



FINANCIAL SERVICES SECTOR OPEN SOURCE DIGEST

February, 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

Spooks scour gambling sites in terror finance probe

February 5 – (International)

Security services are running 23 ongoing investigations into the exploitation of gambling websites to finance terrorism. The evidence shows the online gaming industry is still vulnerable, and a prime target for criminals and terrorists, even after being at the center of the conviction of the man described as the “[godfather of cyber-terrorism for al-Qaida](#)” and two of his associates in 2007. The three men were convicted for inciting people to commit murder through their extremist websites used Windows-based Trojans to steal information such as credit card numbers, and then laundered them using the gambling sites. The convictions were highly publicized, but what was revealed at the ‘[Combatting Cybercrime in Betting and Gaming 2010 Conference](#)’ in London the week of January 25 - 29 was the scale of ongoing investigations into terrorism financing, and that one of those convicted had been accessing 17 gaming sites while in Belmarsh prison. It also came to light that on an unnamed credit card company’s database, all three men came up as clients, along with 17 others whose date of birth, nationality and first name matched the convicted three. Together they had 190 pre-paid credit cards still in circulation, with balances of 10,000 pounds on each card.

The Register: [Spooks scour gambling sites in terror finance probe](#)

New Russian botnet tries to kill rival

February 9 – (International)

An upstart Trojan horse program, “Kill Zeus,” has decided to take on its much-larger rival by stealing data and then removing the malicious program from infected computers. Security researchers say that the relatively unknown added this functionality just a few days ago in a bid to displace its larger rival, known as Zeus. The feature apparently removes the Zeus software from the victim’s PC, giving Spy Eye exclusive access to usernames and passwords. Zeus and Spy Eye are both Trojan-making toolkits, designed to give criminals an easy way to set up their own “botnet” networks of password-stealing programs. These programs emerged as a major problem in 2009, with the U.S. Federal Bureau of Investigation estimating last October that they have caused \$100 million in losses. Trojans such as Zeus and Spy

SECTOR ELEMENTS

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

Eye steal online banking credentials. This information is then used to empty bank accounts by transferring funds to so-called money mules — U.S. residents with bank accounts — who then move the cash out of the country. Sensing an opportunity, a number of similar Trojans have emerged recently, including Filon, Clod and [\[Bugat\]](#), which was discovered just last month.

Computerworld: [New Russian botnet tries to kill rival](#)

New banking trojan discovered targeting businesses' financial accounts

February 9 – (International)

The infamous Zbot botnet that spreads the pervasive Zeus Trojan has been seen distributing a brand-new banking Trojan — one that researchers say could serve as a lower-cost alternative to the popular Zeus and Clampi malware for cybercriminals. The new Bugat Trojan, which was discovered by researchers at SecureWorks, appears to be aimed at mostly business customers of large and midsize banks. It is built for attacks that hack automated clearinghouse (ACH) and wire transfer transactions for check and payment processing — attacks in which U.S.-based small and medium-sized businesses (SMBs) and state and local governments are losing an average of \$100,000 to \$200,000 per day, according to [data](#) [hyperlink will prompt user to download a PDF of the white paper] from Neustar. To date, Zeus and Clampi Trojans have mostly been used for stealing financial credentials. But a security researcher with SecureWorks' Counter Threat Unit (CTU) says Bugat has some of the same features as other banking Trojans, with a few twists: It uses an SSL-encrypted command and control (C&C) infrastructure via HTTP-S, and also goes after FTP and POP credentials via those encrypted sessions.

DarkReading: [New banking trojan discovered targeting businesses' financial accounts](#)

Major flaw discovered in Chip and PIN technology that could allow a fraudster to make purchases with a dummy login

February 15 – (International)

A report by security researchers at Cambridge University has demonstrated a flaw in Chip and PIN technology. It said that the flaw would allow a fraudster to use a genuine card to make a payment without knowing the card's PIN, and to remain undetected even when the merchant has an online connection to the banking network. The fraudster would be able to perform a man-in-the-middle attack to trick the terminal into believing that the PIN verified correctly, while telling the issuing bank that no PIN was entered at all. This would not work at a cashpoint or ATM, but would allow for large purchases. With the use of a man-in-the-middle device, which can intercept and modify the communications between card and terminal, a fraudster can trick the terminal into believing that PIN verification succeeded by responding with 0x9000 to Verify, without actually sending the PIN to the card.

