IDENTITY THEFT: THE NEWEST DIGITAL ATTACK

Karen A. Forcht, North Carolina A & T State University, kaforcht@ncat.edu
Eric Kieschnick, Texas A & M University-Kingsville, eak2278@hotmail.com
Daphyne S. Thomas, James Madison University, thomasds@jmu.edu
Jack D. Shorter, Texas A & M University-Kingsville, jackshorter@hotmail.com

ABSTRACT

This paper discusses the definition of identify theft and the ramifications for the banking industry. In today's environment of on-line banking and e-commerce, ID theft has become a serious problem. Not only can banks lose the confidence and goodwill of their customers, but legal sanctions/actions can result from the bank's not protecting the consumer. While banks focus on protecting the consumer's information, it is imperative that customers follow the correct procedures and take precautionary measures to protect their information and transactions.

Keywords: Identity theft, Identity Theft and Assumption Deterrence Act, credit reports, National Credit Union Administration, incident response, identity fraud, phishing.

INTRODUCTION

Identify theft has become the newest digital attack. Of all the required assets for a successful bank, only one is not mandated by law: a bank's good name in the community. Once a bank's reputation is tarnished, either fairly or unfairly, customers will not be likely to entrust their money to an institution seen as less than "rock solid". In the growing world of e-banking, a bank or financial institution could potentially bear the brunt of an online scam. And while banks focus on protecting consumer's information from that fraud, how do they know that their efforts are being acknowledged.

DEFINITION OF IDENTIFY THEFT

Identify theft is a term that can have several meanings and different interpretations. The Fair Credit Reporting Act defines identity theft as "the use of or attempted use of an account or identification without the owner's permission." [10] The 1998 Identity Theft and Assumption Deterrence Act also describes identity theft as "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." [10]

According to a new consumer awareness survey conducted by SunTrust Bank, Inc., more than 85 per cent of Americans are concerned about the threat of identity theft, yet less than half believe they are taking the right steps to protect their identity and their credit health. The survey also revealed that 42 per cent of consumers are extremely concerned about identity theft, and close to 40 per cent know someone who has been affected by the crime. Gene Kirby, SunTrust Corporate Executive Vice President and Head of Retail Banking stated, "Industry reports suggest that identity theft costs Americans more than $5 billion annually, claiming a new victim every 70 second." [8]. According to the same article, since 2001, an estimated 27 million Americans have had their identity and credit history stolen, but only 52 per cent of consumers say they have taken steps to do something to protect themselves and their ability to take out loans and obtain personal credit. When compared with the 32 per cent of consumers who identified specific ways they have modified their financial transactions, a large number of Americans are still at risk [8]. All these numbers point to the fact that identity theft is on the increase. Yet, not everyone knows exactly how to combat the problem or who should be responsible for stopping this threat.

Identity Theft Prevention

Simple steps to reduce vulnerability to identify theft (SCAM) can include:

1. Users should be stingy about revealing personal information to others unless they have a reason to trust them. Adopt a need-to-know basis for revealing personal data. Keep information printed on personal bank checks to a minimum. If someone contacts you via telephone or the Internet and offers a prize but asks for personal data, ask them to mail a form, and check the company with the Better Business Bureau. When traveling, have mail held at the local post

office or have a trusted person collect the mail. Be careful when throwing out documents that contain personal information.

2. Check financial information often for irregular activity and review statements for any changes or transactions that should not be there. Statements from banks and credit card accounts should arrive monthly.

3. Request a copy of an updated credit report periodically and review it to confirm that no unknown accounts have been opened.

4. Maintain careful records. Keep monthly statements and cancelled checks or their copies for at least a year. These can be useful if you need to dispute them. [10]

Identify Theft Recovery

If the consumer thinks that they have become a victim of identify theft or fraud, immediate action should be taken by:

1. Contacting one of the three major credit bureaus (Experience, Equifax, or Transunion) to have them place a fraud alert in your file. This will require that creditors contact you before opening new accounts in your name or changing information on existing accounts. Once the alert is activated, the other two credit bureaus will be notified.

2. Get a copy of your credit report and review it. Close any accounts that have been tampered with or opened fraudulently. Speak with someone in the fraud/security department of each creditor, and follow up in writing, with copies of supporting documents. Victims of identity theft have the right to request that those debts incurred through fraud are blocked from future credit reports.

3. Report the crime to local police or police in the community where the theft took place. Report the theft to the Federal Trade Commission.

4. Obtain copies of fraudulent credit and account applications from the three major credit bureaus and give copies to the police.

