https://doi.org/10.48009/2_iis_2006_38-42

DATA SECURITY—IDENTITY THEFT: BANKS AND FINANCIAL INSTITUTIONS ARE ON THE LOOKOUT

Eric Kieschnick, Texas A&M University – Kingsville, eak2278@hotmail.com
Richard A. Aukerman, Texas A&M University – Kingsville, kfraa00@tamuk.edu
Jack D. Shorter, Texas A&M University – Kingsville, jackshorter@hotmail.com

ABSTRACT

One battle that has been continuous over the last several years is the battle with Identity Theft. The purpose of this report is to examine the type of fraud that takes place in banking and other financial institutions. The report looks at ways to prevent Identity theft, legal issues involved, the effects of new technology on Identity Theft and the importance of security.

Keywords: Identity Theft, Electronic Banking, Security, On-Line Fraud

INTRODUCTION

In the age of wireless communications, sending and receiving data has never been so easy. Unfortunately, with the advantages that technology brings, disadvantages grow harder and harder to overcome. One battle that has been continuous over the last several years is the battle with Identity Theft. In a report by Janice Lieberman for Good Morning America, she reported that every 79 seconds someone becomes a victim of identity theft. Every 79 seconds! By the time a person hits the snooze button on their alarm in the morning until the time they actually get out of bed 10 minutes later, almost 8 people have become a victim of identity theft. Those numbers are startling. People today don't believe it can happen to them, but when it does, they continually wish they had taken some precautions against it. This report will look deeper into the world of Identity Theft.

IDENTITY THEFT

Phishing

After years of dramatic growth in online banking, the percentage of Americans who conduct personal banking online remained unchanged during the 12-month period ending in August 2005. There are several reasons why the growth of online banking has slowed, but a major reason is the concern about hackers stealing and using personal information. One of the ways hackers acquire this information is through a technique called phishing. Phishing, is defined on webopedia.com as "The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft" [8]. With the emergence of computers and online technology, phishing has become a very popular way for a person's identity to be stolen. In 2004, losses to banks due to phishing may have totaled as much as $367 million [8]. The cost of damage to online banking and related enterprises could have been even higher. As a result of this increased phishing epidemic, there has been a loss of trust and consumer movement away from online banking. An Internet security firm in Dallas, Entrust Inc., conducted a survey that revealed that 80% of online consumers are "specifically concerned" about someone stealing their identity and using that information to access their online bank accounts. The survey also revealed that 73% of consumers who do not currently utilize online banking services would do so if security were improved greatly. Ninety percent of consumers who already bank online would bank more often if security were improved and 22% of online customers likely would switch banks if they thought the other bank offered better security [7]. These findings just touch on the importance of consumer concerns about protecting their financial information online. These fears also impact productivity and economic growth in general. An online article by Gene Koprowski in UPI Science News states, "during the 1990s, many businesses began centering their processes on the Internet rather than the telephone." This resulted in reduced costs and huge productivity gains. Now, it seems consumers are growing increasingly hesitant to do business online and are returning to the way they used to do business. Old-fashioned check writing or personally showing up at a bank to handle a transaction is increasing in popularity again. "In the last six to nine months, consumers are increasingly voting with their keyboards and are no longer paying bills online. About 13 percent of consumers here in the United States and in Europe have stopped paying bills online" [8].

Consumers are taking matters into their own hands and are becoming proactive rather than reactive when dealing with fraudulent e-mails from suspect sources. In Koprowski's article, his research showed that slightly more than half of all consumers who receive phishing e-mails seeking to obtain sensitive information such as Social Security Numbers, date or birth or other private information delete the e-mail immediately without reading the e-mail so they will not be tempted to give out sensitive information. Consumers are also demanding better security solutions from banks, which have, for banks resulted in increasing costs and decreasing profitability, at least in the short run. "Consumers want something for security that goes beyond user name and password. They know that once someone has stolen their password, they have stolen their identity" [8].