SC Magazine: [Major flaw discovered in Chip and PIN technology that could allow a fraudster to make purchases with a dummy login.](#)

Other Cyber Threats Articles:

- *February 1 – (Delaware; National)* **Internet Evolution: [How — and where — cybercriminals hide.](#)** Delaware holds the top spot in the recent [Financial Secrecy Index](#) (FSI) rankings of secretive jurisdictions compiled by the internationally respected Tax Justice Network, an independent organization promoting justice in tax issues. Several other U.S. states – Nevada, Oregon, and Wyoming – have also received international criticism for lax company registration laws, but it is only in Delaware that an applicant can delay providing company member names, and if

SECTOR ELEMENTS

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

timed right, for as long as a year before the state steps in, allowing plenty of time for deals to be completed and illicit funds laundered out of the U.S.

- *February 2 – (National) Forbes: [Cybercrime checks into the hotel industry](#)*. A [report](#) presented by a cybersecurity researcher on February 2 at the Black Hat security conference in Arlington, Virginia, found that over the past year America’s hotels have been hit by increasingly sophisticated invasions by organized cybercriminals.
- *February 3 – (International) Computerworld: [Old security flaws still a major cause of breaches, says report](#)*. An overemphasis on tackling new and emerging security threats may be causing companies to overlook older but far more frequently exploited vulnerabilities, according to a recent [report](#) from Trustwave, which is based on an analysis of data gathered from more than 1,900 penetration tests and over 200 data breach investigations conducted on behalf of clients such as American Express, MasterCard, Discover, Visa and several large retailers.
- *February 4 – (International) The Register: [Carbon trade phish scam disrupts exchanges](#)*. Phishing fraudsters have extended their net beyond harvesting e-banking credentials via a scam that resulted in the theft of 250,000 carbon permits worth over three million Euros. The outbreak resulted in the suspension of trading in several EU registries on February 2. The crooks are thought to have created fake emission registries, promoted via spam emails, before using identity details submitted on these sites to trade rights to blow-off greenhouse gases on the legitimate sites.
- *February 4 – (New York) Associated Press: [NY town says hacker stole \\$378K from bank account](#)*. Officials in a Hudson Valley town say a computer hacker broke into the town’s bank account and stole \$378,000 in municipality funds. The Town of Poughkeepsie supervisor said February 3 that the money was transferred to banks in Ukraine after someone broke into the town’s account last month.
- *February 10 – (National) SC Magazine: [ID theft still on the rise, but victims respond faster](#)*. Incidents of identity fraud and the total cost of fraud climbed again last year, but consumers are becoming better equipped to respond to the occurrences of theft, according to the seventh annual [2010 Identity Fraud Survey Report](#).
- *February 11 – (Michigan; Texas) Bankinfosecurtiy.com: [Customer sues bank after phishing attack: MI-based business lost \\$550,000 in breach](#)*. A Michigan-based metal supply company is suing Comerica Bank, claiming that the bank exposed its customers to phishing attacks. A lawsuit filed by Experi-Metal Inc. (EMI) in Sterling Heights, Michigan, alleges that Dallas-based Comerica opened its customers to phishing attacks by sending emails asking customers to click on a link to update the bank’s security software.
- *February 17 – (International) AuctionBytes.com: [Paymate experiences DDoS attack, no risk to customer data](#)*. Online payment service Paymate was down due to a DDoS (distributed denial-of-service) attack. The company’s vice president of sales and marketing told AuctionBytes the site has been down since early February 16, and at no time was any user data or information been at risk.

