Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 17

July 20, 2008

The Cost of Rumors

We have seen Bear sterns and IndyMac fail following rumors spread that the institutions were on the verge of collapse. Now new rumors are circulating about the health of Freddie Mac, Fannie Mae, and Lehman Brothers [1]. As part of an ongoing investigation, the Security and Exchange Commission (SEC) is looking at the intentional rumors manipulating the markets [2]. Perhaps the biggest concern is that rumors are responsible for the feared "run on a bank," when depositors withdraw their money and the bank collapses. The latest run on banks (Bear Sterns and IndyMac) present challenges to the Treasury [3]. In response, the SEC has come out and warned Walls Street to stop spreading false rumors [4].

Throughout the FDIC are pictures on the walls depicting the long lines of depositors withdrawing funds. The main reason for the FDIC is to provide the depositor confidence that their funds will be safe and thereby prevent the run on the bank. Leading up to the IndyMac collapse, there was a run on the bank with $1.3 billion in deposits withdrawn during 11 business days [5]. This followed the leak of a letter from the Senator Charles Schumer, New York, to the OTS indicating IndyMac was at risk for failure [6]. After receiving considerable negative press, Senator Schumer has placed the blame on the Office of Thrift Supervision for "sleeping at the switch" [7]. A question here is could a Senator's letter spark a run on the bank? Senator Charles Schumer is the chairman for the subcommittee on Housing, Transportation, and Community Development [8]. The follow-on question remains were the regulator's actually asleep at the switch as senator Schumer suggests? This example highlights the risk of rumor in starting a panic. It also highlights the need for regulators to ensure strong confidentiality controls in protecting information that could inadvertently foster a run on a bank.

One of the concerns raised by Senator Schumer in his letter to the OTS was the regulators were not prepared to prevent a collapse of IndyMac or deal with the aftermath should a collapse occur [9]. Readers may recall in the first Newsletter, we questioned if the FDIC's insurance fund is adequate for the losses anticipated. It is estimated that IndyMac alone could absorb up to 15% of the insurance fund [10]. Already there is at least one politician calling for additional funding of the FDIC [11]. The story of IndyMac is not quite over. Since the FDIC has taken over, customers are still withdrawing their funds [12]. A question here is will depositors in other banks,

(Continued on page 2)

Financial News

The Treasury and Fed continue working on a plan to help Fannie Mae and Freddie Mac [1]. As mentioned in the last newsletter, the Fed is adopting a plan to curb shady mortgages in an effort to protect consumers [2]. On the plus side, oil had its largest one week decline in history [3]. If the price continues to fall, this will hopefully mitigate inflation. Citigroup reported a quarterly loss of $2.5 billion; however this was less than anticipated [4]. Shares of Citigroup stock rose 7.7% on Friday based on the better than expected news.

Financial fraud is still in the news. For example, in Florida, 2 advisors were sentenced in a $194 million hedge fund collapse [5].

1. Aversa, Jeannine, AP, *US spells out Fannie-Freddie backstop plan*, July 14,

(Continued on page 2)

Inside this issue:

Special points of interest:

- New Zealand judge spares criminal conviction for $20 million loss hacker
- FBI Bank Crime Statistics—In 2007 $24 million in loot taken

The Cost of Rumors

(Continued from page 1)

with over $100,000 deposited, start withdrawing their money thereby causing more runs on banks? Perhaps it is time for the FDIC to increase the insurance coverage and reduce the angst.

1. Younglai, Rachelle, Reuters, *SEC says expanding rumor crackdown*, July 13, 2008.
2. Aversa, Jeannnine, AP, *SEC opens probe to prevent spread of false info*, July 13, 2008.
3. Petruno, Tom, The Sydney Morning Herald, *Run on banks spells big trouble for US Treasury*, July 14, 2008.
4. Scheer, David, Bloomberg, *SEC to Probe Manipulation Through False Information*, July 13, 2008.
5. Keating, Gina, Reuters, *IndyMac depositors line up for cash after seizure*, July 14, 2008.
6. The Wall Street Journal, *The $4 Billion Senator*, July 15, 2008.
7. Reuters, *Sen. Schumer blames OTS for IndyMac's failure*, July 12, 2008.
8. banking.senate.gov/public/index.cfm?FuseAction=Information.Subcommittees
9. Rugaber, Christopher S., AP, *IndyMac reassures customers after Schumer letter*, July 1, 2008.
10. The Wall Street Journal, *Next Taxpayer Bill: FDIC?*, July 16, 2008.
11. Business Courier of Cincinnati, *Congressional candidate urges FDIC funding*, July 16, 2008.
12. Lazarus, David, Los Angeles Times, *Banks responsible for the loss of trust*, July 20, 2008.

