

## IN THE NEWS

VOLUME 2 ISSUE 7

FEBRUARY 15, 2009

### IT Security

Hackers are continuing to find ways to steal identities. For example, the Federal Aviation Administration (FAA), part of the Department of Transportation made the headlines. Hackers broke into the FAA computer system and accessed the names and Social Security numbers of 45,000 employees and retirees [1]. This breach comes at a time when President Obama ordered a cybersecurity review [2]. The FAA is another casualty of increased identity theft. For example, in 2008, the number of identity theft victims increased from 8.1 million in 2007 to 9.9 million [3]. However, the cost per victim fell 31% to \$496 per victim [4]. In other Government news, the GAO reports that TSA security inspectors could not explain 49% of their work [5].

In Russia, an antivirus security firm fell victim to an SQL injection attack [6]. The security lab, Kaspersky, claims no data was stolen and hired a third party to review the incident [7]. The security company launched an upgraded U.S. tech support site and reverted to the old site following the breach [8]. In another incident, the antivirus company F-Secure also appears to have been victimized by

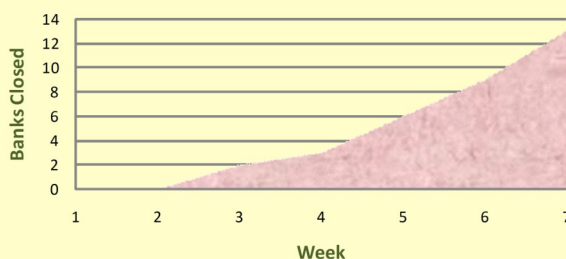
(Continued on page 2)

DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION  
ORVILLE WRIGHT BUILDING

#### Inside this issue:

Electronic Medical Records	3
Space Debris	3
Asian News	4
Crime Report	4

Bank Closings as of 2/15/2009



The number of cases the SEC brought against Ponzi schemes increased from 15 in 2007 to 23 last year [1]. What's more, following congressional complaints over the handling of the Madoff case, the SEC enforcement chief Linda Chatman Thomsen announced she will be leaving [2]. In other news, the Sherman County Bank in Nebraska became the 10<sup>th</sup> bank shuttered by regulators this year [3]. The 11<sup>th</sup> bank closed was the Riverside Bank of the Gulf Coast in Florida

[4]. The 12<sup>th</sup> bank closed was the Corn Belt Bank and Trust Company in Illinois [5]. Finally, the 13<sup>th</sup> bank shuttered was the Pinnacle Bank in Oregon [6].

In an interview on C-SPAN, Rep. Paul Kanjorski of Pennsylvania stated there was electronic run on the banks last September. He claims that in a 1–2 hour period, \$550 billion was withdrawn from money market accounts [7]. Some are now questioning what happened. We point out the following, the

### Economic News

catalyst occurred the Monday before when the 4<sup>th</sup> largest investment bank Lehman Brothers declared bankruptcy [8]. This set the stage for a bailout (that later became known as TARP) [9]. Last October we cited references to the silent bank run against Wachovia were depositors holding more than \$100K pulled money out of their banks, getting their balance below \$100K [10].

Readers of the July 20th Newsletter may recall our warning that deposits above the FDIC \$100K limit were at risk. There are 2 reasons we believed this at the time. First, following the

(Continued on page 2)

#### Special points of interest:

- Federally controlled medical records part of Stimulus Bill
- Hackers break into FAA and access SSNs of 45,000 people
- Microsoft offers \$250K reward for information leading to the arrest and conviction of Conflicter Worm
- Regulators shutter 10<sup>th</sup>, 11<sup>th</sup>, 12<sup>th</sup>, & 13<sup>th</sup> banks

## IT Security

(Continued from page 1)

the same type of SQL injection attack [9]. F-Secure personnel said the problem with its site was due to a bug in a Web application [10].

Last Tuesday, Microsoft delivered a patch to correct eight vulnerabilities [11]. Microsoft is also offering a \$250,000 for information leading to the arrest and conviction of the creators of the Conficker Worm [12].

1. Lowy, Joan, AP, *FAA says Hackers broke into agency computers*, February 10, 2009.
2. Bain, Ben, GCN, *Obama orders cybersecurity review*, February 11, 2009.
3. Stemple, Jonathan, Reuters, *US '08 identity*

*fraud up in total dollars, victims*, February 9, 2009.

4. Choi, Candice, AP, *Survey: Identity theft up, but costs fall sharply*, February 9, 2009.
5. Chunovic, Louis, *Government Security News, TSA can't document how security inspectors spent nearly half their time in 2007, says GAO*, February 6, 2009.
6. Keizer, Gregg, *Computer World, Antivirus firm confirms hackers breached site*, February 9, 2009.
7. Prince, Brian, *eWeek, Kaspersky Lab Pours Cold Water on Claims of Data Breach By Hacker*, February 9, 2009.
8. King, Steven, *USA Today, Hacker cracks Kaspersky Security site*, February 9, 2009.
9. Leyden, John, *The Register, Serial security hackers hit F-secure*, February 13, 2009.
10. Mills, Elinor, *Cnet news, F-Secure provides details on Web site breach*, February 12, 2009.
11. Kaplan, Dan, *SC Magazine, Patch Tuesday: Microsoft fixes "critical" flaws in Exchange, IE*, February 10, 2009.
12. McMillan, IDG New Service, *Microsoft Puts \$250,000 Bounty on Conficker Worm*, February 12, 2009.

