Homeland Security

FINANCIAL SERVICES SECTOR OPEN SOURCE DIGEST

May, 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

Telecom DoS hides cyber crime

May 12 – (National)

The recent spike in unsolicited and mysterious telephone calls may be part of a new scheme to use telecommunications distributed denial of service (DDoS) attacks to distract individuals from ongoing cyber crime, the FBI warned recently. According to the FBI, cyber criminals are using telephone calls to mobile and land lines to distract victims from the attempts by criminals to empty their bank and trading accounts. The attacks, known as telephony denial-of–service (TDOS), have surged in recent weeks, according to telecom companies working with the FBI. Using automated systems, cyber crooks place calls to prospective victims, and while the victim is distracted by the call, the criminals transfer funds from the victim's bank or trading accounts. As a result, financial institutions that detect the fraud are unable to get in touch with the victim until it is too late.

The New New Internet: **Telecom DoS hides cyber crime**

Two-thirds of all phishing attacks generated by a single criminal group, researchers say

May 12 – (International)

Like convenience stores and fast-food restaurants, phishing is no longer a mom-and-pop operation, according to a study released on May 12. A single crime syndicate dubbed "Avalanche" was responsible for some 66 percent of the phishing traffic generated in the second half of 2009, according to a report published by the Anti-Phishing Working Group (APWG). "This criminal enterprise perfected a system for deploying mass-produced phishing sites, and for distributing malware that gives the gang additional capabilities for theft," the study said. Avalanche successfully targeted some 40 banks and online service providers, as well as vulnerable or nonresponsive domain name registrars and registries, in the second half of 2009, according to APWG. Avalanche could be a successor to the "Rock Phish" criminal operation, which became notorious between 2006 and 2008, APWG said. Avalanche was first seen in December 2008, and was responsible for 24 percent of the phishing attacks recorded in the first half of 2009. "Avalanche uses the Rock's techniques but improves upon them, introducing greater volume and sophistication," it said. To

SECTOR ELEMENTS

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

speed its spread of attacks, Avalanche runs on a botnet and uses fast-flux hosting that makes mitigation efforts more difficult, APWG said.
DarkReading: **Two-thirds of all phishing attacks generated by a single criminal group, researchers say**

Authorities arrest first suspect in massive identity-theft ring

May 13 – (International)

Indian police said May 12 that they have detained a Ukranian man charged in the U.S. with stealing some 40 million credit and debit card numbers. The suspect was detained after he landed in New Delhi on a domestic flight from the southwestern holiday state of Goa May 10, a police spokesman said. He is one of 11 people wanted by the U.S. Justice Department in "the largest hacking and identity theft case ever prosecuted," which was filed in August 2008. Besides the suspect, three Americans, two Ukrainians, two Chinese, one Estonian, a Belarussian and an unidentified suspect are on the wanted list, the Justice Department said. The group is accused of obtaining credit and debit card numbers by hacking into the computer networks of major U.S. retailers — including Barnes & Noble, OfficeMax, shoe retailer DSW, and Sports Authority. Once inside the network, "sniffer programs" captured credit card numbers, passwords, and account information, police said. The data was stored in encrypted servers controlled from Eastern Europe and the United States.
DarkReading: **Authorities arrest first suspect in massive identity-theft ring**

Schapiro: SEC may push for market circuit-breakers

May 18 – (National)

The Securities & Exchange Commission chairwoman said May 18 she expects her agency to issue preliminary findings on its inquiries into the "flash crash" on May 6, when the Dow Jones Industrial Average plunged nearly 1,000 points. The "flash crash" saw bellwethers such as Procter & Gamble Co. plunge nearly 40 percent in seconds. Speaking via a video link to the CFA Institute's 2010 Annual Conference in Boston, the chairwoman said that her agency, in conjunction with the Commodity Futures Trading Commission, has been "looking at a number of issues that can be remediated quickly, even before the exact cause of the crash is known." Among the likely recommendations, she said is the implementation of circuit-breakers or "speed bumps" that give stocks "the opportunity to pause throughout all markets." Previously on May 11, the U.S. House of Representatives Financial Services Subcommittee on Capital Markets failed to pinpoint any single cause for the stock market plummet. The committee held several hearings during which members questioned the heads of the U.S. Securities and Exchange Commission (SEC), New York Stock Exchange and Nasdaq in an attempt to gain some insight on what caused the precipitous drop.
Marketwatch: **Schapiro: SEC may push for market circuit-breakers**
See also, Computerworld: **House Committee fails to find smoking gun on market plunge**
See also, Marketwatch: **Stock sell-off leads to probe of faulty trade**