Identity Theft

Rumor grows as it goes–Virgil

Identity theft continues to be a problem perpetrated by bad actors ranging from organized crime syndicates to lone rogues. In Philadelphia, a 22-year old woman admitted to stealing more than $116,000 in goods and services [1]. In Texas, Radio Shack and Select Medical agreed to pay the state $1.5 million for violating laws designed to curb identity theft [2]. In Texas settlement, there is no claim that information was leaked, only that the protection processes were inadequate. So when calculating the cost of identity theft, there may be expenses in complying with new statues. In Illinois, two men are alleged to have used fake documents to defraud 4 banks out of $120,000 [3].

It is worth looking at successful solutions to identity theft. Overseas, Barclays claims to have reduced on-line fraud to zero using multi-factor authentication smart cards with PINs [3]. The Barclays example provides a valuable lesson.

1. Dale, Maryclaire, AP, *Student grifter admits $116K fraud in Pa. ID theft*, July 14, 2008.
2. McGraw, Dan X., The Dallas Morning News, *RadioShack and Select Medical pay $1.5 million to settle ID theft claims*, July 16, 2008.
3. Chicago Tribune, *2 men accused of defrauding 4 Des Plaines banks*, July 17, 2008.
4. Broersma, Matthew, ZDNet UK, *Barclays claims card-reader has eliminated fraud*, July 18, 2008.

Financial News

(Continued from page 1)

2008.
2. Aversa, Jeannine, AP, *Fed adopts plan to curb shady mortgage practices*, July 14, 2008.
3. Schreck, Adam, AP, *Oil prices tumble in biggest weekly drop ever*, July 19, 2008.
4. Read, Madlen, AP, *Citigroup posts $2.5B loss, but beats expectations*, July 18, 2008.
5. Department of Justice, *Hedge Fund Advisors Sentenced in $194 Million Hedge Fund Collapse*, July 17, 2008.

Fraud

A woman was indicted in a scheme to defraud clients of 1031 Tax Group LLP (1031TG) out of $130 million [1]. In Las Vegas, 5 more pleaded guilty to a mortgage scheme that cost federally insured banks $18 million [2]. The now defunct IndyMac bank is being investigated by the FBI for possible fraud [3]. It was reported that the FBI currently has 21 investigations related to the subprime market industry [4]. At the same time, the Securities and Exchange Commission has more than 4 dozen ongoing subprime investigations [5].

1. Department of Justice, *Virginia Woman Indicted In $132 Million Scheme to Defraud Clients Of Funds Allegedly Held In Trust*, July 11, 2008.
2. Department of Justice, *Five Defendants Enter Guilty Pleas in Las Vegas Mortgage Fraud Scheme*, July 11, 2008.
3. Jordan, Lara Jakes, AP, *FBI looking into IndyMac Bancorp*, July 16, 2008.
4. Reuters, *FBI probing IndyMac for possible fraud - report*, July 16, 2008.
5. Reuters, *US SEC: more than 4 dozen subprime cases underway*, July 15, 2008.

Bank Crime Statistics

The FBI has released the Bank Crime Statistics for 2007. The total money taken for all physical bank crimes was $24 million and over $11 million was recovered. Contrast this with the $18 million mortgage fraud scam in Utah [1]. Or the $20 million mortgage fraud case in New York [2]. Or the $76 million Medicare fraud case where dead doctor's names were used to order wheel chairs [3]. Clearly the big risk to financial institutions comes not from an armed robber but rather some computer based attack.

If we look at the FBI provided information, there were 1609 robberies, burglaries and larcenies reported for 2007. This is approximately $15,000 per incident. Contrast this with the average identity theft criminal where each victim's loss is estimated by the Federal Trade Commission at $1882 [4]. An armed robber stands a good chance of getting caught and some chance getting shot. In contrast, online crime stands less chance of conviction and little chance of getting shot.

1. Fattah, Geoffrey, Deseret News, *6 in mortgage fraud file to block evidence*, July 14, 2008.
2. Schram, Jamie, New York Post, *$20M Mortgage Crook in 'DWI'*, July 16, 2008.
3. Starkm, Lisa, Barrett, Kate, ABC News, *Scam Artists Use Dead Doctors' IDs to Abuse Medicare*, July 8, 2008.
4. Federal Trade Commision—2006 Identity Theft Survey Report, November 2007.