## Economic News

(Continued from page 1)

failure of IndyMac, there were reports some of the funds were not covered by the FDIC and depositors might lose these assets [11]. Second, financial people, such as Suze Orman, were pointing out FDIC insurance only covered up to \$100,000 [12]. To compound the problem, Suze was featured in an FDIC advertising campaign and is referenced on the FDIC's main Web page under Consumer Resources. If you had \$200K in deposits at a bank, and the FDIC launched a marketing campaign warning insurance was limited to \$100K; at the first sign of bank trouble, what would you do?

1. Kimelman, John, *Baron's, Staying a Step Ahead of Stock Swindler*, February 9, 2009.
2. Moyer, Liz, *Forbes, Mad-off Claims Another Victim*,

February 9, 2009.

3. FDIC Press Release, *Heritage Bank, Wood River, Nebraska, Assumes All the Deposits of Sherman County Bank, Loup City, Nebraska*, February 13, 2009.
  4. FDIC Press Release, *TIB Bank, Naples, Florida, Assumes All of the Deposits of Riverside Bank of the Gulf Coast, Cape Coral, Florida*, February 13, 2009.
  5. FDIC Press Release, *The Carlinville National Bank, Carlinville, Illinois, Assumes All of the Deposits of Corn Belt Bank and Trust Company, Pittsfield, Illinois*, February 13, 2009.
  6. FDIC Press Release, *Washington Trust Bank, Spokane, Washington, Acquires All of the Deposits of Pinnacle Bank, Beaverton, Oregon*, February 13,
- 2009
7. Krawczeniuk, Borys, *Scranton Times, Kanjorski: Economy teetered near collapse*, February 13, 2009.
  8. Solomon, Deborah, *Wall Street Journal, Shock Forced Paulson's Hand*, September 21, 2008.
  9. Oneal, Michael, *Chicago Tribune, Bailout: 'Whatever it takes'*, September 20, 2008.
  10. Rothacker, Rick, *McClatchy Newspapers, Wachovia experienced \$5 billion run on deposits*, October 10, 2008.
  11. Savage, Terry, *The Street, IndyMac Lesson: Check for FDIC Insurance*, July 12, 2008.
  12. Orman, Suze, *CNBC, What You Need to Know About FDIC Insurance*, July 17, 2008.

---

*Well done is better than well said—Benjamin Franklin*

---

## Electronic Medical Records

Now that the American Recovery and Reinvestment Act of 2009 (stimulus bill) has cleared congress; it's an appropriate time to explore some of the Information Technology descriptions. For example, the bill calls for the creation of the National Coordinator of Health Information Technology and a Government system to control all medical records [1]. The Office of the National Coordinator for Health Information Technology (ONCHIT) will be part of HHS. One challenge for the organization will be ensuring record privacy. Under the new stimulus bill,

individuals must be notified when protected health information (PHI) is compromised. With the multiplicity of application vulnerabilities, privacy breaches should be anticipated. For example, in the FAA privacy breach, Personally Identifiable Information (PII) for 45,000 people was placed at risk [2].

It may be helpful to have a template for alerting victims such as the following example. In 2005 following its data breach, the FDIC sent letters to people potentially impacted [2]. After contacting the FDIC, we learned that the leaked information was from a

computer printout containing PII for all 2002 employees. Furthermore, as a remedy, the FDIC offered 2 years free credit monitoring.

1. McCaughey, Betsy, Bloomberg, *Ruin Your Health With the Obama Stimulus Plan: Betsy McCaughey*, February 9, 2009.
2. Mosquera, Mary, FCW, *FAA suffers massive data breach; more than 45,000 affected*, February 10, 2009.
3. [www.femto-second.com/papers/NewsLetters/FDIC-Data-Breach.pdf](http://www.femto-second.com/papers/NewsLetters/FDIC-Data-Breach.pdf)

## Space Debris

Last week, a Russian Cosmos communications satellite collided with a U.S. Iridium satellite resulting in a debris field of 500 pieces [1]. The collision took place 485 miles above the Russian Arctic [2]. The Russian satellite was nonfunctional whereas the U.S. spacecraft was part of an operational 66 constellation providing global telephone communications [3].

What is interesting is the Iridium satellite could have adjusted its orbit [4]. Unfortunately, there is no FAA equivalent for commercial satellites so there was no warning [5]. It is estimated that within a month, the debris field should stabilize and a better risk picture emerge [6]. For decades, other spacecraft will need to avoid the debris from last week's collision [7]. What's more, the debris could remain in orbit for 10,000 years [8].

