



Fraud/Scam Report



The following banking-related items were recently reported by the Department of Homeland Security as part of their [Daily Open Source Infrastructure Protection Report](#).

International and National News

Undetectable fake ATM keyboard steals PINs in real time

January 6, Help Net Security

Thieves and scammers are an inventive bunch, especially when it comes to stealing money indirectly. And the latest discovery of a fake keyboard placed over an ATM's legitimate one that records the typed-in PIN — in conjunction with a fake magnetic strip reader that can be manufactured from cheap spare electronic parts — shows this kind of crime does not require a lot of funds and can bring in quite a lot of money. According to Gizmodo, the keyboard is virtually undetectable by anyone who is not an expert, and looks exactly like the real thing.

[Read More.](#)

Federal charges filed against man accused of defrauding St. Paul Croatian Federal Credit Union

January 6, Willoughby News-Herald

A person who resides in both Eastlake, Ohio, and Skopje, Macedonia, is facing two charges of bank fraud and one charge of money laundering. The suspect is accused of fraudulently obtaining several loans totaling \$2.5 million from St. Paul Croatian Federal Credit Union in Eastlake between July and August 2009, according to the United States attorney for the Northern District of Ohio. Authorities believe he obtained most of the loans by falsely listing the names of other persons as the applicants and intended recipients, he said.

[Read More.](#)

AOL customers targeted in new phishing attack

January 5, Softpedia

A new phishing attack is targeting AOL subscribers by claiming that they need to update their account billing information in order to avoid facing restrictions. The rogue emails have their header spoofed to appear as originating from —AOL Member Billing Services|| and bear a subject of —Billing update on file must be performedz.|| The body uses an AOL template which includes an AOL Member Services banner and the enclosed message reads: —Our records indicate that your account hasn't been updated as a part of our regular account maintenance. Our new SSL servers check each account for activity and your information has been randomly chosen for verification. AOL Member Services strives to serve their customers with better and secure banking service. Notification: Failure to update your account information may result in account limitation at shopping on our portal.

[Read More.](#)

The evolution of cyber criminal operations

January 4, Help Net Security

There is a concerning evolutionary step cyber criminal operations are taking to more effectively diversify the distribution of their ill-gotten gains, according to Fortinet. The campaigns, which were seeded in a number of Asian and European countries, solicited local individuals who already have or had established relationships in the banking industry or were looking for work as 'online sales administrators'. To make these 'localized' campaigns even more effective, they incorporated regional-sounding domain names, such as cv-eur.com, asia-sitezen.com, and australia-resume.com. Upon closer scrutiny, Fortinet discovered all three domains were registered to the same Russian contact, and all contact addresses for worldwide recruitment used Google mail hosting.

[Read More.](#)

The evolution of check fraud

January 4, BankInfoSecurity.com

Despite an overall, albeit gradual, decline in check use, check fraud continues to plague the financial industry. And banks and credit unions are challenged to curb these evolving crimes. According to the new Faces of Fraud Survey, check fraud is one of the top three fraud forms plaguing banking institutions, joining the likes of phishing and vishing, and payment card fraud. Sixty-three percent of survey respondents say they experienced check fraud in 2010. Yet only 34 percent of banks and credit unions say they are well equipped to fight these crimes. —Check fraud is so prevalent because it's easy,|| said the vice president of the Center for Regulatory Compliance within the Financial Policy and Regulatory Affairs division of the American Bankers Association. —This is low-tech crime, and a lot of fraud prevention in this area is focused on training frontline tellers to ask questions. ... When human interaction is involved, the human analysis is your best line of defense.||

[Read More.](#)

French trial for 8 suspects in terror finance ring

January 3, Associated Press

Eight men went on trial on January 3 in Paris for their alleged roles in an armed gang accused of using explosives and the threat of violence to finance Islamic terror operations. Prosecutors say the gang set up a restaurant and a cybercafe to try and hide their criminal activities — an —elaborate strategy to promote and finance the cause|| of terror, the indictment alleges. The trial, set to continue until January 28, takes place five years after the suspects' arrest in an anti-terror sweep. It is common in France for investigators to work on cases for years before they go to trial. Some of the suspects have acknowledged being members of a criminal gang, but all have denied that their goal was to finance terrorism, Le Figaro newspaper reported. [Read More.](#)

Kansas man pleads guilty to role in embezzlement by bank president

January 3, LoanSafe.org

A Jefferson County man has pleaded guilty to helping the former president of a bank in Meriden, Kansas, steal from the bank, a U.S. Attorney said January 3. The man pleaded guilty in U.S. District Court in Kansas City, Kansas, January 3 to one count of aiding and abetting theft by a bank officer. In his plea, the man admitted that in 2001 and 2002 he helped the former Meriden State Bank president embezzle bank funds. During that time, the former bank president convinced the bank's board to construct a branch on Fairlawn Street in Topeka, Kansas. The two men concealed from the board the fact the former bank president would be serving as the undisclosed general contractor on the project.

