.
- *June 16 – (National) Victoria Advocate:* [Security breach pushes First Victoria to block signature-based transactions on debit cards](#). First Victoria bank in Texas placed blocks on its MasterCard debit cards after a small amount of card numbers were compromised by a third-party source.
- *June 24 – (International) The Register:* [Scotland Yard cuffs teens for role in cybercrime forum](#). Two teenagers have been arrested for their alleged involvement in the world's largest English-language cybercrime forum. An 8-month investigation into the forum, which has not been named, found it had almost 8,000 members who traded malware, cybercrime tutorials, and stolen banking information.

**Physical Security****Al Qaeda front says it bombed Iraq bank; 18 die**

*June 24 – (International)*

An al Qaeda front group claimed responsibility on June 23 for bombing a state-run investment bank, gloating over its ease in penetrating security in an attack that killed at least 18 people. The June 20 attack on the Trade Bank of Iraq was meant to



REUTERS  
Smoke rises from the site of a bomb attack in Baghdad .

**SECTOR ELEMENTS**

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

expose the weakness of the country's stalled government, according to a statement posted on the Web site of the Islamic State of Iraq. The statement called the bank a "stronghold of evil" because it was established to attract foreign investment. The group, which is allied with al Qaeda, taunted the government for its inability to keep the peace. The same group claimed responsibility for the recent strike on the Central Bank of Iraq, the nation's treasury, in which at least 26 died in a commando-style assault by bombers and shooters. In that assault, armed men wearing police-commando uniforms briefly overran Iraq's Central Bank June 13 in a brazen daylight assault. After storming two separate entrances, the gunmen apparently roamed through the building. Security forces fearing a hostage scenario ringed the bank, and when they finally entered shortly after 7 p.m., they found only dead and injured bank employees and the seven bodies of suspected assailants who had used suicide vests.

**Associated Press:** [Al Qaeda front says it bombed Iraq bank; 18 die](#)

**For more information, see Los Angeles Times:** [At least 24 killed as gunmen storm Iraq's Central Bank](#)

## Woman arrested on explosives charge ahead of G-20

*June 24 – (International)*

The wife of a man charged with possession of explosives in what police are calling a Group of 20 summit-related arrest has also been charged in the investigation. A police spokeswoman said June 24 that the 37-year-old suspect has been charged with possession of an explosive device and possession of a weapon. The suspect's partner, a computer-security expert, was charged June 23 with several offenses, including possession of explosives and dangerous weapons, and intimidating a justice system participant. An Internet activist and contributor to the Canadian Broadcasting Corp. said the computer expert told a May meeting of activists and professors that he planned to monitor police chatter about the G-20 summit and post it on Twitter. He also said he would buy items online to attract police attention. Officers armed with a search warrant went to the couple's million-dollar-plus home in a wealthy neighborhood in Toronto's north end June 22. They charged the computer expert and have now charged his wife after searching two cottage homes in rural Ontario. The police spokeswoman said she could not say what the explosives are but said there is no risk to public safety. Police said the investigation is part of the ongoing effort to ensure a safe and secure G-20 Summit.

**Associated Press:** [Woman arrested on explosives charge ahead of G-20](#)

### Other Physical Security Articles:

- *June 14 – (North Carolina) WRAL 5 Raleigh:* [Raleigh police: Bank robber getting 'more dangerous'](#). A bank robber suspected in a series of crimes in Raleigh, North Carolina is "getting progressively more dangerous with each crime," authorities said June 14, and they are concerned he could become even more violent.
- *June 14 – (Florida) Bradenton Herald:* [Manatee sheriff: Woman's bomb/bank robbery claims ring true](#). There is evidence that a woman who claims she was told by kidnapers that a bomb had been strapped to her back and that it would be detonated if she did not rob a bank may be true, Manatee County Sheriff's Office officials said June 14.