5. Contact the Social Security Administration if you suspect your social security number is being used. [10]

PREVENTION AND MITIGATION

Financial institutions' consumer education and employee training are tools that can be used to fight e-mail frauds. The National Credit Union Administration sent a letter to Federally Insured Credit Unions in December, 2005. In the letter, it described phishing as "a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords, account, credit card details, etc. by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message." [6] The forms often include messages that warn of a potential problem to a specific account and require a click on a link that goes to a fraudulent website where the consumer is asked to give personal information. These particular e-mails even go as far as putting specific logos in the "from" line to make them seem legitimate. But in the end, all the information that is submitted will make its way to a perpetrator who will either use the personal information illegally or sell it to somebody who will. The National Credit Union Administration article lists several ways to help prevent and mitigate the problem:

1. Implement a policy that your financial institution will not solicit confidential information or sensitive materials via e-mail and inform customers of the policy on a periodic basis.

2. Provide a notice to customers describing your security policies and practices including the role the customer can play in protecting his or her own information.

3. Adopt a policy to personalize e-mails to customers using their names in the message and inform customers of the policy.

4. Keep informed of advances in technology designed to protect customer information and reduce e-mail fraud and take advantage of those that are effective and practical for your financial institution.

5. Train security and service staff regarding your policies and procedures for protecting customer information, including those concerning phishing and other forms of e-mail fraud so they are sensitive to customer comments. [6]

Incident Response

If a bank or other financial institution should become aware of actual phishing incidents using their names or logos as an attempt to solicit information from their customers, the bank should take action by following these procedures:

1. Post an alert notice on their website's homepage.

2. Monitor customer accounts for unusual activity and trends.

3. Flag and monitor closely the accounts of customers who report that they have been a victim of a phishing scam.

4. Alert their staff to the incident so that they are sensitive to the situation and report activity such as unusual address change requests, account transactions, or new account activity.

5. Encourage customers who believe that they have been a victim of a phishing scam to report it to authorities. [6]

Information Protection Lacking

Banks and other financial institutions spend large amounts of money on a daily, weekly, monthly and yearly basis trying to protect their customer's personal information from criminals. Even though these institutions commit funding to this effort, the protection of personal information is not a top priority. Banks, just like all other financial institutions, are in the business of making money. They intend to do what they can to satisfy the customer, but in the end, it all comes down to profits. Safeguarding private information and all security measures are costs to businesses that cut away profits and are sometimes sacrificed in order to please owners or shareholders. According to an article on Ezinearticle.com "even if security were a high priority for banks, security spending could go on forever. In such situations, accepting risk overrides spending. Business managers decide between protecting personal information and producing profits."[10] Security is an issue, but accepting a certain amount of risk is warranted in their eyes to obtain the profit level that is deemed to be satisfactory.

Banks and their leaders aren't the only ones to blame. The consumer has some responsibility concerning the problem of identity theft. The majority of the time it appears that consumers choose less security. Consumers are not willing to pay the extra price for security. Most believe it is worth the risk in order to save a dollar, and the same goes for convenience. Bank customers want things now or want their transaction to happen faster and easier and are not concerned with the risks that go along with that convenience. According to that same Enzinearticles.com journal "businesses won't put in security measures to inconvenience customers unless its competitors do, or everyone's forced to do." [10] When security is present in banks, it is only to manage losses and is not there to protect consumers. In the end, it is always about profits, and managing losses increases the bottom line.

The major crux of this situation is that no one wants to pay for security. Banks don't want to incur the costs to protect their customers, while consumers are not willing to spend the extra money to protect their interests. Everyone wants the benefits of security to stop identity theft, but no one wants to pay the costs or bear the inconvenience that goes with increased security for privacy. "Just as shoplifting is built into the cost of retail merchandise, banks recoup their losses through higher customer services fees and interest rates." [11]

Stealing Information Is Easy

Think about all the junk mail that a consumer receives in their mailbox on a daily basis. Think about how quickly it is tossed in the trash. The majority of that junk mail has personal information in it that can be used to steal a person's identity. Buying a shredder is becoming a good way to protect personal information, including bank statements that have account numbers and, in some cases, social security numbers. Individuals should consider using a shredder for their sensitive information, such as bank statements, credit card statements, pre-approved credit card offers, telephone calling cards, tax information, pay stubs and credit card carbons. If the theft occurs from a person's mailbox, it becomes a federal offense and the Federal Government can get involved. Some useful guidelines to remember are:

1. Individuals should also deposit mail in post office collection boxes, not their own mailbox.

2. Individuals should quickly remove mail from their mailbox after delivery and request that mail be held when they are gone. [2]