Researcher finds new type of phishing attack

May 25 – (International)

A researcher has found a new method for carrying out phishing attacks "that takes advantage of the way that browsers handle tabbed browsing and enables an attacker to use a script running in one tab to completely change the content in another tab," according to ThreatPost. The attack, discovered by a researcher for Mozilla, relies on users visiting a controlled infected Web site. When the user visits the infected Web site, it reads what other tabs the user has opened in the browser and changes itself to look

SECTOR ELEMENTS

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

like a selected page. The researcher actually demonstrates it on his Web site in which the page alters to appear as the log-in page for Google. The system could also be used in the case of banking Web sites, etc. to steal login and account information.
The New New Internet: **Researcher finds new type of phishing attack**

Other Cyber Threats Articles:

- *May 4 – (National)* **Gov Info Security: Treasury: Cloud computing host hacked.** The Treasury Department blamed a cloud computing provider for the disruption of its Web site that provides the Internet face of the Bureau of Engraving and Printing, the agency that prints U.S. currency. A blog on May 3 reported that the sites were hacked. The bureau's Web site was inaccessible on May 4 as well. According to the chief research office for IT security software vender AVG, the attack originated from an attack site in Ukraine.
- *May 5 – (International)* **IDG News Service: Hacker develops multi-platform rootkit for ATMs.** A security researcher plans to deliver a talk on security vulnerabilities to ATM's and disclose a new ATM rootkit at the Black Hat computer security conference in July.
- *May 8 – (International)* **Krebs on Security: Visa warns of fraud attack from criminal group.** Visa warned financial institutions that it has received reliable intelligence that an organized criminal group plans to attempt to move large amounts of fraudulent payments through a merchant account in Eastern Europe. The alert states that the criminals claimed to have access to account numbers and the ability to submit a large batch-settlement upload to occur over a weekend.
- *May 10 – (International)* **The H Security: Police apprehend Romanian phishing gang.** Romanian police investigators have exposed a gang of criminals who fraudulently gained online access to bank accounts and for months, continued to draw money from these accounts. Since October 2009, the gang is said to have obtained sensitive data, such as online banking and credit card user names and passwords, particularly of Bank of America customers, via phishing attacks
- *May 17 – (International)* **Krebs on Security: Teach a man to phish....** Phishing may not be the most sophisticated form of cyber crime, but it can be a lucrative trade for those who decide to make it their day jobs. When PhishLabs plotted an average phisher's daily online activity, the resulting graph displayed like a bell curve showing the sort of hourly workload a person would typically see in a regular 9-5 job, a researcher said.
- *May 18 – (International)* **Help Net Security: Phishing page steals prepaid debit card account information.** Symantec revealed that there are phishing sites on the internet that are posing as the main Web site of well-known prepaid debit-card service companies in order to steal card information.
- *May 18 – (International)* **IDG News Service: EFF: Forget cookies, your browser has fingerprints.** Even without cookies, popular browsers such as Internet Explorer and Firefox give Web sites enough information to get a unique picture of their visitors about 94 percent of the time, according to research compiled over the past few months by the Electronic Frontier Foundation.
- *May 18 – (International)* **Krebs on Security: Fraud bazaar carders.cc hacked.** Carders.cc, a German online forum dedicated to helping criminals trade and sell financial data stolen through hacking, has itself been hacked. The once-guarded contents of its servers are now being traded on public file-sharing networks, leading to the exposure of potentially identifying information on the forum's users as well as countless passwords and credit card accounts swiped from unsuspecting victims.