While many people focus on the effects that phishing and other forms of identity theft have on consumers, what often gets overlooked is the effect that these problems have on financial institutions. In most cases, victims of identity theft are eventually reimbursed for any losses, while the bank has to take the hit in the form of lost revenue. And while big banks can certainly fall victim to these crooks, smaller community banks are more vulnerable to fraud losses. Karen Hoffman writes, "Things are not always what they seem. From a fraudster's point of view, a big target isn't necessarily a better target. And, a community bank may or may not recognize the criminal element in its midst." Foiled by increasingly better detection techniques at the larger banks, many crooks are said to be moving their game down to mid-size and community banks [6]. Smaller institutions are believed to be easier targets because they generally lack the resources, whether financial or in personnel, and the sophisticated fraud detection programs that larger banks can afford.

Spoofing

Spoofing is another type of Internet and e-mail fraud that many people are unaware of. Spoofing involves scamming via websites. It is also more difficult to spot because it involves using sophisticated technology to set up fake or mirror sites that pretend to be the official Website of a particular company. According to the Website, www.digi-sign.com, only trained specialists would identify that a Website is not in fact official and is being operated by fraudsters. The Website also lists signs of spotting spoof e-mails. The first sign is that they may show a sign or sense of urgency. An example would be an e-mail that stated that your account would be closed or temporarily suspended and that you'll be charged a fee if you don't respond [4]. This example seems to be very popular. Another sign is there are embedded links that look legitimate because they contain all or part of a real company's name. These links may take you to spoof sites or to pop-up windows that ask an individual to enter, confirm or update sensitive personal information. If you don't know the company or are unsure in any way, don't give out personal information without a little bit of research into the company [4]. If there's no address or phone number where someone can be reached, it's probably fake. One obvious sign that you may be on a spoof site is the appearance of obvious spelling and grammar errors. These intentional errors help spoof e-mails avoid Spam filters. The online article goes on to explain the difficulty of detecting spoof websites, "Spoof websites can be more difficult to detect because even address bars and padlocks that appear in your browser can be faked" [4]. An obvious was to combat this is to try several forms of a web address to see if any of these variations of the web address take you to the same place.

Spyware

Spyware is the latest threat to banks. According to spychecker.com, spyware is defined as "Internet jargon for Advertising Supported software**.** It is a way for shareware authors to make money from a product, other than by selling it to the users. There are several large media companies that offer to place banner ads in their products in exchange for a portion of the revenue from banner sales. This way, you don't have to pay for the software and the developers are still getting paid. If you find the banners annoying, there is usually an option to remove them, by paying the regular licensing fee." And while spyware is a great threat to banks, it is not illegal. "Still, the risk from spyware itself is significant, because 90 percent of spyware traversing the Internet is written for criminal purposes" [8]. That is why it is still a big enough threat that the FDIC recommends that banks consider threats from spyware as part of their risk-assessment process. They should bolster Internet security and enhance employee training to understand the mechanics of hackers" [8]. Although these suggestions by the FDIC are a step in the right direction, it appears some experts have a mixed reaction to these plans. In Koprowski's article, a quote from Terry Brown, chief executive officer of Caymas Systems in Petaluma, California, a network security firm, states his beliefs that the governments recommendations do not go far enough and will not alter the risks that consumers face [8]. As spyware increases in intelligence, banks and consumers alike have to begin to monitor online transactions from beginning to end and be on the lookout for suspicious activity.

Preventing ID Theft

Identity theft has plagued American consumers for many years and the threat of theft continues to grow. "ID theft and security breaches are crimes like no other, they won't completely go away," says Joseph Ansanelli, CEO of data monitoring solutions provider Vontu [3]. It began as crooks raiding trashcans or swiping wallets seeking to impersonate an individual for financial gain. Now, with the emergence of the Internet, crooks have a new focus when trying to steal someone's personal information. And the stakes have been raised with the ever-increasing dependence on electronic data. Consumers now are beginning to realize just how vulnerable their information is to theft, specifically identity theft.