[REad More.](#)

Top 9 security threats of 2011

January 3, BankInfoSecurity.com

Mobile banking and social networks are expected to pose new security threats in the payments space in 2011. But security experts said those threats would not displace the Zeus botnet, malware attacks, and phishing threats, which for years have plagued banking institutions. Fraud attempts will escalate, not diminish, as new threats and channels blossom in 2011. As 2010 came to a close, Information Security Media Group caught up with a handful of leading industry experts to get their takes on the top security threats of 2011.

[Read More.](#)

FBI: Organized retail crime costs U.S. \$30B a year

January 3, SecurityInfoWatch.com

According to an article published the week of January 3 by the FBI, organized retail crime, which includes merchandise theft, as well as credit card fraud, gift card fraud, and price tag switching, costs the United States about \$30 billion per year. The agency said the stores targeted by perpetrators of

organized retail crime range from small specialty shops to major department stores. The groups responsible for these crimes include South American theft groups, Mexican criminal groups, as well as Cuban criminal groups from South Florida, and Asian street gangs from California.

[Read More.](#)

Insider probe nets new arrest

December 30, New York Post

The U.S. Attorney for the Southern District of New York arrested a sixth person on charges of leaking secrets as part of his widespread crackdown on insider trading. The attorney first broke open the gang of trading cheats involving hedge funds, bankers, and consultants a year ago, snaring several executives and traders. On December 29, he arrested a Silicon Valley, California businesswoman accused of peddling technology company secrets to the highest bidders among portfolio managers going back to 2006.

[Read More.](#)

Domain name of Russia's largest online payment processor hijacked

December 30, Softpedia

Fraudsters have managed to hijack the domain name of ChronoPay, Russia's biggest online payment processor, and point it to a fake version of the site in order to steal credit card details. An analyst reports chronopay.com directed visitors to the phishing page for several hours during the night between December 25 and December 26. Criminals managed to steal credit card data from 800 customers during that period and then posted a message in the company's name saying the entire database of transactions from 2009 and 2010 was compromised.

[Read MOre.](#)

Major cyber fraud syndicate dismantled in Asia

December 30, Softpedia

Authorities in the Philippines and China have arrested more than 100 members of a crime syndicate involved in a variety of telecommunications, bank, and credit card scams. A total of 24 men were arrested December 28 during simultaneous raids coordinated by Philippines' National Bureau of Investigation (NBI) at six locations in Manila. One suspect resisted arrest and attacked an NBI agent with a knife. He was shot in the stomach and was taken to the hospital. The Philippine Star reports that, at first, authorities did not even know the nationalities of the suspects. Interrogators eventually got them to write down their names in Chinese characters, and the Chinese embassy sent a representative to help establish identities.

[Read More.](#)

State and Local News

Woman FBI calls the 'church lady bandit' indicted in 12 robberies

January 6, Columbus Dispatch – (Ohio)

The first bank robbery now attributed to the "church lady bandit" occurred January 10, 2006 — right around the time, auditor's records show, the suspect lost her Northeast Side house in Columbus, Ohio in foreclosure. Three more robberies linked to the bandit occurred in October 2008, the same month the suspect embezzled \$2,500 from her employer using a company credit card, according to court records.

[Read More.](#)

Police officers charged in armored car caper

January 6, Associated Press; Texarkana Gazette – (Arkansas)

Three Arkansas police officers have been charged with conspiracy to rob an armored car in Little Rock, and one of their two alleged accomplices was indicted for stealing \$400,000 from an armored car driver in 2007, according to an indictment released January 5.