## Insider Threats

### Ex-call center operator pleads guilty to bank fraud

*June 2 – (Florida)*

**SECTOR ELEMENTS**

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

A former bank call center operator pleaded guilty June 2 to stealing customer information and trying to sell it. The 28-year-old defendant of Riverview, Florida faces up to 30 years in federal prison after pleading guilty to one count of bank fraud. A sentencing date has not been set. The defendant was a Bank of America customer-service operator, handling calls from customers who had questions about their accounts. In March, he and an unnamed man met with an undercover FBI agent at a restaurant in east Hillsborough County. The defendant offered to sell customers' personal information in return for part of the proceeds of raiding the accounts. The information included name, birthday, address, tax identification number and telephonic password. According to his plea agreement, the defendant wanted to target only customers with more than \$100,000 in their accounts and wanted half of any stolen funds. He later reduced his demand to a quarter of the swag; he received \$2,500 in the sting operation. **Tampa Tribune:** [Ex-call center operator pleads guilty to bank fraud](#)

**How to avoid hiring fraudsters**

*June 11 – (New York)*

Recently, a CFO ran away with \$600 million stolen from his employer who sold computers in New York City. When the president of Corporate Resolutions Inc, a business-consulting firm, investigated this case, he found glaring disconnects: The CFO had lied about his experience and credential in his resume, and he had listed three business references — one was dead; one did not exist; the last reference said they would never hire him. The leader for Ernst & Young's information security practice for the Americas finds three common fraudulent behaviors specific to security professionals: Misusing access to retrieve critical information and/or view restricted information like pornographic material; Engaging with coworkers on a side online business and deleting logs and activities, and deliberately failing to monitor required systems; and overstating security credentials. According to a new report by the [Association of Certified Fraud Examiners \(ACFE\)](#), about 5 percent of organizational revenue is lost annually to organizational fraud, mostly employee theft. That translates into a potential total loss of about \$3 trillion per year. Among the warning signs to look for when hiring security professionals: Candidates who do not stay in a job over a year; Someone who is not interested in benefits; One who does not provide accurate information on their current state of certifications; Lack of business references; Person is uncomfortable performing "hands-on" tests and exercises to demonstrate skill; Someone listed and associated with underground hacker groups; and anyone experiencing financial problems.

**Bank Info Security:** [How to avoid hiring fraudsters](#)

**Other Insider Threat Articles:**

- *June 2 – (Iowa) KPTH 44 Sioux City:* [Bank worker sentenced for Sac City fraud](#). A former Sac City, Iowa bank employee was sentenced for a 13-year, bank-fraud scheme. The 49-year-old suspect will spend more than seven years behind bars for selling \$4 million worth of fake certificates of deposit to 40 victims.
- *June 3 – (National) Reuters:* [Ex-Goldman analyst who fled must pay \\$27.8 million](#). A former Goldman Sachs Group Inc. analyst who pleaded guilty to running an insider trading scheme and later fled while on probation has been ordered to pay nearly \$27.8 million.
- *June 8 – (California) Contra Costa Times:* [Antioch bank teller sentenced to five years for armed robbery scheme](#). A bank teller was sentenced in federal court June 3 for his role in an armed takeover of an Antioch, California credit union.

**SECTOR ELEMENTS**

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

Authorities said the suspect pretended to be a hostage while helping to orchestrate the February 25, 2009, robbery at the Metro 1 on Lone Tree Way, modeling the plan after a takeover robbery he witnessed the previous year.

- *June 15 – (New Jersey) **Bank Info Security: [Ex-Teller guilty of insider scheme](#)**.* A former JPMorgan Chase employee pleaded guilty to participating in a scheme to steal more than \$60,000 from New Jersey bank customers' accounts. The suspect was a teller at the JPMorgan Chase bank in Hackettstown, New Jersey. According to a [press release](#) from the U.S. Department of Justice, the suspect accessed 12 customer account profiles and sold them to two people in Pennsylvania.
- *June 28 – (Massachusetts) **Associated Press: [Peabody bank teller sentenced in fraud case](#)**.* A former bank teller from Peabody, Massachusetts has been sentenced to nearly three and a half years in prison for stealing customer account information that led to the theft of more than \$330,000. The suspect used his access to bank customer data to steal customer names and account information from November 2004 to February 2006. He then sold the information usually for \$2,000 per account.