SECTOR ELEMENTS

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

- *May 26 – (International)* **SC Magazine: American Express may have failed to encrypt data.** American Express may be in hot water after a computer engineer discovered a portion of the card brand's website, which claims to be secure, sending private information in the clear.
- *May 26 – (Minnesota; North Dakota)* **The New New Internet: Hackers target small businesses.** The Better Business Bureau of Minnesota and North Dakota, and the Minnesota Cyber Crime Task Force are urging all small businesses with outdated or insufficient online security software to be aware of foreign hackers stealing credit card information and then selling it on the Web.

Physical Security

3 dead in fire at Greek bank during Athens riots

May 5 – (International)

Three people died when an Athens bank went up in flames on May 5 as tens of thousands of Greeks took to the streets to protest harsh spending cuts aimed at saving the country from bankruptcy. Tear gas drifted across the city's center as hundreds of rioters hurled paving stones and Molotov cocktails at police, who responded with heavy use of tear gas. At least two buildings were on fire. The fire brigade said the bodies were found in the wreckage of a Marfin Bank branch, on the route of the march in the city center. An estimated 100,000 people took to the streets as part of nationwide strikes to protest austerity measures imposed as a condition of bailout loans from the International Monetary Fund and other eurozone governments. Three days earlier on May 2, a bomb exploded at a branch of HSBC bank in Athens, damaging the entrance but causing no injuries, police said.

AP

Firefighters extinguish a fire at the Finance Ministry's department in central Athens, Wednesday, May 5, 2010.

Associated Press: 3 dead in fire at Greek bank during Athens riots
See also, Reuters: Explosion damages HSBC branch in Athens, no injuries

Suspects identified in Ottawa firebombing

May 21 – (International)

Police have identified suspects in the May 18 firebombing of a Royal Bank as Ottawa residents linked to an anarchist group, FFFC-Ottawa. The firebombing, which was filmed and posted online, was an unsophisticated attack, said detectives who have collected trace evidence from the burned-out building at Bank Street and First Avenue. Investigators have obtained security video from storefronts along the streets, including high-definition images. The suspects, of which there are believed to be at least four, said in the video that they firebombed the building because the Royal Bank was a sponsor of the Vancouver Olympic Games, which the group claims was held on stolen indigenous land. They also say the Royal is a major backer of Alberta's tar sands, which they describe as one of the most destructive industrial projects in human history. They made their getaway in an SUV. The suspects are linked to an online independent media site and an anti-establishment network that organizes protests against G8 and G20 summits, unfair trade and government cuts to welfare. Several anarchist Web sites are threatening confrontations at the June G8 summit in Huntsville, Ontario, and the G20 summit in

SECTOR ELEMENTS

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

Toronto.
Canwest News Service: Suspects identified in Ottawa firebombing
See also, Australian Broadcasting Corporation: Anarchist group threatens G20 summit

Other Physical Security Articles:

- *May 4 – (Pennsylvania)* **KYW 3 Philidelphia:** **Gauze-wearing bandit uses improvised explosive device to rob Wyncote Bank.** The FBI is searching for a bandit who used an apparent improvised explosive device to rob a Montgomery County bank on May 4. The suspect presented a threatening demand note to a teller, and displayed what appeared to be an improvised explosive device in the bag he was carrying.
- *May 7 – (Florida)* **Sarasota Herald-Tribune:** **Bomb used as weapon in Bradenton bank robbery.** The Manatee County Sheriff's bomb squad examined a device left inside a Bradenton, Florida bank during a robbery May 7. A man put the pipe-bomb type device on the counter of a Wachovia bank and demanded money. The bank was evacuated shortly after the man fled on foot with an undisclosed amount of cash.
- *May 10 – (Georgia)* **Savannah Morning News:** **Mysterious substance found at Ogeechee Road bank.** Authorities shut down a Wachovia bank branch in Savannah, Georgia after an unidentified substance was discovered on cash a customer deposited the afternoon of May 10. Crews were working to decontaminate the bank's interior, contain the material, and identify the substance. The substance was later found to be none threatening.
- *May 14 – (International)* **Hindustan Times:** **Explosions rock Bangkok's financial district.** Six explosions rocked the Bangkok, Thailand financial district May 14, as troops and protesters clashed to control the heart of the capital. Unknown assailants fired M79 grenades at soldiers stationed at the Saladaeng skytrain station on Silom Road, the main financial district and a popular entertainment area, Thai media reports said.
- *May 20 – (Kentucky)* **WSAZ 3 Huntington/Charleston:** **Man dressed as woman arrested for attempted bank bombing.** Prestonsburg, Kentucky Police said a suspect in an attempted bank bombing entered the BB&T bank located on Glynnview Plaza twice before he was taken into custody. Police said that the suspect was carrying a purse full of explosives, but it was not able to detonate.
- *May 26 – (International)* **BBC:** **German bank 'blown up by robbers in botched raid'.** Suspected robbers in Germany appear to have miscalculated the quantity of explosives needed to blow their way into a rural bank. The building housing the bank in the northern village of Malliss was largely destroyed by an explosion on May 26.