Physical Security

Explosion at Darwin insurance office injures 15

February 3 – (International)

Fifteen people were admitted to the hospital in the northern Australian city of Darwin on February 3 after an explosion at an insurance office, officials said. A man is in custody and the major crimes unit is probing the blast at the Territory Insurance Office, Northern Territory police said. A “disgruntled claimant” was behind the attack, wheeling a

SECTOR ELEMENTS

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

shopping trolley containing three jerry cans and fireworks into the office, the Australian Broadcasting Corp. reported. “This is not a terrorist incident,” the broadcaster cited a commander as saying. Four people were in a serious but stable condition after being treated for burns and respiratory problems caused by smoke inhalation, a spokeswoman for Royal Darwin Hospital said in a telephone interview. The rest were stable and expected to be discharged later today. Six staff members were among those injured, TIO’s chief executive said in an e-mailed statement. Police “believe this is an isolated incident and there is no ongoing threat to TIO, its staff or its customers,” the chief executive said.

Bloomberg: [Explosion at Darwin insurance office injures 15](#)



ABC NEWS
Police attend the scene of an explosion at the Woolworths complex on Smith Street in Darwin.

Bomb blast hits J.P. Morgan building in Greece

February 16 – (International)

A medium-sized bomb exploded on February 16 at a building housing offices of financial services firm J.P. Morgan in Athens, Greek police said. A warning was phoned to a Greek newspaper 30 minutes before the explosion, and police evacuated the building, a police spokesman told CNN. No one was hurt. The callers did not identify themselves, he said. The warning call “means they don’t want to have victims,” he said. “They never say who it is when they call. They claim it after.”

CNN: [Bomb blast hits J.P. Morgan building in Greece](#)

White powder found at Paterson police headquarters found to be harmless

February 17 – (New Jersey)

An envelope containing a white powdery substance was sent to the Patterson, New Jersey’s Public Safety Complex, the latest in a series of similar incidents in Passaic and Bergen counties. The white powder turned out to be harmless. Authorities are still investigating envelopes containing white powder that were sent to a Bank of America bank in Paterson, and state Motor Vehicle Commission offices in Wayne and Eatontown, and Hackensack City Hall on February 11. On February 15 employees at an interior design store in Westwood discovered a white substance in an envelope they opened by mistake. The letter was addressed to a Citibank branch, an employee said.

North Jersey Record: [White powder found at Paterson police headquarters found to be harmless](#)

Security up after Thai bank blasts

February 28 – (International)

Thailand’s prime minister ordered stepped-up security in Bangkok on February 28 after four banks were targeted with small explosive devices. The attacks the evening of February 27, in which no one was hurt, came a day after the Supreme Court ordered \$1.4 billion of a exiled former leader’s assets seized for corruption. Authorities had voiced concern the verdict could spark violent protests by his supporters but none occurred. The Prime Minister told reporters on February 28 that he



REUTERS
Police secure the area as a bomb squad investigates an explosion outside a branch of the Bangkok Bank

SECTOR ELEMENTS

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

did not know who was behind the attacks on Bangkok Bank, the country's biggest commercial bank. Police said only minor damage was caused when grenades exploded at two of the bank's branches, and were found unexploded at two others.

Associated Press: [Security up after Thai bank blasts](#)

Other Physical Security Articles:

- *February 2 - (Colorado)* Associated Press: [Colo. banks urged to report suspicious people](#). With a nearly 30 percent jump in bank robberies last year when compared with 2008, banks in Colorado are being encouraged to report suspicious people entering their banks as a way to discourage would-be bank robbers. "It could be something as simple as asking people to take off their sunglasses and hats," said Denver's district attorney on February 1.
- *February 9 - (New York)* NBC New York: [FBI hunts Queens bank robbers who use gun, fake bomb](#). Armed with a handgun and a fake bomb, two men robbed four banks in Queens in a two week period. No one has been hurt in the hold-ups. But FBI and NYPD officials are worried it is only a matter of time before they hurt someone if they are not caught. This bank robbery spree began back on January 22.
- *February 14 - (Minnesota)* Associated Press: [Alleged AIDS patient robs bank with syringe](#). FBI officials said a man claiming to have AIDS and "nothing to live for" used a hypodermic needle to hold up a Minneapolis bank. The FBI said the robber walked into TCF Bank about 3 p.m. on February 12. He allegedly threatened three tellers with a syringe that appeared to contain blood.

