Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 13

June 22, 2008

Is the Worse Yet to Come?

Since the first newsletter, we have presented reports of continued weaknesses in the financial institution industry. We also asked how much loss can be attributed to weak security controls. Now the Government Accountability Office (GAO) recommends Federal Reserve banks fix identified information security control weaknesses [1]. In describing one weakness, the GAO reports: "The *general information security control deficiencies that "we identified relate to logical access controls. Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges.*"[2] That passwords are still used in an area cited for a security weakness suggests legacy applications are not being upgraded to address current threats. Recall from last week's newsletter the problem in DC relying on a software application to enforce security culminated in a $50 million (and growing) fraud. Perhaps a more strategic approach looking beyond passwords and at technology such as cryptographically strong smart cards should be considered. Increases to legacy application risk should be offset with improved security controls.

> *We recommend that the Director of the Division of Reserve Bank Operations and Payment Systems direct the appropriate FRB officials to implement the 14 detailed recommendations set forth in the separately issued Limited Official Use Only version of this report.* [2]

To see how well the Federal Reserve Bank information technology systems are protected, it is worth looking at past GAO reports to gain insight. In 2006, the GAO completed a review of the Treasury auction system and found a number of weaknesses including weak identification & authentication (I&A) and weak encryption [3]. When the Federal Reserve Banks implement poor security controls what should we expect from the smaller financial institutions? Why is it that only auditors find severe security weaknesses? Might this be an indicator of a lack of strategic planning? Again, as we observe the current *Subprime* meltdown in the financial industry, we need to ponder if security was adequate, would there still be crisis?

> The FRBs did not adequately identify and authenticate users. For example, due to the weak design of password reset functionality for one of the distributed-based auction applications, anyone on the Internet could potentially change the password for a user in the application by having only his or her userID. Recognizing the severity of this vulnerability, the FRBs took steps to immediately correct this weakness. [3]

(Continued on page 2)

Fake Goods

In Newsletter 7, we explored knock-off Cisco routers that found their way into Government networks. The problem goes beyond Cisco equipment. For example, estimates are that intellectual theft costs the US $200 billion and 750,000 jobs per year [1].

In Myrtle Beach, police raided a store and found nearly $350,000 in counterfeit hand bags, sun glasses, clothing, and other goods [2].

Fake goods also include drugs and food. For example, in Canada, police and customs agencies are warning of fake drugs manufactured in India and China [3]. In the US, Spammers are making money selling on-line fake drugs [4]. Finally, the Food and Drug Administration has warned 23 US and 2 foreign companies to stop claiming

(Continued on page 2)

Inside this issue:

Special points of interest:

- GAO finds security weaknesses at Federal Reserve Banks
- Malware nearly ruins a life
- The FDIC ordered Fremont General Corporation to stop making subprime loans in March 2007
- Fremont General Corporation files for Chapter 11 bankruptcy protection

Is the Worse Yet to Come?

(Continued from page 1)

Usually, banks downplay any potential risks so that customers don't panic. However, the Royal Bank of Scotland is advising clients to brace for a crash of stock and credit markets over the next three months [4]. This at a time when one report suggests the loss to financial institutions will be $1.3 trillion [5].

1. Mosquera, Mary, FCW, *GAO: Banks need stricter access controls*, June 18, 2008.
2. Government Accountability Office, GAO-08-836R, *Information Security Controls at FRBs*, June 16, 2008.
3. Government Accountability Office, GAO-06-659, *Federal Reserve Needs to Address Treasury Auction Systems*, August, 2006.
4. Evans-Pritchard, Ambrose, The Telegraph (UK), *RBS issues global stock and credit crash alert*, June 18, 2008.
5. Cahill, Tom, and Trowbridge, Poppy, Bloomberg, *Paulson & Co. Says Writedowns May Reach $1.3 Trillion*, June 18, 2008.

Marriner S. Eccles Building

Mortgage Fraud

Sometimes we stare so long at a door that is closing that we see too late the one that is open.– Alexander Graham Bell

Being more reactive than proactive, it usually takes a significant loss before any action is taken. The subprime crisis provides a good case in point. Since March 1, the FBI has arrested over 300 people in mortgage fraud amounting to $1 billion [1]. In California, a loan broker and employee of Washington Mutual were charged in connection with a multimillion dollar mortgage fraud ring [2]. In Maryland, 8 people were charged with conspiracy, mail fraud and money laundering in a $35 million scam [3]. The Maryland case is being called the biggest mortgage fraud case in the state and at least 100 former homeowners lost their homes [4]. One report indicates the FBI is shifting its focus in 26 offices from financial crimes to mortgage fraud [5].