## **Criminal Investigation**

### **Credit union demands \$42 million, claims Fannie Mae bought 'stolen' mortgages**

*June 2 – (National)*

Fannie Mae refuses to return \$42 million worth of "stolen" mortgages to Suffolk Federal Credit Union, the credit union [claims](#) in Federal Court. Suffolk claims U.S. Mortgage Corp. and its CEO, along with another U.S. Mortgage employee, serviced its mortgage loans, but "signed loan transfer documents that falsely identified themselves as executives of Suffolk." Suffolk claims the CEO then sold the loans to Fannie Mae, which never checked his authority to execute such documents on behalf of the credit union. "Fannie Mae ignored obvious signs of falsified financial statements, payment irregularities, commingling of funds, and dangerously speculative securities trading, all of which pointed to a situation ripe for fraud," Suffolk claims. Even after the CEO pleaded guilty to stealing the mortgages, Suffolk says, Fannie Mae refused to return them, claiming it bought the loans fair and square in good faith. But the credit union insists that the law states, "purchasers of negotiable instruments who stick their heads in the sand cannot claim ownership of stolen property."

**Courthouse News Service: [Credit union demands \\$42 million, claims Fannie Mae bought 'stolen' mortgages](#)**

### **Police warn of new credit card scam in area**

*June 13 – (Michigan)*

The Michigan State Police Department is warning retailers of a new credit card scheme happening in Battle Creek. The culprits scramble a store's satellite system, used to send credit card information with aluminum foil, police said, knocking out the card-4verification systems and allowing the thieves to use stolen credit cards unnoticed. Police warn stores against accepting business from customers using a variety of credit cards for purchases, and said businesses with satellite dishes attached to low roofs are especially vulnerable. Businesses are asked to call 911 if they suspect they have been scammed.

**Battle Creek Enquirer: [Police warn of new credit card scam in area](#)**



WWMT 3 BATTLE CREEK  
Video: An explanation of the incident and the aluminum foil tactic

## SECTOR ELEMENTS

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

## U.S. government accuses former mortgage executive of multibillion-dollar scam

*June 17 – (National)*

The U.S. government [accused](#) the former chairman of one of the nation's largest mortgage firms of a multibillion-dollar scam June 16, unveiling what is to date the biggest criminal case related to the crisis that nearly brought down the financial system. The Justice Department accused the former chairman of Taylor, Bean & Whitaker of committing a \$1.9-billion fraud against investors and the federal government that led to the demise of his firm, and one of the nation's largest regional banks, Colonial Bank in Alabama. But beyond the indictment, federal officials described an even wider scheme, and they said the collateral damage to federal agencies has only begun to be tallied. The suspect allegedly hid how sick it had become, enabling the firm to fraudulently meet government conditions and become one of the largest business partners of the Federal Housing Administration and Ginnie Mae, federal agencies that cover losses suffered by mortgage lenders and their financiers. Federal officials said the scheme caused the two agencies' largest losses ever, totaling at least \$3 billion. The officials warned that the final figure could be higher. The suspect's activities could also prove costly to Freddie Mac, which helps finance mortgage lending.

**The Washington Post:** [U.S. government accuses former mortgage executive of multibillion-dollar scam](#)

## Authorities reveal mortgage fraud crackdown, 485 arrests

*June 17 – (National)*

U.S. authorities have charged 1,215 people in [hundreds of mortgage](#) fraud cases that resulted in estimated losses of \$2.3 billion, top presidential administration officials said June 17, unveiling a crackdown after the housing market collapse. The administration has been under pressure to root out mortgage fraud and improve oversight of the housing market after the housing bubble touched off a global economic slide, and led to a cascade of home foreclosures in the United States. Over the last three-and-a-half months, authorities have made 485 arrests in the fraud cases, obtained 336 individual convictions and recovered more than \$147 million, the Justice Department said. The announcement comes a day after U.S. prosecutors unveiled charges against the former head of a now-defunct mortgage lender for an alleged fraud scheme that led to multibillion-dollar losses.