Insider Threats**Ex-National Penn Bank officer charged in \$4.4 million embezzlement scheme**

February 24 - (International)

Federal authorities on February 23 charged a former National Penn Bank officer with embezzling more than \$4.4 million and using the money to pay off debts and buy property and vehicles. Prosecutors said a former vice president of loan operations created lines of credit using fictitious names and electronically transferred the funds into accounts held by herself and relatives. The 62 year old suspect of Boyertown is charged with one count each of bank fraud, embezzlement by a bank employee, and filing a false tax return, a U.S. attorney said. The suspect filed a tax return for 2007 that did not include \$719,571 in income, prosecutors said. Prosecutors said the suspect, while employed at the Boyertown-based bank, spent much of the money on vehicles, several residences and other items. They said she also transferred hundreds of thousands of dollars to relatives and others. The National Penn senior vice president for corporate communications said in a statement that no customer funds were lost.

Reading Eagle: [Ex-National Penn Bank officer charged in \\$4.4 million embezzlement scheme](#)

Criminal Investigation**FBI: 'High Country Bandits' target Marana bank, others throughout Southwest**

February 18 - (National)

A two-man crew has been holding up rural banks throughout the Southwest over the past five months, including one in Marana, Arizona, according to the FBI. The duo, dubbed the "High Country Bandits," by the FBI are believed to be responsible for at least 12 heists in Arizona, Colorado, and New Mexico between September and earlier

SECTOR ELEMENTS

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

this month, according to an agency news release. The first stickup occurred September 8 in the White Mountains community of Heber, while other Arizona locales allegedly hit include Flagstaff (twice), Gold Canyon, Payson, Phoenix, Pinetop and Prescott Valley, the release said. The Marana swindle happened on December 15 at a Wells Fargo. **Arizona Daily Star:** [FBI: 'High Country Bandits' target Marana bank, others throughout Southwest](#)

Criminals hide payment-card skimmers inside gas station pumps

February 22 – (International)

Criminals hid bank card-skimming devices inside gas pumps — in at least one case, even completely replacing the front panel of a pump — in a recent wave of attacks that demonstrate a more sophisticated method of stealing money from unsuspecting victims filling up their gas tanks. Some 180 gas stations in Utah, from Salt Lake City to Provo, were reportedly found with skimming devices sitting inside the gas pumps. The scam was first discovered when a California bank's fraud department discovered that multiple bank card victims reporting problems had all used the same gas pump at a 7-Eleven store in Utah. Card skimming has been on the rise during the past year, with most attackers rigging or replacing merchant card readers with their own sniffer devices or ATM machines. The chief technology officer for BT Counterpane says attackers in Europe are also moving skimming devices inside gas pumps as a way to avoid detection. **DarkReading:** [Criminals hide payment-card skimmers inside gas station pumps](#)



KSL 5 SALT LAKE CITY
A fake gas pump panel scans and transmits personal information, including PIN numbers, via Bluetooth.

3 Bulgarians charged in 44-day ATM hacking spree

February 24 – (Massachusetts)

Three Bulgarian men were charged on February 24 with defrauding banks of more than \$137,000 in a scheme that attached electronic skimming devices to numerous automatic teller machines in Massachusetts. In the 44-day hacking spree, the men planted skimmers on ATMs maintained by Bank of America and Citizens Bank and secretly recorded information stored on the magnetic strips of cards as they were being used. The men also allegedly used concealed cameras to record the corresponding personal identification numbers. The men compromised “numerous” ATMs throughout eastern Massachusetts. In a separate event in Florida, Four Bulgarian men put “skimmers” on ATM machines at SunTrust banks in Hillsborough and Pinellas counties in the summer of 2009 and obtained identifying information on hundreds of bank accounts, according to a federal complaint. The information was used to withdraw nearly \$200,000 from the compromised accounts. Federal authorities have arrested one of the suspects and are searching for the other three. All four men were arrested by Pinellas County sheriff's deputies in December but were later released when state charges were dropped.

The Register: [3 Bulgarians charged in 44-day ATM hacking spree](#)

See also, Tampa Tribune: [1 arrested, 3 sought in ATM 'skimmer' scheme](#)

Other Criminal Investigation Articles:

- *February 1 – (Florida)* **Orlando Sentinel:** [Lake investigating scam targeting debit card customers](#). Fraud investigators in Lake County are looking into reports that debit card users are being targeted by scam artists. Some bank customers reported receiving text messages or recorded messages on their phones informing

SECTOR ELEMENTS

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

them that their debit cards were cancelled or somehow compromised, the Lake County Sheriff's Office said.

