

IN THE NEWS

VOLUME 1 ISSUE 23

AUGUST 31, 2008

FDIC News

In this newsletter, we explore some of the news surrounding the FDIC. First, Forbes listed the FDIC Chairman, Sheila C. Bair, as the second most powerful woman in the world [1]. This as banks reported their lowest earning since 1991 [2]. The ninth FDIC-insured bank failure this year, the Columbian Bank and Trust, was acquired by Citizens Bank and Trust [3]. The tenth bank to fail this year, the Integrity Bank of Alpharetta, Georgia had \$1.1 billion in assets [4]. What is interesting is Georgia law limits the amount of credit secured by real estate that a bank can lend one borrower to 25% of available capital [5]. One report suggests the Georgia bank had loans of \$83 million to entities owned by the same guarantor; that amount represented almost all of the bank's available capital early last year [6].

Mortgage failures are contributing to the financial stress on banks. Many mortgages were predicated on the belief that property prices would continue their upward direction indefinitely. However, in the latest 20 city survey, prices have consistently fallen for three months and prices on average are 15.9% lower than this time last year [7]. The strain on banks and thrifts can best be summarized by the number of troubled institutions on the FDIC's watch list. The number increase from 90 to 117 banks and thrifts during one quarter [8]. More significant, the troubled bank assets increased from \$26.3 billion to \$ 78.3 billion [9]. To put this in proper perspective, while the number of banks increased by 30% the bank assets increased nearly 200%. This means larger banks are joining the watch list. Moreover, originally the FDIC had estimated the Indy-Mac failure would cost the Insurance fund \$4–8 billion. This has been revised upwards to \$8.9 billion [10]. For the Integrity Bank, the estimated cost to the insurance fund is estimated between \$250 million and \$350 million [11]. When calculating actual losses, one needs to consider what assets will actually bring. For example, the FDIC is auctioning 80 properties in the Detroit area [12]. As the property values decrease, the funds recovered by the FDIC may be less than expected.

In a sign of things to come, the FDIC may have to borrow money from the Treasury to cover short term losses [13]. The FDIC can borrow \$40 billion from the Federal Finance-

(Continued on page 2)



Inside this issue:

Does Crime Pay?	3
Malicious Software	3
Fraud	3
China	4
Identity Theft	4

Special points of interest:

- FDIC may need to borrow money from Treasury
- Computer virus infects space station laptops
- Forbes lists FDIC Chairman, Sheila Bair, as second most powerful woman in the world
- Integrity Bank 10th bank closed

Hackers

In a recent hacker attack, the open source Linux vendor, Red Hat, was victimized when hackers accessed servers [1]. Researchers have found 75% of web sites have vulnerabilities [2]. At the same time, other researchers are observing how cyber-attacks propagate

through the Internet [3]. Before the onslaught of financial institutions, one of the more visible hacker targets was the department of Defense (DoD). Some estimate the cost in responding to hacker attacks on the unclassified DoD networks is \$100 million

per year [4].

With the global Internet, attacks can be launched from virtually any location. When a hacker is located in another country, trying to bring them to justice can be challenging. Consider the case of a Scottish hacker that admits to breaking

(Continued on page 2)

FDIC News

(Continued from page 1)

ing Bank and another \$30 billion from the Treasury Department if necessary [14]. This as the Deposit Insurance Fund fell from \$52.8 to \$45.2 billion in three months [15]. Some have argued that the watch list is not a good indicator. Case in point, the May watch list did not include IndyMac as its assets were greater than the 90 bank combined list of \$26.3 [16]. Given that IndyMac was not on the list, we can infer that the rumor of collapse was the most likely reason for the collapse. We are at a point when malicious rumors can quickly result in healthy financial institutions failing. Moreover, consider the speed of the collapse. Without adequate safeguards what is to prevent future fear induced failures?