AFP
Fire crews worked to clear debris from the explosion

Insider Threats

Security guard enters guilty plea for hacking employer's computers

May 17 – (Texas)

According to Computerworld, a former security guard has pleaded guilty to to two counts of transmitting malicious code for hacking into his employer's computers while

SECTOR ELEMENTS

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

working the night shift at a Dallas hospital. It was not hard to find the 25-year-old hacker, who goes by the name Ghost Exodus, as he posted videos of his misadventures to YouTube. Apparently, he is a member of a hacking group known as the Electronik Tribulation Army and he installed the botnet code in an effort to take down a rival group's Web site. Each count carries a 10-year prison sentence. The man is scheduled to be sentenced September 16.
IT Business Edge: **Security guard enters guilty plea for hacking employer's computers**

Criminal Investigation

Sad stories as mortgage scam complaints leap

May 7 – (National)

The number of complaints involving mortgage foreclosure scams is up 126 percent, according to the Better Business Bureau. Officials with the organization say consumers need to continue to research the potential company offering to help, talk to the lender involved, and take time before signing a contract. State and Federal regulators are also warning about a surge in healthcare-related scams due to the tight economy and the national healthcare reform bill. According to an October 2009 survey conducted by the Coalition Against Insurance Fraud, 57 percent of state fraud bureaus reported a higher incidence of health insurance fraud in 2009 compared to the previous year. The increase was largely attributed to "unauthorized entities selling fake coverage" and "the rise of medical discount plans." Additionally, shortly after the healthcare reform bill was signed into law, the U.S. Department of Health and Human Services issued a warning to consumers to beware of health insurance offers claiming to be part of new federal regulations. For example in Missouri, the State Insurance director warned that a door-to-door salesman was claiming to be a federal agent selling insurance under the new law.

BBB
Video: A spokeswoman from the Better Business Bureau explains the current wave of fraud.

WBBM 780 Chicago: **Sad stories as mortgage scam complaints leap**
See also, Better Business Bureau: **BBB warns that insurance scams are flourishing in current economy**

FBI promises action against money mules

May 11 – (National)

The FBI's top anti-cyber crime official said May 12 that the agency is planning a law enforcement action against so-called "money mules," individuals willingly or unwittingly roped into helping organized computer crooks launder money stolen through online banking fraud. The acting chief of the FBI's cyber criminal section said mules are an integral component of an international crime wave that is costing U.S. banks and companies hundreds of millions of dollars. He said the agency hopes the enforcement action will help spread awareness that money mules are helping to perpetrate crimes. "We want to make sure the public understands this is illegal activity and one of the best ways we can think of to give that message is to have some prosecutions," the director said at a Federal Deposit Insurance Corporation (FDIC) symposium in Arlington, Virginia, May 11. The conference focused on combating commercial payments fraud. Money mules typically are first contacted by e-mail, usually with a greeting that claims the prospective employer found the recipient's