One of the most overlooked ways that information can be compromised is the exposure of personal information on computers. According to Alex Berson, a director with consultancy BearingPoint, companies too often leave data exposed. He explains that information can be viewed in two ways, data in transit and data at rest. When data is in transit, it's moving over a particular network and normally is encrypted. But when data is sitting in storage, it usually is not encrypted. In a Newsweek article titled "Grand Theft Identity" by Steven Levy, examples are given as to how critical information can be lost. Citifinancial, a unit of Citigroup, packed their information in boxes and put it in a UPS truck this past May. Well, the box never made it to its destination and 3.9 million customers were told that their identities are at risk [9]. Another way critical information can be lost is with the disappearance of a laptop computers. Last March at UC Berkeley, someone made away with a computer holding personal information of almost 100,000 grad students and applicants. Laptops provide convenience, but the downside to that is that they can walk away very easily [9]. Terrifying as it may sound, an increasing problem is what insiders may do with personal information. In April, Hackensack, N.J., police arrested eight employees at Bank of America, Wachovia, PNC and Commerce banks for selling customer account numbers to an unlicensed collection agency run by a convicted criminal [9]. The operation snared data on more than 676,000 people, including customers from six additional banks. Some institutions just simply lose information. While that is unacceptable, it does happen quite often. Bank of America is still looking for backup tapes with information on 1.2 million government workers, discovered lost last December. They may be hiding in the same place as the records that Time Warner lost in March, containing 600,000 missing records in past and current employees and their families [9]. That's the major challenge for banks today, protecting the data that's at rest. But not necessarily protecting the data from theft, but protecting it from loss.

But how do banks begin to protect the data that is so critical to their existence? The first step may be to analyze the data banks need to use or share. Of the information that banks ask of customers, what is really necessary? Banks may have to have an individual's social security number on hand, but having it completely accessible to all employees is not necessary. Information that is less desirable by criminals, such as an address or phone number, may be accessible to all employees, without threat of theft. According to Carmi Levy, a senior research analyst with Info-Tech Research in Ontario, "security should not be viewed as merely a technology fix. Security should also include the people and processes associated with making data safe [3]. Some banks are attacking identity theft at the teller end. When trying to be more service oriented, tellers can easily give out information that they shouldn't. That's why Peoples Bank in Bridgeport, Connecticut "employ address verification technology to help thwart employees from giving out too much information" [3].

With the advent of outsourcing, banks need to consider extending their security perimeter to reach outside the bank. "Outsourcing inevitably increases data security risks, and the spate of recent, highly publicized breaches illustrates the importance of banks knowing who is handling their customers' data and how" [3]. According to People's Bank Jim Gerace, "banks need to use outside providers, but they must make sure the connections are secure and contractually make sure the company that's handling the data is doing its part to protect it" [3].

Importance of Security

As technology, specifically in financial institutions, continues to grow, there is an increased importance of securing sensitive information. When it comes to securing peoples' financial information, "there are no half-way measures" [5]. And while breaches in security happen at a retailer or service provider, banks often get the headlines if the breach involves financial information. According to Ms. Duke's article, an incident occurred in June (2005), where a computer hacker tried to obtain the names, banks and account numbers of as many as 40 million credit card customers. Another incident involved the Federal Deposit Insurance Corporation (FDIC). Data was lost that affected approximately 6,000 of the agency's employees. But these losses aren't necessarily fraud. Some are a result of simple neglect, while others can happen as a result of illegal acts [5]. Ms. Duke also goes on to state that the media has taken this type of information, and in her words, "ran with it." "While millions of consumers have had their information stolen, not all of the stolen information translates into thieves getting their hands on the information and using it in ways to harm customers. It doesn't happen near as many times and the press reports" [5]. Still, it appears that data loss and fraud attempts are on the rise.

While banks care about their customers and protecting their privacy, their main reason for fighting for their privacy is to keep costs down. When information is lost and the customer loses money, the bank is normally the entity that takes the financial hit. "We're standing behind our customers, notifying them when we know of a breach, opening new accounts for them as soon as possible and, above all, covering their losses" [5].

According to Ms. Duke's article, the Federal Trade Commission obtained a settlement from BJ's Wholesale Club, who was charged with failing to take adequate measures to protect its customer's online information. "For the first time, the FTC alleges that inadequate data security can be an unfair business practice" [5].