Fraudulently Obtained Credit Reports

An individual's credit report obtains a handful of information that identity thieves would love to get their hands on. As identity theft becomes more of a problem, credit report agencies have fortunately taken more steps to protect personal information that is given to businesses and are more careful about the types of businesses that can get such information. The best way to combat this is to monitor credit reports on a frequent basis and notify the credit reporting agencies when anything is suspicious or criminal on an account. "A suspicious inquiry is one that is not the result of you applying for credit." [2] It could be someone else applying for credit using your name or a business checking on a consumer credit report for no reason. [2]

Theft and Others

One of the more logical ways to get your personal information, yet a sometimes overlooked way, is by simple theft. Although it is still upsetting and inconvenient when it happens, when someone is robbed, they at least know that their information has been taken and can take steps to prevent the assailant from doing any severe damage to their bank accounts or financials. They can call and cancel credit cards or checks and even catch criminals who try to use their personal information by placing an alert with the credit reporting agencies. Sometimes a problem can be dishonest employees or co-workers who give out information or sometimes can carelessly give it out through email or instant messaging.

It is hard to protect your information at all times. It is so easy to let information slip through the cracks and go to someone who is dishonest. But the more a person practices good habits with their personal information, the easier it becomes to protect it. [2]

An article on prenewswire.com offers information and some insights into the problems banks and other financial institutions face. "While financial institutions see the value in and continue to move towards implementation of security solutions aimed at prevention and detection of identify fraud, many still primarily emphasize after-the-fact resolution of identify fraud". [8] The research done by Javelin in the newswire article, "found that more focus on the prevention and detection of identity fraud will likely result in fewer losses and greater efficiencies" [4]

STATISTICS ON IDENTITY THEFT

Statistics on identity theft really bring the severity of the problem to the forefront and show how, unfortunately, the problem doesn't seem to be getting any better.

Survey findings include:

- The number of US adult victims of identity theft fraud decreased from 10.1 million in 2003 and 9.3 million in 2005 to 8.9 million in 2006.
- Total one year fraud amount rose from $53.2 billion in 2003 and $54.4 billion in 2005 to $56.6 billion in 2006.
- With the mean fraud amount per fraud victim rising from $5,249 in 2003 and $5,885 in 2005 to $6,383 in 2006.
- The mean resolution time is at a high of 40 hours per victim in 2006 compared to 28 hours in 2005 and 33 hours in 2003. [3]

The Unisys Corporation has conducted research that shows U.S. banks are at risk of a customer exodus as a result of growing consumer awareness of identity theft issues. The study found that nearly half of U.S. households would be willing to switch their accounts to financial institutions that offer stronger theft detection and alert services. [12]

Banks face mounting pressures not only to improve identity theft prevention, but also to help customers better understand how they can combat fraud. While trust in banks remains high (84 percent of consumers believe their banks are doing all that can be done to prevent identity theft), the Unisys research points to rising concerns. More than half of those surveyed are worried about the safety of their money. The study found that one in five U.S. households – more than 21 million – have been directly affected by identity theft. [12]

The Unisys study found that nearly two-thirds of U.S. consumers believe it is possible for banks to prevent fraud before it occurs, and more than three-quarters (78 percent) believe it is a bank's responsibility to do so. Consumers, however, are not enthusiastic about bearing the cost of identity theft protection, with only 27 percent at least somewhat willing to pay extra for these services. [12]

PREVENTIVE STEPS BY FINANCIAL INSTITUTIONS

Steps financial institutions should consider to reduce online fraud that can lead to identity theft are:

- Upgrade existing password-based single-factor customer authentication systems to two-factor authentication.

- Use scanning software to proactively identify and defend against phishing attacks. The further development and use of fraud detection software to identify account hijacking, similar to existing software that detects credit card fraud, could also help to reduce account hijacking.

- Strengthening educational programs to help consumers avoid online scams, such as phishing, that can lead to account hijacking and other forms of identity theft and take appropriate action to limit their ability.