SECTOR ELEMENTS

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

resume on Careerbuilder.com, Monster.com, or some other job-search site. The fraudsters usually represent themselves as international finance or tax companies that are looking to hire "financial agents" to help customers move their money abroad speedily. Candidates often are told the position is a work-at-home job, that no experience is necessary, and that they need only have access to a computer with an Internet connection.
Krebs on Security: **FBI promises action against money mules**

Underground broker network a bane in terror probes

May 14 – (International)

Long before there was MoneyGram and Western Union, people in South Asian countries often used an informal network of brokers, called an "hawala," to transfer money over long distances when it was too inconvenient or dangerous to send cash by courier. Today, the centuries-old system still exists and is used to move billions of dollars annually in and out of countries like Pakistan, Afghanistan, and Somalia. A federal law enforcement official told The Associated Press that a terror suspect is believed to have tapped into such a network to help fund a plot to detonate a car bomb in Times Square May 1. Authorities said three Pakistani men — two in the Boston area and one in Maine — supplied funds to the suspect but may not have known how the money would be spent. The three have been arrested on immigration violations. While most money transfers made through these hawaladars, or brokers, are benign, the system is also routinely used by drug smugglers, terrorists, and other criminals who want to move money without leaving a paper trail.
Associate Press: **Underground broker network a bane in terror probes**

Other Criminal Investigation Articles:

- *May 4 – (Texas)* **Wired:** **Former con man helps feds thwart alleged ATM hacking spree.** A North Carolina grocery worker is being held without bail in Houston on attempted computer hacking charges after inadvertently partnering with an undercover FBI agent in an alleged citywide ATM-reprogramming caper. The 19 -year-old was arrested at a Houston flea market last month after trying a default administrative passcode on a Tranax Mini-Bank ATM there, according to the FBI. The suspect had allegedly hoped to reprogram the machine to think it was loaded with $1 bills instead of $20 bills.
- *May 7 – (Georgia)* **Associated Press:** **3 accused in massive bank fraud.** Federal prosecutors said two former executives of Integrity Bank of Alpharetta, Georgia, and a Florida developer are charged with fraud in connection with $80 million in loans made before the bank collapsed two years ago.
- *May 8 – (Virginia)* **Roanoke Times:** **National Bank again targeted in scam.** Officials of the National Bank of Blacksburg, Virginia said on May 7 that residents are reporting receiving scam phone calls requesting confidential debit card and bank account information. Officials said the calls appear to be a continuation of a large-scale phishing attack on the bank in mid-April when fraudulent e-mails, phone calls and text messages using the bank's name, logo and Web site were sent to some Southwest Virginia residents.
- *May 9 – (National)* **KEZI 9 Eugene:** **ATM users on alert after skimming cases along West Coast.** An unidentified suspect is wanted by authorities in three different states, including Oregon. Police said he is stealing bank card numbers and pins using an ATM skimming device.

SECTOR ELEMENTS

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

- *May 12 – (New York)* **Wall Street Journal: Wall Street probe widens.** Federal prosecutors, working with securities regulators, are conducting a preliminary criminal probe into whether several major Wall Street banks misled investors about their roles in mortgage-bond deals, according to a person familiar with the matter.
- *May 17 – (Illinois)* **Chicago Sun-Times: FBI offers $10K reward for info on 'Citibank Bandit'.** The FBI is offering a reward of up to $10,000 for information about the "Citibank Bandit," responsible for the robbery of 11 banks, six of which were Citibank branches, in and around the downtown Chicago area since February 2009.
- *May 20 – (Colorado)* **KKTV 11 Colorado Springs: FBI catches alleged bank robber dubbed 'portfolio bandit'.** An accused bank robber has been caught and indicted on 11 counts. The suspect, dubbed the "portfolio bandit" by the FBI, allegedly robbed 11 banks in Denver.
- *May 23 – (Oregon)* **Associated Press: Man arrested in Eugene accused as 'Grandpa Bandit'.** A man arrested in Eugene, Oregon in connection with a bank robbery has been indicted by a federal grand jury on charges that he robbed seven Oregon banks in a spree attributed to the "Grandpa Bandit."
- *May 24 – (National)* **Washington Post: District food servers charged in theft of patrons' credit card numbers.** Three servers at the Cheesecake Factory restaurant on Wisconsin Avenue in Washington D.C. allegedly stole credit card numbers from patrons as part of a scheme that racked up more than $117,000 in fraudulent charges between 2008 and last year, authorities said.
- *May 25 – (Arizona; Nevada)* **Las Vegas Review-Journal: Las Vegas Investigation: Crime ring busted, FBI says.** Federal authorities allege that two cells of Bulgarian organized criminals defrauded Las Vegas and Phoenix area car dealers out of $1.6 million and stole at least $700,000 from bank ATMs around the valley. In all, 11 people were charged in three separate indictments unsealed recently in federal court after a two-year FBI investigation that involved the use of court-approved wiretaps.
- *May 25 – (Wisconsin)* **Associated Press: 'Tinfoil bandits' arrested in Rock County.** Rock County, Wisconsin authorities have arrested three people they say disabled a convenience store's credit card system by covering the store's satellite with tin foil, disabling it from transmitting credit transactions, and then made multiple purchases.