New Technology

A developing technology in the banking world is the birth of contact less payments in the form of "No-Touch" cards. This technology consists of openly transmitting consumer account data between cards and readers that process sales [2]. Requests from merchants for this contact less card technology changed plans to have the cards start in just a few markets. This mass distribution has caused some security issues. One major issue is the range of receiver on the card. "In theory, if somebody knows that you've got a contact less card in your wallet and your wallet is in your pants pocket, they can walk up behind you and create false transactions. However, since the maximum frequency distance transmission is 10 centimeters, or 2.5 inches, transmission is unlikely to occur through a wallet" say John Gould, director of the Bank Card Research service at TowerGroup [10]. Contact less technology is also protected from fraud through the use of a unique code in every transaction. "A digital signature is generated by the reader and embedded in the transaction-authorization request. The digital signal is a unique number that changes with every transaction," says Rosa Alfonso, a spokesperson for American Express.

With the addition of new technology comes security risks that are associated with the new technology. Preventing and detecting fraudulent transactions seems to be an ever-present challenge in the payment card business, but according to Patrick Gauthier, a Vice-President with Visa, contact fewer cards are well positioned to combat fraud. "Crooks are creative, so we built technology around the card to consider this fact" [10]. Chip based cards are more secure because the data on magnetic stripe cards can be copied and used to create duplicates. These cards are also designed so that only readers that recognize and authenticate the secret codes used by a particular payment scheme can extract data. Gauthier also notes that "contact less cards provide consumers with more security and control because the card does not have to be handed by the merchant [10].

Into the Future

The 2006 Identity Fraud Survey Report—released by the Council of Better Business Bureaus and Javelin Strategy & Research—provides new facts on how identity fraud occurs, counterintuitive insights that challenge conventionally accepted beliefs about these crimes, and steps consumers can take to further protect themselves against this problem [1].

The comprehensive, longitudinal survey, independently produced by Javelin Strategy & Research, is believed to be the largest ever on identity fraud, with an increased 2005 sample size of 5,000 telephone interviews with consumers. The survey was, in part, made possible by CheckFree, Visa and Wells Fargo & Company. The findings show that despite growing fears, the growth of identity fraud is contained and that data compromise through the Internet is actually less severe, less costly, and not as widespread as previously thought [1].

However, caution where Internet security is concerned is still a necessary and useful strategy. The wonderful world of technology is enhanced by the brilliant minds of Americans and others across the international banking world. But as stated earlier, those brilliant minds can also be used in criminal ways. As long as there are computer criminals, there will be noble souls who research ways to combat this illegal activity [7]. As long as individuals cherish their personal information, there will be those who try to obtain that information. One can only hope that minds that look to preserve that personal information will continue to defeat those who look to take it for their own personal gain.

REFERENCES

1. BBB OnLine. (2006). *Identity theft*. Available: www.bbbonline.org /idtheft/ index.asp
2. Brenner, R. (2005). Contact less payments: No-touch cards are in touch on security, Issuers and vendors insist transactions are safe. *Bank Technology News, 18*(8). Available: www.Keepmedia.com /pubs/BankTechnologyNews/2005/08/01/951256 ?extID=10032&oliID=213.
3. Bruno-Britz, M. (2005). Preventing identity theft: Banks, vendors and the government strategize on ways to foil ID thieves. *Bank Systems & Technology,* 9(1). Available: www.banktech.com/story/showArtilcle.jhtml?articleID=170101851
4. Digi-Sign Home Page. (2005). *Internet and Email Fraud.* Available: www.digi-sign.com/about/fraud /index.php?id=access.
5. Duke, B. (2005). Data security: Behind the headlines. *ABA Banking Journal, 97*(8). Available: www.allbusiness.com/periodicals/article/495529-1.html
6. Epper-Hoffman, K. (2005) Familiar faces or shadowy figures? *Banking Strategies, 81*(4). Available: www.bai.org/bankingstrategies/2005-jul-aug/familiar/index.asp.
7. FDIC Home Page. (2005). Latest FDIC findings on identity theft suggest need for new safeguards for internet banking. *The Monitor.* Available:www.fdic.gov/news/news/ press/2005/pr5805.html.
8. Koprowski, G. (2005) The web: Phishing rattles consumers. *UPI Science News, 7*(1), 2.
9. Levy, S., & Stone, B. (2005). Grand theft identity. *Newsweek,July.* Available: www.msnbc.msn.com/id/8359692/site/newsweek.
10. Noe, J. (2005). Contactless cards: The next big thing? *ABA Banking Journal, 97*(9). Available: www.allbusiness.com/periodicals/article/553287-1.html.