- Place a continuing emphasis on information sharing among the financial services industry, government, and technology providers. [1]

Other banks continue to heavily promote or market identity prevention services in the form of credit report monitoring. These services, which alert customers to changes in their credit files at the three major credit bureaus discussed earlier, have been big moneymakers, with companies making millions of sales through banks. But it appears the days are numbered for such services, because consumers are realizing that credit monitoring is ineffective in preventing identity theft and because the service is being ineffective as a moneymaker as other companies offer it for free. In Scott Mitic's article in the American Banker, he states, "consumers consider banks their identity protectors". [5]

Consumers want and need banks to help protect their identities. Failure by banks to recognize this could end in enormous cost in terms of customer retention. Real identity protection lies in giving consumers control of all aspects of their financial life. The ability not just to monitor transactions, but also to control them, is essential. In the future, consumers will be able to provide or withhold authorization for anything that affects their financial identity: originating a mortgage, opening a deposit account, cashing a check, using a credit card or completing an automatic transfer of funds. This can be seen as a current trend, as states across the country begin passing credit-freeze laws. "Freezes let consumers control how the credit bureaus handle their information" [5] This control effectively eliminates the potential for a credit report to be used fraudulently to open an account. Legislators have pushed bills into Congress attempting to make credit freezes a standard, but the banking industry has been fighting these provisions due to the cost and time commitment of implementation of these procedures.

Phishing: Preventative Measures by Banks

Banks historically have tried to curb consumer fears of robberies by hiring an armed guard or police officer to patrol their lobbies. But as technology improved, the need for armed guards diminished and banks started using surveillance cameras to monitor bank lobbies and money vaults. Bankers have now learned they must guard the vaults against thieves who would hijack passwords and PIN numbers to steal money.

As a defense against phishing, these two-factor cues produce for each online banking customer a pop-up image, generally a colored square with some type of word of symbol inside the square. This visual symbol is summoned automatically before a password is entered and could not be duplicated by a phisher. [7] The thought process behind this is that the absence of a symbol would automatically suggest that something is wrong and that the Web site or e-mail is fraudulent and just trying to lure one into giving up personal information that could cost hundreds to thousands of dollars.

CONCLUSION

The ways to prevent identify theft are:

- -Protect your credit
- -Shred for safety
- -Double check credit card statements
- -Protect your mail
- -Be careful when sharing
- -Be smart about ATM's
- -Use a "real" password
- -Protect your social security number at all times
- -Keep your credit cards to a minimum
- -Secure your computer [9]

Over the past decade, identity theft has increased exponentially and that trend only seems to be getting worse as technology advances. With the advent of advanced technology comes a disadvantage of having to continuously battle the wrong doers that try to steal someone's identity in order to profit from the use of an individual's good credit history. This continuing battle will never go away. But as long as banks continue to try and fight against wrongdoers, there will always be that hope that good will prevail and online banking will one day become very safe.

REFERENCES

1. FDIC Home Page (2006, October) FDIC: Putting an end to Account-Hijacking Identity Theft. www.fdic.gov/consumers/consumer/idtheftstudy
2. How do Identity Thieves Steal your Information? Knowing how an Identity Thief can get your information is one step to prevention. http://101identitytheft.com
3. Javelin/Better Business Bureau Survey (2006, January) http://www.privacyrights.org/ar/idtheftsurveys.htm#BBB06
4. Javelin Strategy & Research Ranks Top U.S. Banks on Their Ability to Protect Consumers Against Identity Fraud. http://www.prnewswire.com/cgi-bin/stories
5. Mitic, Scott. (2006, September 8). Give Consumers More Control Over Data. American Banker, Volume 171, Issue 173, p11-11, 3/5p, 1c
6. National Credit Union Administration (2005, December). Phishing Guidance for Credit Unions and Their Members NCUA Letter to Credit Unions
7. Newman, Richard. (2006, April 6). Banking on tight online security; Business fights identity theft. The Record, Sunday edition business section, Pg. B09. or http://web.lexis-nexis.com/universe/document?_m=fdccbb4232fa29
8. Portman, Erin (2006, May 8). SunTrust Bank First to Offer Clients Free Equifax Credit Watch With Selected Checking Accounts; Consumer Awareness Campaign Turns Spotlight on Identity Theft Prevention. http://www.prnewswire.com
9. Ten Ways to Prevent Identity Theft. http://www.staples.com/sbd/ content/article/i-n/identitytheft.html?cm_mmc=sdb_cd-_-Newsletter
10. Tom, Henry (2006, October) The Inside Secret of Identity Theft and What You must do to Protect Yourself. http://ezinearticles.com/?The-Inside-Secret-Of-Identity-Theft-And-What-You-Must-Do-To-Protect-Yourself&id=297669
11. Thome, Jared and Segal, Andy. (2006, May 18). Identity theft: The new way to rob a bank. http://edition.cnn.com/2006/US/05/18/identity.theft/
12. Unisys Home Page (2005, November) Unisys Research Shows Banks Face Potential Customer Exodus Over Identity Theft. http://www.unisys.com/about_unisys.htm