Other Industry Reports

PCI Security Council updates requirements for payment card devices

May 12 – (International)

The council that administers the Payment Card Industry Data Security Standard released on May 12 new requirements that vendors of payment card devices will be expected to incorporate into their products going forward. The new requirements are in the latest version of the council's PIN Transaction Security (PTS) requirements and are designed to bolster security on retail point-of-sale card readers and unattended kiosks and payment terminals, such as those found at airports and gas stations. Version 3.0 of the PCI council's PTS includes three new modules to secure sensitive card data for device vendors and their customers. One of the modules contains requirements pertaining to the secure reading and exchange of data on payment-card devices. The requirements would enable the secure reading and encryption of sensitive cardholder data at the point where a credit or debit card is swiped. A second module spells out the

SECTOR ELEMENTS

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

security standards that device vendors will be expected to follow while integrating all of the different components that make up an unattended point-of-sale device that accepts PIN-based debit-card transactions. The third module, called Open Protocols, contains a set of new requirements related to wireless-enabled payment-card devices.
Computerworld: **PCI Security Council updates requirements for payment card devices**

RBC Bank, Wachovia, SunTrust on Weiss list of vulnerable banks

May 25 – (National)

Raleigh-based RBC Bank is one of 20 large U.S. banks and 11 Triangle-based banks considered vulnerable by Weiss Ratings, a Florida-based company that evaluates the financial strength of insurers, banks and savings and loans. A new Weiss report gives RBC Bank, the U.S. banking arm of the Royal Bank of Canada a "D-" The bank, with $27.5 billion in assets, has been dealing with a loan portfolio weighed down by depressed real estate in Florida. Three other huge players in the Triangle banking market also are on the Weiss list of weakest banks. Atlanta-based SunTrust Banks joins RBC Bank in receiving a D- rating. Weiss gave D ratings to Bank of America, the country's largest commercial bank but No. 5 in the Triangle, and Triangle-market leader Wachovia, a Charlotte-based bank now owned by San Francisco-based Wells Fargo & Co. All told, Weiss says, 2,259 U.S. banks and savings and loans, controlling $5.8 trillion, or 43.8 percent of the industry's total assets, are vulnerable. Those banks are given grades ranging from D+ to D-. The Federal Deposit Insurance Corp. said May 20 that the number of banks on its confidential "problem" list grew to 775 in the January-March period from 702 in the previous quarter. "The banking system still has many problems to work through, and we cannot ignore the possibility of more financial market volatility," the FDIC chairman acknowledged. But she added: "The trends continue to move in the right direction."
Triangle Business Journal: **RBC Bank, Wachovia, SunTrust on Weiss list of vulnerable banks**
See also, Associated Press: **FDIC says number of 'problem' banks is growing**

Walmart to support smartcard payments

May 21 – (National)