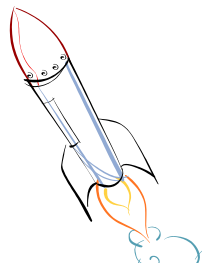
As military and commercial reliance on space continues, the consequences of debris could be far reaching. When

China shot down a weather satellite, it created a debris field [9]. Now countries such as Iran are developing space capable rockets [10]. Consider the reliance on GPS satellites that currently operate at approximately 10,000 miles above the surface. Should these be destroyed in a space war, the debris would remain a threat for many generations.

1. Sunseri, Gina, and Martinez, Luis, ABC News, *An Unprecedented Space Collision*, February 12, 2009.
2. Baker, Luke, Reuters, *Satellite crash poses new political risk*, February 12, 2009.
3. Broad, William J., New York Times, *Debris Spews Into Space After Satellites Collide*, February 11, 2009.
4. Birch, Douglas and Isachenkov, Vladimir, AP, *Crash of US, Russian satellites a threat in space*, February 12,

2009.

5. Koltz, Irene, Discovery, *Crash highlights lack of space traffic control*, February 12, 2009.
6. Morris, Jefferson, *Aviation week, Debris From Collision Should Stabilize Soon*, February 12, 2009.
7. Wolf, Jim, Reuters, *U.S. warns of space "dodgeball" after satellite crash*, February 12, 2009.
8. Isachenkov, Vladimir, AP, *Space crash debris to orbit Earth for 10,000 years*, February 13, 2009.
9. BBC News, *China confirms satellite downed*, January 23, 2007.
10. Brinton, Turner, Space News, *Iran's Satellite Launch a Signal of Missile Progress, Analysts Say*, February 12, 2009.



---

*Men have become the tools of  
their tools—Henry David  
Thoreau*

---

## Asian News

In Beijing, a 44-story, 520-foot building was completely destroyed by fire [1]. It appears the fire was caused by illegal fireworks [2]. In other news, the monthly U.S. trade deficit increased 1.9% to \$12.3 billion in China's favor [3]. Furthermore, China has indicated that for now it will continue to purchase U.S. Bonds [4]. The company at the heart of the tainted milk scandal, the Sanlu Group is bankrupt and the Chinese product safety regulators are checking a unit of the French Danone group to see if it also used the toxic chemical melamine [5]. Moreover, Congressman Bernie Thompson blamed China as the source

for cyber attacks against the U.S. government, electric-utility, and financial computer networks [6].

In Pakistan, the government there has acknowledged that parts of the terrorist attack on Mumbai were planned domestically [7]. What's more, India is urging more action be taken by Pakistan indicating the situation is still volatile [8].

1. Fong, Mei, and Dean, Jason, wall street Journal, *Beijing Hotel Tower Is Destroyed by Fire*, February 10, 2009.
2. BBC News, *Arrests follow China tower fire*, February 12, 2009.
3. McDonald, Joe, AP,

*China's January exports plunge 17.5 percent*, February 11, 2009.

4. Sender, Henny, Financial Times, *China to stick with US bonds*, February 11, 2009.
5. BBC News, *China milk scandal firm bankrupt*, February 12, 2009.
6. Bliss, Jeff, Bloomberg, *Chinese Hackers Attack U.S. Computers*, Thompson Says, February 12, 2009.
7. Masood, Salman, New York Times, *Pakistan Announces Arrests for Mumbai Attacks*, February 12, 2009.
8. BBC News, *India urges more action on Mumbai*, February 13, 2009.

## Crime Report

---

*The infectiousness of crime is like that of the plague—*  
*Napoleon Bonaparte*

---

The increase in the number of fraud cases is straining the FBI [1]. For example, in Colorado, a man was indicted on charges of wire fraud and money laundering relating to a multi-million dollar loan scheme [2]. One suspect in a \$100 million mortgage fraud was caught at the Canadian border carrying \$1 million in Swiss bank certificates, \$70,000 in cash, and four ounces of platinum [3]. In Florida, a man accused of an \$83 million bank fraud scheme was arrested [4]. In Kentucky, two men were sentenced in a \$4.5 million bank fraud scheme [5]. In Pennsylvania, a Canadian national was indicted by a grand jury for operating an international stock fraud ring that resulted in losses of \$26 million [6].

Nigerian scams continue to find fresh victims. For example, Utah lost \$2.5 million from its treasury to a Nigerian web scam fraud [7]. The state

thought it was paying money to the University of Utah's design and construction department but was instead scammed [8].

1. Bloomberg News, *Rise in fraud cases is 'straining' FBI*, February 12, 2009.
2. FBI, *David Gwin indicted for multi-million loan scheme*, February 11, 2009.
3. Thompson, Don, AP, *Calif. fraud suspect caught with \$70,000 in boots*, February 11, 2009.
4. Bradenton Herald, *Bank fraud mastermind arrested*, February 10, 2009.
5. WZTV, *Tenn. men sentenced in western Ky. fraud scheme*, February 12, 2009.
6. FBI, *Canadian Charged in Multi-Million Dollar International Stock Fraud Ring*, February 12, 2009.
7. Carlisle, Nate, Salt Lake

*Tribune, Nigerian web scam bilked Utah out of \$2.5M*, February 12, 2009.

8. Adams, Andrew, KSL, *Thieves steal \$2.5 million from state funds*, February 12, 2009.