- *February 4 – (New Hampshire) Associated Press: [Manchester police probe 3 bank heists in 3 days](#).* Manchester police are investigating the city's third bank robbery in as many days. Police say a man demanded money on January 3 from a TD Bank branch on South Main Street. The robbery came one day after a holdup at a Citizen's Bank branch on Elm Street. A Bank of New England branch on Elm Street was robbed on February 1.
- *February 4 – (Michigan) WWJ 950 Detroit: [State shuts down fake mortgage company](#).* State officials have shut down a fake Detroit mortgage company that they say was trying to steal consumers' money and identity. The Office of Financial and Insurance Regulation pulled the plug on the phony company's website, called "Kenneth and Doyle Financial," and ordered it to stop doing business.
- *February 5 – (Texas) Houston Chronicle: [FBI: 'Billy goat bandit' strikes 12th bank](#).* A man suspected of robbing 11 Houston-area banks made it an even dozen on February 5 when he struck a bank inside a grocery in Katy, authorities said. While he had been dubbed the "billy goat bandit" because of his prominent facial hair, the robber was clean-shaven when he hit a First Convenience Bank branch shortly after noon inside the Kroger, FBI officials said.
- *February 17 – (California) Court House News Service: [Long Beach man admits to \\$33M Ponzi scam](#).* A Long Beach man pleaded guilty to defrauding more than 50 investors out of \$33 million in a real estate Ponzi scheme, the U.S. Attorney's Office announced on February 17. The 33 year old pleaded guilty on February 16 to federal wire fraud for promising high returns on real estate investments that turned out to be a Ponzi scam.
- *February 18 – (National) Housingwire: [FinCEN sees spike in possible foreclosure and mortgage modification scams](#).* Nearly a year after issuing a red flag advisory to servicers in April 2009 to beware of foreclosure scams, the Financial Crimes Enforcement Network (FinCEN), an overseer of financial activities for the US Treasury, says it received hundreds of suspicious activity reports (SARs) regarding the fraud. In data released on February 18, FinCEN also gave information on the more popular forms of mortgage modification fraud.
- *February 19 – (Georgia) Associated Press: [1 arrested in \\$25 million credit card scheme](#).* Federal agents have arrested a Marietta man believed responsible for a nationwide telemarketing scheme that defrauded consumers out of \$25 million. Prosecutors say the 34-year-old suspect and two others would promise through telemarketing to save customers thousands of dollars by negotiating lower credit card rates for a fee of at least \$749. Authorities say in an affidavit that the three would rarely follow through.

Other Industry Reports

White House proposes increase in FDIC deposit insurance fund

February 2 – (National)

The U.S. President's administration wants to increase the size of the insurance fund that repays depositors in failed banks, a step that would require all banks to pay larger fees to the Federal Deposit Insurance Corp. (FDIC.) The change, which would require legislation, is part of a broader effort by the administration to raise taxes and fees on banks to discourage risk-taking and to create better shock absorbers for future crises. The FDIC fund is designed to gather money in good times and spend it in bad times. But the fund drained quickly as banks failed over the past two years, forcing the FDIC to

SECTOR ELEMENTS

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

increase fees and impose special assessments at the very moment that banks could ill afford the additional expense. The insurance fund also ran out of money during the last banking crisis, in the late 1980s and early 1990s. The administration's budget proposal, released on February 1, suggests that the FDIC needs a larger insurance fund.

Washington Post: [White House proposes increase in FDIC deposit insurance fund](#)

US Treasury backs listing threats to financial system.

February 19 – (International)

The U.S. Treasury Department said it endorsed a report from the international body fighting money laundering that blacklisted Iran, Angola, North Korea, Ecuador and Ethiopia for posing risks to the international financial system. "The U.S. Treasury Department welcomes the [Financial Action Task Force \(FATF\) report](#) statements this week identifying countries with strategic deficiencies in the area of anti-money laundering and combating the financing of terrorism," the Treasury said. The task force said on February 18 that Pakistan, Turkmenistan and Sao Tome and Principe were jurisdictions that also continue to have deficiencies in their systems for countering money laundering and terror financing that need to be addressed. The task force said other countries should "advise their financial institutions to give special attention to business relationships and transactions with Iran" and with Iranian institutions to head off any "financing of terrorism risks emanating from Iran."