[Read More.](#)

FBI investigating possible bank robbery ring

January 6, WFXT 25 Boston – (Massachusetts)

One bank robbery January 5 in Burlington, Massachusetts could turn out to be a hit by a major organized crime crew. The FBI violent crimes task force has been chasing a group of organized bank robbers for nearly a month now. Since December 15, they have hit banks in Lynnfield, Reading, Malden, Westford, Salem, Westford, and, most recently, Burlington. At first authorities thought they were dealing with a single bank robber, but now they believe this is a bank robbery ring — one that is considered armed and dangerous.

[Read MOre.](#)

Neenah police search for bank robbery suspect

January 6, WLUK 11 Green Bay – (Wisconsin)

A bomb threat, turned bank robbery had a Neenah, Wisconsin, grocery store evacuated for nearly 4 hours January 5. It began around 5:30 p.m. at the Pick 'n Save on Fox Point Plaza. Authorities said a man wearing a black hooded sweatshirt pulled a package he claimed was a bomb from a grocery bag. He then demanded money from the Associated Bank inside the store. The Brown County Bomb Squad determined the package was harmless, but police said the robbery caused quite a scare. "We treated it as carefully as we could.

[Read More.](#)

Fake-bomb bandit believed to be serial robber

January 5, Orange County Register – (California)

A man who used a fake bomb to rob a Bank of America January 4 in Orange, California is believed to be a serial robber who has hit banks in Los Angeles County, officials said. At about 2:45 p.m., a man wearing a baseball cap sat down with an employee and opened what looked to be a day planner, authorities said. Inside was a device that looked like a bomb, complete with cylinder-shaped objects that resembled flares, wiring, and electronic components. A man law-enforcement officials have dubbed the "Scanner Bandit" is believed to be responsible for four robberies, including the January 4 heist. The serial bank robber is known for using devices that look like bombs. The object in the January 4 heist was determined to have been a fake bomb, and FBI officials said the robbery closely resembled similar incidents in banks in Torrance, Whittier, and Norwalk.

[Read MOre.](#)

'Fedora robber' in custody, tied to holdups in Hackensack, Fairview, Guttenberg

January 4, Cliffview Pilot – (New Jersey)

Union City, New Jersey police tracked a bank robbery suspect after he tried to hold up a TD Bank branch off 43rd Street less than 2 hours after making off with \$1,000 from the Guttenberg Savings and Loan off 68th Street on December 14, investigators said. Both branches are on Bergenline Avenue. "Our investigation revealed he was also responsible for" robbing the Valley National Bank in Hackensack on September 9 and the Oritani Bank on Fairview Avenue on December 4, an agent told the Cliffview Pilot.

[REad More.](#)

Thieves come up with new, easier way to steal credit card data

January 3, KY 3 Springfield – (Missouri)

City police say they have learned criminals can swipe information on a credit card account without ever touching or even seeing the card. The police chief call it electronic pickpocketing. By getting within two or three feet of a purse or wallet, thieves can use a credit card reading device to steal personal bank information. It is a device that any thief can buy on the Internet. Credit card companies tout the new payWave or pay pass systems as the latest and greatest way to get in and out quickly. You can charge something to your credit card without ever swiping it by just holding it near a pay-out machine.

[Read More.](#)

Minivan is tool, getaway vehicle in WA ATM theft

January 3, Associated Press – (Washington)

Vancouver, Washington police said a minivan driver used his vehicle as both a tool and a getaway car in the theft of an automatic teller machine from a bowling alley January 3. The Columbian reports a man drove a minivan through the glass doors of Allen's Crosley Lanes at about 3 a.m. and crashed into the ATM. Surveillance footage of the robbery shows a person then jumping out of the van, grabbing the ATM, hoisting it into the vehicle and driving off.

[Read More.](#)

Four suspected in nine bank robberies

December 30, Longmont Times – (Colorado)

FBI investigators suspect that four people arrested December 28 on suspicion of robbing a Broomfield, Colorado bank are also responsible for up to eight other bank robberies, including one earlier during the evening of December 28 in Lafayette, Colorado. An FBI spokesman said Broomfield police arrested four suspects — two men and two women — after the TCF Bank in Broomfield at 4100 West 144th Ave. was robbed at 6:40 p.m.

[Read More.](#)

ABA Fraud/Scam Report is a service of the American Bankers Association. ABA Members: To unsubscribe and to manage your subscriptions, please visit [ABA E-mail Bulletins](#) and check or uncheck the appropriate boxes. For other inquiries, please contact ABA's [Rachael Davis](#) at 1-800-BANKERS.

American Bankers Association, 1120 Conn. Ave. NW, Washington, DC 20036