Finally, in New Jersey, mortgage brokers were charged in a racketeering scheme involving $5 million in fraudulent mortgages [6].

1. CNN Money, *Mortgage fraud inquiry nets hundreds*, June 19, 2008.
2. Warren, George, News 10 (Sacramento), *Broker, Bank Employee Charged in Valley Mortgage Fraud*, June 16, 2008.
3. Associated Press/Carroll Country Times, *$35M mortgage fraud uncovered: Eight people indicted on alleged foreclosure rescue scheme*, June 16, 2008.
4. Collins, David, WBAL (Baltimore), *Group's Mortgage Fraud Scheme Duped 100*, Feds Say, June 13, 2008.
5. Chandler, Susan, Chicago Tribune, *FBI shifting focus to mortgage fraud at two dozen offices*, June 15, 2008.
6. Gold, Jeffrey, associated Press, *NJ charges fraud in $5 million worth of mortgages*, June 17, 2008

Fake Goods

(Continued from page 1)

their products prevent or cure cancer [5].

1. Coolidge, Georgina, Reuters, *Counterfeit, pirated goods costing U.S. billions*, June 17, 2008.
2. Baker, Molly, WBTW News, *Police arrest several for $344,000 in counterfeit goods*, June 17, 2008.
3. Hogben, David, Vancouver Sun, *Fake erectile dysfunction drugs flooding Vancouver*, June 17, 2008.
4. Menn, Joseph, *Los Angeles Times, Spammers are making real money on fake drugs*, June 11, 2008.
5. Nizza, Mike, The New York Times, *F.D.A. Takes Aim at Herbal Cancer 'Cures'*, June 18, 2008.

Police Impersonators

When determining the identity of a person, how do we know that person is who they claim to be? When a bad actor can masquerade as a police officer, do we need better credentials?

In west Virginia, police arrested a person charged with impersonating a police officer [1]. In Honolulu, a police imposter robbed 4 teens at gun-point [2]. In Mississippi, a police imposter dressed in uniform, ridding a car with a blue lights, pulled over a woman [3]. In Virginia, a man impersonating a police officer was caught [4]. In Florida, a police impersonator was sentenced to 60 days in jail [5]. In Tennessee, a woman was pulled over by a police imposter and asked to pay a fine of $250 for speeding [6]. In Nevada, a man who got out of a traffic accident by claiming to be a military police officer about to be deployed was sentenced to five years probation [7]. In Staten Island, a man pretending to be a DEA agent and robbing drug dealers was sentenced to 11 years in state prison [8]. In Arkansas, travelers were robbed of nearly $1,000 in their motel by a person impersonating a sheriff's officer [9]. In Birmingham, Alabama, a man was charged with impersonating an off-duty police officer, kidnapping, and raping a woman [10]. In North Carolina, an armed robber may have used fake police identification [11].

In New York, a man pleaded guilty to criminal impersonation of a police officer, aggravated cruelty to animals, first-degree coercion, third-degree criminal sexual act, unlawful imprisonment and two counts of grand larceny [12]. This imposter operated in Long Island from 2004 until his arrest in February 2007 and he even operated a fake police station [13].

1. WVVA, *Police impersonator is caught*, June 17, 2008.
2. KITV, *Police Impersonator Robs Kailua Teens*, June 16, 2008.
3. Wright, Ryan, The Mississippi Press, *Woman stopped by police impersonator in Pascagoula*, June 12, 2008.
4. Chesterfield Observer, *Police impersonator caught*, June 11, 2008.
5. Alund, Natalie Neysa, Bradenton Herald, *Reported police impersonator sentenced*, May 30, 2008.
6. Welsch, Anthony, WBIR, *Oak Ridge investigates "police impostor"*, June 12, 2008.
7. Rogers, Keith, Las Vegas Review-Journal, *Military police impostor gets probation*, May 26, 2008.
8. Staten Island Advance, *Fake cop who went on crime spree sentenced*, June 12, 2008.
9. Smith, Alan, Times Herald, *Fake cop robs travelers at motel*, June 9, 2008.
10. WSFA, *Fake-Cop Accused of Kidnapping/Rape*, June 17, 2008.
11. Lytlle, Steve, The Charlotte Observer, *Fake police ID used in robbery*, June 4, 2008.
12. Perez, Luis, newsday.com, *Cop impersonator cops plea, faces long jail term*, May 31, 2008.
13. CBS/AP, *Fake L.I. Cop Faces 54 New Charges*, June 4, 2007.