1. Egan, Mary Ellen, and Schoenberger, Chana R., Forbes, *The World's 100 Most Powerful Women*, August 27, 2008.

2. Vekshin, Alison, Bloomberg, *U.S. Bank Earnings Plunge to Second-Lowest Level Since 1991*, August 26, 2008.
3. AP, *Closed Kansas bank agrees with Fed on capital plan*, August 25, 2008.
4. Vekshin, Alison, Bloomberg, *Integrity Bank Becomes 10th U.S. Failure This Year*, August 29, 2008.
5. Wei, Lingling, The Wall Street Journal, *Georgia Bank Bet Big on One Horse*, August 29, 2008.
6. Fitzpatrick, Dan, The Wall Street Journal, *Regulators Shut Integrity Bancshares In 10th U.S. Bank Failure This Year*, August 30, 2008.
7. AP, *S&P: Home prices tumble by record amount*, August 26, 2008.
8. Gordon, Marcy, AP, *FDIC: 117 troubled banks, highest level since 2003*, August 26, 2008.
9. Gutierrez, Carl, Forbes, *FDIC Under Pressure*, August 27, 2008.
10. Wutkowski, Karey, Reuters, *FDIC says IndyMac failure costlier than expected*, August 26, 2008.
11. Reuters, *Georgia bank becomes 10th U.S. failed bank-FDIC*, August 29, 2008.
12. Marker Watch, *More Than 80 Detroit Area Properties to Be Offered at FDIC Auction*, August 25, 2008.
13. Reuters, *FDIC may borrow money from Treasury: report*, August 27, 2008.
14. Reuters, *FDIC says has options if bank failures soar*, August 27, 2008.
15. Luhby, Tami, CNN Money, *FDIC to boost insurance fund*, August 26, 2008.
16. Ellis, David, CNN Money, *What the FDIC problem list isn't telling us*, August 28, 2008.

If you owe the bank \$100 that's your problem. If you owe the bank \$100 million, that's the bank's problem—J. Paul Getty

Hackers

(Continued from page 1)

into 97 U.S. military and NASA computers [5]. Before the suspect could be tried in the U.S., the extradition had to be approved by European courts [6]. The hacker in question was first indicted back in 2002 for offenses committed in 2001 and was eventually arrested in 2005 [7]. Six years after identifying the hacker, justice has yet to be served. So how would we respond to a state sponsored attack say from China, Russia, or Iran? As long as there are safe ha-

vens for hackers, legal enforcement will be challenging at best.

1. Haskins, Walaika, Linux Insider, *Hackers Get Under Red Hat's Skin*, August 25, 2008.
2. Hart, Kim, The Washington Post, *A New Breed Of Hackers Tracks Online Acts of War*, August 27, 2008.
3. Jackson, William, GCN, *Studies find Web sites rife with unpatched vulnerabilities*, August 28, 2008.
4. Kash, Wyatt, GCN, *Cyber chief argues for new approaches*, August 22, 2008.
5. UPI, *Scottish hacker may be extradited to U.S.*, August 28, 2008.
6. Sayer, Peter, PC World, *European Court Won't Stop UK Hacker's Extradition to US*, August 28, 2008.
7. McKinnon, Gary, Info World, *European court won't stop U.K. hacker's extradition to U.S.*, August 28, 2008.

Does Crime Pay?

Different crimes result in different punishment. Consider the case where three people are charged with defrauding and escrow fun of nearly \$13 million [1]. Each of the 21 counts could result in a maximum \$250,000 fine for each and 20 years jail time at most. Actual sentencing will most likely be far less. The fines could reach \$5,250,000 resulting in a difference of \$6,750,000. A potential criminal might work the math and conclude it's worth the risk. Consider the example of a mortgage broker in Maryland sentenced to 97 months in prison for fraud losses estimated at \$650,000 [2]. With a Web based activity over a three year period of time, the broker was able to amass a small nest egg.

Now consider the bank robber. This person is most likely to get caught and penalties are steep. For example, a man was sentenced to 58 months in prison for three bank robberies that netted \$1,010, \$4,010, and \$1,515 for a total of \$6,535 [3]. For the crime of bank robbery, it would seem that crime does not pay.

In Kansas City, a man involved in a \$16 million mortgage fraud received a sentence of 5 year in prison and a \$2,500 fine [4]. Another aspect to consider is that not all prisons are equal.

1. FBI, *Three men indicted in construction escrow fraud scheme*, August 26, 2008.
2. FBI, *Mortgage broker sentenced to more than eight years in prison for fraud*,

money laundering, and obstructing justice, August 26, 2008.

3. FBI, *Man sentenced for robbing banks in Arden Hills, Blaine*, August 27, 2008.
4. Kansas City Business Journal, *Lenexa man gets five years in mortgage-fraud scheme*, August 29, 2008.



California Bank Robber—FBI

Malicious Software

Password grabbing viruses are no longer confined to Earth. Reports indicate two laptops aboard the space station were infected [1]. Perhaps The space station laptops are the exception; most password grabbing programs target on-line games [2].

As if the problems in space were not bad enough, the high bandwidth terrestrial

networks may be at risk. An exploit to the high end routing, the Border Gateway Protocol (BGP) was demonstrated that the Hacker DefCon conference [3]. Perhaps this is one reason OMB is mandating the use of Domain Name Service security [4].

1. Moore, Matthew, The Telegraph (UK), *Computer virus infects International Space Station laptops*,

August 26, 2008.