**Reuters:** [Authorities reveal mortgage fraud crackdown, 485 arrests](#)

### Other Criminal Investigation Articles:

- *June 1 – (National)* **Associated Press:** [FBI says 'Granddad Bandit' may be responsible for 21 bank holdups across the eastern U.S.](#) A man dubbed the "Granddad Bandit" is proving elusive. The FBI in St. Louis said an older man suspected of robbing a Regions Bank branch in St. Louis County May 18 is also suspected of 20 other bank robberies across the eastern and central United States.
- *June 10 – (Oregon)* **KPTV 12 Portland:** ['Beastie Boys Bandit' sought in bank robberies.](#) Oregon police said they are looking for a man they are calling the "Beastie Boys Bandit" after two recent bank robberies in east Portland. In June, a man wearing a



KPTV 12 PORTLAND  
Beastie Boys Bandit' Sought In Bank Robberies

**SECTOR ELEMENTS**

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

wig, fake mustache, sunglasses and a dark suit with a white, button-up shirt robbed two U.S. Bank branches.

- *June 10 – (New York) Wall Street Journal: [FBI raids alleged boiler room](#).* A suspected member of the Bonnano organized-crime family, and half a dozen others, were arrested in a raid June 9, quickly followed by a search and seizure of an alleged “boiler room” operation in Manhattan’s Garment District.
- *June 15 – (Virginia) Associated Press: [2 Va. men plead guilty in mortgage fraud scheme](#).* Two Lynchburg, Virginia men have pleaded guilty to participating in a mortgage-fraud scheme that cost lenders at least \$7 million.
- *June 17 – (Virginia) Virginian-Pilot: [Va. Beach man charged with smuggling holograms](#).* A Virginia Beach man faces an 18-count federal indictment charging him with trying to smuggle hundreds of credit-card holograms into the country from the Middle East.
- *June 21 – (Texas) Shreveport Times: [Four arrested in credit card scam](#).* Four people are in jail for manufacturing credit cards using stolen information, said the Caddo, Louisiana sheriff. Credit card numbers were stolen from customers who used their cards at a local fast-food restaurant in June. An employee of the restaurant sold those numbers to three Texas men who turned them into new credit cards, the sheriff said.
- *June 25 – (California) CNN: [‘Geezer bandit’ wanted in string of bank robberies](#).* A Southern California bank robber dubbed the “Geezer bandit” has struck again, possibly knocking off his 11th bank in San Diego and Riverside County, the FBI said.

---

### Featured Incidents: Skimming, June 2010

---

#### Skimming from the sofa

*June—7 (National)*

Skimming devices attached to cash machines to read users’ card details increasingly return their data to the criminals via SMS text messages. The devices copy the magnetic strip of cash point and credit cards at the card slot and spy on PINs via keyboard attachments or mini cameras. The data is subsequently used by the skimmers to withdraw money from users’ accounts. The new generation of skimming devices no longer store the data over a period of time for later collection, but transmit it via SMS directly to the criminals, allowing them to clone card details from the comfort of their own living room. The risk of getting caught is reduced by 50 percent because criminals no longer need to retrieve the skimming device to read out the data.

**The H Security:** [Skimming from the sofa](#)

#### Other skimming incidents in the U.S.:

- *June 2 –(Louisiana) [Shreveport Times](#):* A Bossier City, Louisiana man faces theft charges after allegedly using a skimming device to steal people’s credit card information. The suspect is accused of using a skimming device over the past several weeks to steal credit card information from customers in the drive through lane at the McDonald’s Express restaurant where he was employed.
- *June 6—(International) [Vancouver Sun](#):* A 15-year-old boy was arrested in May at a Canadian gas station for connection to a credit-card skimming operation. The boy is suspected of copying credit card information from several hundred customers without their knowledge, and then selling the stolen information to organized crime

**SECTOR ELEMENTS**

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

- groups who could use the credit cards to make purchases.
- *June 8 -(Maryland) [WTTG 5 Washington D.C.](#)*: Over the last several weeks, thieves have been targeting ATMs in Waldorf, Maryland where they have made off with thousands of dollars in cash. Twice in May and once in April, the thieves attached devices onto ATMs at two Bank of America branches in Waldorf as well as a BB&T bank on Leonardtown Road.
- *June 9—(New York) [Wall Street Journal](#)*: "Cloned" debit cards have been used to steal more than \$200,000 from Long Island banks between April and the end of May, police said.
- *June 10 -(California) [KXTV 10 Sacramento](#)*: After an investigation led to the discovery of three identical credit-card skimming machines inside gasoline pumps in California in Placer County, Sacramento and Folsom, authorities are now looking for the people who may have used the machines to collect personal identification information.
- *June 21—(Illinois) [WBBM 780 Chicago](#)*: A Serbian national living in north suburban Niles, Illinois was arrested June 18 for allegedly trying to buy a device commonly used for ATM skimming.