If a problem cannot be solved, enlarge it.–Dwight D. Eisenhower

Can Malware Ruin you Life?

Sometimes victims pay for crimes they did not commit. Years ago, some bad actors would create a bogus presidential death threat email and send it to the white House. Immediately, the Secret Service would initiate an interview of the alleged sender. The then new technology of email was used to basically ruin another person's life. Unless that person could prove he or she did not send the email (very difficult back then) the allegation was likely to follow the person throughout their life. We also see from phishing attacks, how seductively real email messages can be made to appear.

In Massachusetts, a former state employee was wrongly accused of downloading child pornography on his laptop computer [1]. Experts examined his laptop and determined the cause to be malware [2]. The state employee was fired before experts determined that malware was surreptitiously visiting illegal Web sites [3]. The investigation began when Verizon reported the employee's phone bill was four times higher than it should have been [4].

1. ABC News, *A Misconfigured Laptop, a Wrecked Life*, June 18, 2008.
2. USA Today, *Mass. state worker cleared of child-porn charges; Experts blame malware*, June 18, 2008.
3. Mills, Elinor, cnet Blog, *State worker cleared on child porn charges that were due to malware*, June 17, 2008.
4. Thomson, Lain, VNU net, *Man cleared as child porn possession blamed on virus*, June 19, 2008.

Students Change Grades

In California, two teenagers with uninspiring grades broke into the school computer and changed their grades to a higher standing [1]. The 2,800 student high school regularly makes the Newsweek list of best American high schools [2]. Given that intellectually challenged students were able to hack the school system; what does this say about the state of school security?

Changing grades are not the only malicious act students do. Case in point, in Pennsylvania, a 9th grade student hacked into a school computer and copied social security numbers for 9,000 students and 41,000 residents [3].

1. McMillan, Robert, IDG News Service, *Teens Charged With Loading Spyware, Changing Grades*, June 18, 2008.
2. Novack, Al, WKYN, *Police: 15-Year-Old Hacked Downingtown School District Computer System*, May 22, 2008.
3. Mehta, Seema, and Rosenblatt, Susannah, Los Angeles Times, *Teens face felony charges of computer break-ins, grade changes at Tesoro High School*, June 18, 2008.

Financial News

In a sign of the times, Fremont General Corp, with stock selling for $12 per share last year, filed for bankruptcy [1]. Fremont was one of the largest subprime mortgage lenders [2]. The FDIC and California Department of Financial Institutions approved the sale of the banking unit, with $5.6 billion in deposits, to Maryland's CapitalSource Inc. [3] The Fremont General Corporation was ordered by the FDIC to stop making subprime loans in March 2007 [4]. So if the regulators knew subprime lending was risky, why was it allowed to flourish for so long?

As if this is not bad enough, consider the email exchanged by two former Bear Stearns hedge fund managers indicted for fraud. It seems they sent incriminating information using email [5]. So not only was the information vulnerable to hackers but they now face 20 year imprisonment if convicted.

Intellectual property has the shelf life of a banana.– Bill Gates

1. Associated Press, *Fremont General files for bankruptcy protection*, June 19, 2008.
2. Reuters, *Fremont General seeks bankruptcy protection*, June 18, 2008.
3. Beighley, Dan, Orange County Business Journal, *Fremont Gets Bank Sale OK; Holding Company Files for Bankruptcy*, June 18, 2008.
4. Charlotte Business Journal/bizjournals, *Fremont declares bankruptcy as part of CapitalSource deal*, June 19, 2008.
5. Larson, Erik, and Kolker. Carlyn, Bloomberg, *Bear Stearns Defendants Showed Disregard for E-Mail Risks*, June 21, 2008.

Financial Malfeasance

There was a time when Swiss Banks were know for confidentiality. However, now a former banker for the Swiss bank, UBS, has agreed to tell all regarding the internal culture of the Swiss bank [1]. The former UBS banker pleaded guilty to helping a wealthy real estate developer evade taxes on $200 million [2]. There are estimates that UBS may have helped 20,000 wealthy Americans evade taxes by managing $20 billion in accounts held offshore [3].

1. Jagger, Suzy, The Times (UK), *Former banker vows to reveal all as American officials ask whether UBS aided tax tricks*, June 20, 2008.
2. Browining, Lynnley, New York Times, *Former UBS Banker Pleads Guilty to Aiding Tax Evasion*, June 19, 2008.
3. Brown, Tom, Reuters, *Ex-UBS banker pleads guilty to U.S. tax evasion scheme*, June 19, 2008.