Reuters: [US Treasury backs listing threats to financial system](#)

Highlight: Bank and Credit Union Closings for February 2010

Four banking institutions - two banks and two credit unions - were closed by state and federal regulators recently. These latest closings bring to 24 the total number of failed institutions so far in 2010. These closings are the most recent, with an additional five banks closing since the beginning of February.

- The National Credit Union Administration (NCUA) on February 25 liquidated Friendship Community Federal Credit Union of Clarksdale, Mississippi, and accepted Shreveport Federal Credit Union's offer to purchase and assume the credit union
- The NCUA liquidated Mutual Diversified Employees FCU of Santa Ana, California, and accepted Schools First Federal Credit Union's offer to purchase and assume it.
- River Community Bank, Carson City, Nevada, was closed by the Nevada Department of Business and Industry, Financial Institutions Division, which appointed the Federal Deposit Insurance Corporation (FDIC) as receiver.
- Rainier Pacific Bank, Tacoma, Washington, was closed by the Washington Department of Financial Institutions, which appointed the FDIC as receiver.
- Marco Community Bank, Marco Island, Florida, was closed by the Florida Office of Financial Regulation, which appointed the FDIC as receiver.
- The La Coste National Bank, La Coste, Texas, was closed by the Office of the Comptroller of the Currency, which appointed the FDIC as receiver.
- George Washington Savings Bank, Orland Park, Illinois, was closed by the Illinois Department of Financial Professional Regulation - Division of Banking, which appointed the FDIC as receiver.
- La Jolla Bank, FSB, La Jolla, California, was closed by the Office of Thrift Supervision, which appointed the FDIC as receiver.
- Regulators in Minnesota closed 1st American State Bank. The Federal Deposit Insurance Corp. said Community Development Bank FSB in Ogema would take over.

Bank Info Security: [Two banks, two credit unions closed Feb. 26](#)

See also, **Bank Info Security:** [Four banks closed on Feb. 19](#)

See also, **American Banker:** [Minnesota bank fails in 16th failure of '10](#)

**SECTOR
ELEMENTS**

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

Other Industry Reports Articles:

- *February 3 – (National) Reuters: [US Treasury to recover \\$170 bln after PNC repayment](#).* The U.S. Treasury Department said on February 3 it will have recovered \$170 billion in financial rescue funds once PNC Financial Services Group Inc has repaid money loaned to it from the government’s bailout program.
- *February 4 – (National) Washington Post: [Treasury offers loans to banks funding community development](#).* The Treasury Department said February 3 that it will offer up to \$1 billion in low-cost loans to banks that focus on funding development in lower-income communities, part of the administration’s new emphasis on helping smaller banks. The special program, which offers more favorable terms than those available to most banks, will benefit a group of institutions that work in areas where mainstream banks make few loans.
- *February 11 – (International) SC Magazine: [PCI DSS regulations should not be written off as being unsuitable, as an understanding of the terms and options are often ignored](#).* Credit card companies should be encouraged to work with smaller vendors when it comes to compliance, but it is too soon to write off PCI regulations. Following claims made on February 10 that the Payment Card Industry Data Security Standard (PCI DSS) are not suitable for small businesses, and that enforcements could cause a business to go under, the head of PCI at ProCheckUp Labs agreed with the principal that PCI DSS is by no means a ‘one-size fits all’ standard, but complaining about it will not get companies anywhere.
- *February 19 – (National) Washington Post: [Fed raises interest rate on emergency loans to banks](#).* The Federal Reserve on February 18 took another step toward winding down its expansive efforts to prop up the financial system, raising the interest rate that banks must pay to take out emergency loans. Banks that need emergency funds through the Fed’s “discount window” will now have to pay 0.75 percent, not the 0.5 percent they have been paying.

Your comments
and suggestions
are highly valued.
Please send us
feedback at:

cikr.productfeedback@dhs.gov