Retail giant Walmart Stores Inc. is reportedly planning on making all its payment terminals in the U.S. compliant with a smartcard-based credit card technology that is widely used around the world but is not common in the U.S. Walmart's plans were disclosed at a smartcard conference being held this week, and were first reported by Storefront Backtalk. Storefront Backtalk quoted Walmart's director of payment services as saying the retailer was working on making all payment terminals in its domestic stores chip-and-PIN-capable. The director was reported as having said that signature-based credit-card transactions had become a "waste of time" for Walmart. Such a move by Walmart would have widespread ripple effects. As the largest retailer in the world, a Walmart decision to support chip-and-PIN could finally nudge card issuers, payment processors and other merchants to adopt the technology.
Computerworld: **Walmart to support smartcard payments**

Other Industry Reports Articles:

- *May 19 – (National)* **SC Magazine:** **US regulators form plans to encourage banks to better protect customers from online fraud.** A panel of regulators in the U.S. are drafting plans to force banks to protect their customers better from a surge in online account fraud. The panel with representatives from the FDIC, the Federal

SECTOR ELEMENTS

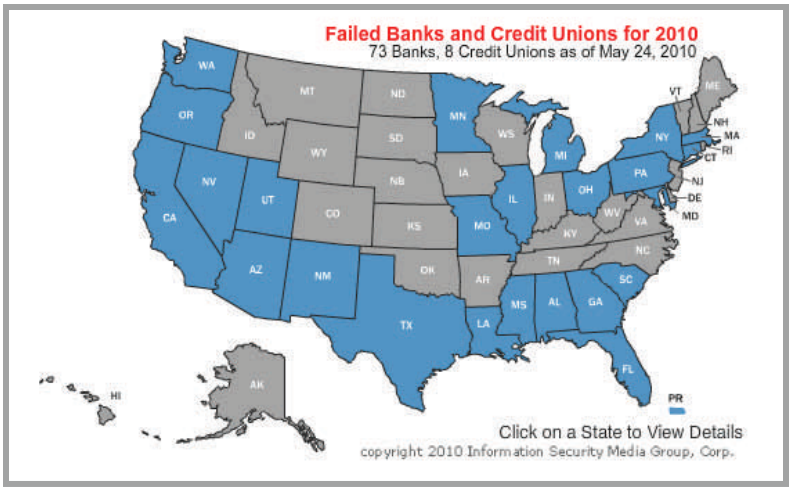
- Cyber Threats
- Physical Security
- Insider Threats
- Criminal Investigation
- Other Industry Reports

Reserve System and other agencies is reacting to the rapid evolution of malicious computer programs designed to drain accounts.

- *May 20 – (National)* **New York Times: Bill passed in Senate broadly expands oversight of Wall St.** The U.S. Senate May 20, approved a far-reaching financial regulatory bill putting Congress on the brink of approving a broad expansion of government oversight of the increasingly complex banking system and financial markets. The legislation is intended to prevent a repeat of the 2008 financial crisis, but also reshapes the role of numerous federal agencies and vastly empowers the Federal Reserve in an attempt to predict and contain future debacles.
- *May 21 – (National)* **USA Today: Feds unite to form a new financial fraud task force.** On May 21, federal officials plan to unveil May 21 a potentially important effort to investigate and prosecute financial fraud cases. The U.S. Attorney's Office in Richmond will coordinate the Virginia Financial and Securities Fraud Task Force with representatives of the Securities and Exchange Commission, Commodity Futures Trading Commission, FBI, U.S. Postal Service and IRS, as well as state law enforcement agencies.

Featured Incidents: Bank and Credit Union Closings, March 2010

State and federal regulators closed one bank May 21. This closing raises to 81 the number of failed institutions so far in 2010. Click on the following picture to open to an interactive map of the United States for more information on state by state bank and credit union closings. For more information on all bank closures for the month of May, please click on one of the following links.



For more information on bank and credit union failures, see:
7 banks fail on April 30
Four banks fail May 7
U.S. bank failures inch to 72
1 bank closed on May 21

Your comments and suggestions are highly valued. Please send us feedback at: 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: CIKRISEaccess@DHS.gov.