**Other Industry Reports****Microsoft opens center for reports of stolen identity and data theft***June 18 - (National)*

In a major step to slow cybercrime, Microsoft June 17 launched a coalition that will serve as a clearinghouse for reports about caches of stolen data stashed all across the Internet. Malicious programs crafted to swipe financial and personal data have come to saturate the Internet — so much so that security researchers routinely ferret out computer servers used by cyber-crooks to hoard stolen data. Until now, there was no specific process for reporting such discoveries. The Internet Fraud Alert center — spearheaded by Microsoft, and managed by the [National Cyber-Forensics & Training Alliance](#) (NCFTA) — will serve as a reporting hub. Stolen payment-card numbers and online banking-account logons will be routed to the issuing banks. The institutions will then decide whether to alert customers, suspend the accounts or pursue legal remedies. Stolen Social Security numbers, birth dates and other personal data will be archived offline by the NCFTA and made available, as needed, to law enforcement.

USA Today: [Microsoft opens center for reports of stolen identity and data theft](#)

**Negotiators in Congress OK sweeping reform of big banks***June 25 - (National)*

House and Senate lawmakers early June 25 approved the most significant increase in the regulation of U.S. banks since the Great Depression, placing new restrictions on the nation's biggest lenders, reining in the Federal Reserve, and crafting new consumer protections. It requires "too-big-to-fail" banks to install new capital and leverage limits, instructs the government to conduct unprecedented ongoing audits of the Fed's lending programs, as well as a one-time audit of its emergency-response programs. Also included in the sweeping package is a tough rule that would limit insured banks' speculative proprietary-trading activities. The controversial proposal would also force big banks to divest their major interests in hedge funds and private equity firms, allowing them to hold no more than 3 percent of a fund's capital, though big banks could have as long as seven years to comply

MarketWatch: [Negotiators in Congress OK sweeping reform of big banks](#)

**Other Industry Reports Articles:**

**SECTOR ELEMENTS**

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

- *June 4 – (International) IDG News Service:* [Visa Launches one-time passcode cards in Europe](#). Visa has launched a payment card in Europe that contains a keypad and an eight-character display for showing a one-time passcode, an additional defense against potentially fraudulent Internet transactions.
- *June 9 – (National) Wall Street Journal:* [FBI uses terror-probe tactics on fraud](#). Federal Bureau of Investigation officials in New York are increasingly employing tools and techniques used to hunt terrorists to take aim at a different kind of criminal: white-collar con artists and inside traders.
- *June 14 – (International) SC Magazine:* [Development of call protection could lead to the end of the theft of customer payment data exchanged over the telephone](#). Ten major audio-data thefts that have occurred in the last year have led to the development of a device that detects and blocks the “DTMF” (dual-tone multi-frequency signaling) tones and obscures card details.
- *June 22 – (National) DarkReading:* [PCI standards stretched to three-year cycle](#). Merchants have gained breathing room for complying with PCI: The PCI Standards Council June 22 announced its standards cycle will move from a two- to three-year cycle.
- *June 29 – (New York) New York Times:* [Circuit breaker kicks in for Citigroup trading](#). An experimental circuit breaker for stock markets that was put in place after last month’s so-called flash crash kicked in for the second time on June 29 after an erroneous trade caused a sudden plunge in the price of Citigroup shares.

### Featured Incidents: Bank and Credit Union Closings, June 2010

Federal and state regulators closed three banks and placed one credit union into conservatorship June 25 raising the number of failed institutions to 96 so far in 2010. Click on the map for more information on state by state bank and credit union closings.

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

[Three banks closed on June 4](#) , [Bank, credit union closed on June 11](#) , [1 bank closed June 18](#) , and [Three banks closed on June 25](#)



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