2. Greenberg, Andy, Forbes, *Cybercrime Gets Its Game On*, August 29, 2008.
3. Zetter, Kim, Wired, *Revealed: The Internet's Biggest Security Hole*, August 26, 2008.
4. Krebs, Brian, The Washington Post, *White House Imposes New Security Mandate for Federal Agencies*, August 27, 2008.

Fraud

Most of the reports on fraud listed are limited to the high dollar well publicized incidents. We expect that the total cost of fraud is much higher. With that, two people pleaded guilty to their part in defrauding Medicare out of \$37 million [1]. The article also indicates others were involved in a \$ 110 mil-

lion HIV infusion fraud and money laundering scheme.

With the downturn in housing, there are more reports of fraud. Compare the second quarters, for last and this year; even though the number of loans has decreased by 30%, the reports of fraud increased by 42% [2].

1. FBI, *Miami physician and HIV clinic administrator plead guilty for their roles in a \$37 million medicare fraud scheme*, August 26, 2008.
2. Hamey, Kenneth R., The Washington Post, *Fewer Loans, But Still More Fraud*, August 30, 2008.

It is well that the people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning—Henry Ford

China

As the geopolitical landscape changes, it is worth looking at the emerging Asian giant, China. In both wealth and technology, China is advancing rapidly. In technology, China is the third country to launch people into space using its own rocket. They also have plans to develop a homegrown petaflop computer in 2010 [1]. Readers may recognize that a petaflop is a million billion calculations (quadrillion) per second. Coincidentally, such a machine calculates each instruction in one femtosecond.

As the U.S. dollar falls, the number of imports American can afford should fall. However, one report indicates China is quietly purchasing dollars thereby keeping their exports strong [2].

While US Banks struggle to remain profitable, the Bank of China, smallest of China's big 4, reported a profit of \$6.17 billion for the first 6 months [3]. The second largest Chinese bank, China Construction, reports half year earnings

of \$8.6 billion [4].

There is still unrest within China. Recall that during the Olympics, 16 police were killed in Western China [5]. Last week, in Xinjiang 10 bombers hit 17 sites resulting in 2 policemen killed [6].

In past newsletters, we have discussed the trade deficit in some detail. The first Asian giant to successfully transfer much of the US wealth was Japan. They are currently the second largest economy in the world [7]. So how does Japan maintain its wealth? Consider that in 2006, in response to another rising Asian country, Korea, a 27.2 % tariff was applied to DRAM memory chips [8]. Additionally, Japan will tariff electrolytic manganese dioxide imported from Australia, China, South Africa and Spain for five years from September 1 to "safeguard domestic makers from cheap imports" [9]. Is there a lesson we can learn from Japan?

1. Niccolai, James, *China aims for petaflop computer in 2010*, August 27, 2008.

2. Telegraph (UK), *Beijing swells dollar reserves through stealth*, August 26, 2008.
3. Or, Amy, *The Wall Street Journal*, *Bank of China's Net Climbs 43%*, August 18, 2008.
4. Chen, Eadie, and Bi, Victoria, *Reuters*, *China Construction Bank eyes faster loan growth*, August 25, 2008.
5. BBC, *Two police die in Xinjiang clash*, August 28, 2008.
6. Ang, Audra, AP, *2 Chinese policemen killed, 7 injured in Xinjiang*, August 28, 2008.
7. Kageyama, Yuri, AP, *Japan unveils \$18 billion stimulus package*, August 29, 2008.
8. Shimbun, Yomiuri, AP, *Tariffs on ROK computer chips to be eased*, August 23, 2008.
9. TMC Net, *Japan to keep retaliatory tariffs over U.S. antidumping law*, August 22, 2008.

*It is better to be alone
than in bad company—
George Washington*

There are estimates that in the United States 220 million private records were lost or stolen since 2005 [1]. The largest data breach so far in 2008 was the NY Mellon bank, now estimated to impact 12.5 million people [2]. We have been conditioned to expect terrible news. Case in point, there was report that indicated an Indian hacker compromised Best Western customers. The hotel chain has disputed the number of identities compromised claim-

Identity Theft

ing only 13 people were involved [3]. This was in response to articles indicating every visitor since 2007, approximately 8 million, were compromised [4]. What we can infer is there was a data breach and the number of identities stolen is not known but small compared to original reports.

1. Greengard, Samuel, *Communications of the ACM*, *Privacy Matters*, August 8, 2008.
2. Stempel, Jonathan,

Reuters, *Bank of NY Mellon data breach now affects 12.5 mln*, August 28, 2008.

3. Claburn, Thomas, *Information Week*, *8 Million-Record Data Breach Claim 'Grossly Unsubstantiated,' Says Best Western*, August 25, 2008.
4. Lonescu, Daniel, *PC World*, *Hackers Rob Best Western Hotel Group, Steal 8M Guest Records*, August 25, 2008.