The easiest way to keep a secret is without help—Unknown

FBI 2007 Bank Crime Statistics

Type	Robberies	Burglaries	Larcenies
Commercial Banks	1393	32	4
Mutual Savings Banks	21	1	0
Savings and Loan Associations	23	0	0
Credit Unions	124	10	1
Total	1561	43	5

Violations by Type of Institution

Cash	$23,127,885.47
Securities—Face Value	0.00
Checks (including Traveler's Checks)	1,403,018.77
Food Stamps	0.00
Other Property	7,624.00
Total	$24,538,528.24

Loot Taken

Cash	$10,350,660.92
Securities—Face Value	0.00
Checks (including Traveler's Checks)	1,400,160.00
Food Stamps	0.00
Other Property	20.00
Total	$11,750,840.92

Loot Recovered

Bribery

We have all read stories about kickbacks with Government contracts. A former CEO of a security guard company paid a former GSA employee over $100,000 in bribes [1]. The former Federal employee pleaded guilty to bribery and tax evasion [2].

In exchange for the bribes, the former employee helped secure Government contracts valued at $130 million [3]. In Texas, a former Customs and Border Protection (CBP) officer pleaded guilty pleaded guilty to conspiring to fraudulently produce official travel documents in exchange for cash [4].

Bribery is not confined to the Federal level but also hits the states. In Florida, 5 correctional guards were charged with allowing drugs to flow into the prison in exchange for cash [5]. Consider the case in South Carolina, where the former mayor and zoning commissioner of a small town, Union, were indicted of accepting $30,000 in kickbacks [6]. In Tennessee, a former state senator was convicted of taking more than $800,000 from government contractors [7].

1. Department of Justice, *Former CEO Sentenced In Bribery Scheme Involving $130 Million In Federal Contracts*, July 14, 2008.
2. Lee, Henry K., San Francisco Chronicle, *Guilty plea in federal contract bribery case*, July 18, 2008.
3. Washington Times, *Ex-officer sentenced for contract bribery*, July 15, 2008.
4. Department of Justice, *Former CPB Officer and another Laredo Man Plead Guilty to Travel Permit Scheme*, July 15, 2008.
5. Department of Justice, Five State Correctional Guards Charged Federally for Smuggling Drugs into Correctional Institution, July 18, 2008.
6. WYFF, *Mayor Resigns Hours Before Indictment*, July 17, 2008.
7. AP, *Ford Convicted on Corruption Charges*, July 19, 2008.

Give me control of a nation's money and I care not who makes it's laws.- Mayer Amschel Bauer Rothschild

Computer Crime

A disgruntled city computer engineer, using a privileged password he created commandeered San Francisco's new multimillion-dollar Fiber WAN network [1]. City officials are estimating that the loss could be in the $ millions [2]. The alleged disgruntled employee has pleaded not guilty to the charges [3]. The alleged hacker's lawyer claims his client is willing to cooperate in releasing the password to the locked system which stores 60% of all city government data, including e-mails, law enforcement records, and payroll documents [4].

A hacker ran up 30 hour phone call to India costing the Massachusetts town of Duxbury's library $7,000 [5]. One would think that with the destination number, this crime might be solvable.

Overseas, in Romania arrested 19 people were arrested for a number of cyber-crime activities that cost US victims at least $635,000 [6]. In New Zealand a notorious hacker will not be going to jail [7]. The admitted hacker developed a bank hacking application that stole money from bank accounts resulting in the collective loss of over $20 million [8]. It was reported that the hacker received one job offer from the police [9]. When criminals benefit from their actions, it sends the wrong message to others considering the same line of work. In this case, reliance on other country laws was ineffective. Van Derbeken, Jaxon, San Francisco Chronicle, *S.F. officials locked out of computer network*, July 15, 2008.

1. Gonsalves, Antone, Information Week, *Jailed City Worker Allegedly Hijacks San Francisco's Computer System*, July 15, 2008.
2. AP, *S.F. engineer pleads not guilty to cyber crime*, July 17, 2008.
3. Gonsalves, Antone, Information Week, *Suspect In Hijacking Of San Francisco Computer Network 'Willing To Cooperate'*, July 18, 2008.
4. AP, *Hacker runs up big phone bill for library*, July 18, 2008.
5. Kirk, Jeremy, IDG News Service, *Losses Likely to Rise From Latest Romanian Crime Ring*, July 17, 2008.
6. The Wall street Journal, *Police Arrest, Try to Hire Computer Hacker*, July 18, 2008.
7. McNevin, Ambrose, Computing (UK), *Bank hacking software developer walks free*, July 16, 2008.
8. New Zealand Herald, *Conviction would harm hacker's future - judge*, July 15, 2008.