The Identity Theft Crisis Has Arrived!

Charles R. B. Stowe, Kenneth Balusek, Keith Jenkins*

Abstract

Identity theft is emerging as a major criminal activity and security headache for legitimate businesses, consumers and for financial institutions. It has reached a crisis level. The reasons for the popularity of identity theft include the following: technology has empowered individuals living far away from their victims to exploit false identities, sophisticated groups have discovered that the changes of getting caught from stealing $1 from a million victims is less likely than robbing a bank of a million in cash, and all but the most sophisticated law enforcement agencies lack the ability to electronically identify the culprits. Federal agencies tend to focus investigations on major thefts from institutions rather than crimes involving small amounts of money.

Introduction

When this presentation was first delivered at the annual conference sponsored by the Association of Computer Educators for Texas in October 2005, the title "An Emerging Crisis" seemed to be an appropriate title describing the growth of activities described as identity theft. By Spring of 2005, the title no longer seems descriptive. This article has been retitled: "The Identity Theft Crisis Has Arrived!"

The U.S. Postal Inspection Service has reported that identity theft cost the nation roughly $5 billion last year, not including lost productivity. In 2005, headlines suggest that the identity theft issue is no longer a threat but a reality. Identity theft has become the economic crime of 2005. For example, Time-Warner Inc. reported that an outside storage company lost data on some 600,000 current and former employees used to administer retirement, compensation and other benefits. Some 40 computer tapes were reported missing by the outside contractor, Iron Mountain Inc (CNN Money). On April 19, 2005 Ameritrade Inc. advised 200,000 current and former customers that a computer backup tape containing their personal information had been lost (Sullivan). ChoicePoint reported it had a breach of personal data involving between 145,000 and 500,000, and Bank of America reported that it "lost" 1.2 million customer records during Spring 2005 (Lemos). Of the 1.2 million customers, 900,000 belonged to Defense Department employees and many belonged to United States Senators (Morrison). In February 2005, 1.2 million records in SmartPay charge card program which has over $21 billion in

---

* Charles R. B. Stowe MBA, JD, Ph.D, Professor; Ken Balusek JD, Assistant Professor; and Keith Jenkins JD, Associate Professor, College of Business Administration, Sam Houston State University.

annual transactions reported the loss of its back up computer tapes (Lemos). Even universities have been targets of web thieves. In January 2005, George Mason University admitted that attackers broker into a server holding the names, photos and social security numbers of 30,000 students, faculty and staff (Lemos). Even terrorists have recognized that internet based identify theft is a gold mine to finance their operations. Imam Samudra, convicted of masterminding the bombing that killed 202 in Bali, Indonesia, wrote a book while in prison containing a chapter "Hacking, Why Not?" that explains the financial benefits that can be achieved through identity theft (Swartz).

Defining Identity Theft

Identity theft can be defined as the illicit use of another's identifying facts to perpetuate an economic fraud. The identifying facts usually stolen are name, date of birth, Social Security number, address, phone number, checking account number, credit card account number or other similar information. The economic fraud usually consists of the thief misusing an existing credit account, such as a credit card, using the stolen information to open new credit accounts, rent housing, obtain medical care, obtain employment, or file a fraudulent tax return to gain an undeserved refund. The thief will also use the stolen identity to commit other crimes.

According to the FBI, "perpetrators consider this a 'faceless' crime, since their targets are financial institutions or retail stores. Little if any thought is ever given to the harm their actions bring to the individuals whose identities they have stolen." Federal Bureau of Investigation, "Protecting Yourself Against Identity Fraud" (September 7, 1999). If this is true, then it is easy for the thief to rationalize his crime by telling himself that the victim is a business or other entity that can absorb the loss he creates. In actuality, there are two direct victims of the thief's actions, the entity that relied on the stolen identity and the individual whose identity was stolen.

With the increase in Internet transactions, businesses are compiling computer databases, which are used to store their customers' identifying information. Hackers can break into these databases and steal the information. Some Internet-connected computer servers store billions of pieces of identifying information making it easier for the thief to assume someone else's identity. In the days of yore, before widespread computer usage, businesses stored identifying information of customers in a manner that was not accessible to millions and millions of people. There have even been computer programs created that generate credit card numbers that will pass an authorization check. Craig Bicknell, *Credit Card Fraud Bedevils Web*, Wired News (April 2, 1999).

Stealing identities may also be accomplished through:

- Stealing pre-approved credit applications, bank and credit card statements, telephone calling cards, and tax information from mailboxes.
- Submitting change of address forms to divert mail from the true recipient to themselves.
- Running credit histories under false pretenses.
- Pickpocketing wallets or purses and using the credit cards, identification, and PIN numbers stored therein.

- Rummaging through trash dumpsters for discarded receipts, transaction records and other files that contain identifying information.
- Procuring employment in financial institutions or other entities with access to consumer credit reports or other identifying information.
- Searching through desks or files of fellow employees at work.
- Stealing checks from checkbooks or mailboxes.
- Buying identifying information from inside sources at businesses that has access to the information.
- Hacking into computers by replay attacks or eavesdropping on passwords, or by guessing passwords.
- Intercepting a calling card number by “shoulder surfing” (i.e. watching from a nearby location as a person punches in a telephone calling card number or credit card number or listening in on conversations if the person is giving their credit card number over the phone to a hotel or rental car company.

Internet based schemes include the following:

- Phlishing is sending out mass emails hoping to get gullible readers to voluntarily give up personal information. The culprits use a variety of strategies. On is to inform the unsuspecting that they have won a lottery and need to provide certain information in order to collect their winnings. Another version is to use the trademarked logos of legitimate banks, financial institutions and even the E-bay logo to warn people that they need to reconfirm information on their account. Another strategy is the compelling letter from Nigeria, Botswana or wherever informing the reader that they have been selected to serve as an agent for "lost funds" or "funds belonging to a deceased" or inherited funds that need to be invested in the United States. The recipient of these emails are directed to hit a web link or respond to a particular email address (not the one of the sender) in order to go on to the next step which is providing personal information.
- The other strategy is the compelling charity whereby individuals are mass solicited to give money to a recognized charity like the Red Cross. Although the American Red Cross is a fine organization, they have no idea that some organized cyber-gang is heisting money from potential donors through the use of false internet sites actually belonging to the gang and not to the real American Red Cross. Because these cyber-gangs lift the trademarks from existing web sites, it is impossible for many to tell the difference between a real organization's site and the thieves' site.

Using the Stolen Identity

There are many uses for real names, addresses, social security numbers and other personal identifiers. These include:

- Change the address for your current credit card account so that the owner will be unaware of charges to the account.
- Open new credit card accounts in the name of the theft victim.

- Open a new phone number or cellular account in the name of the victim.
- Open a bank account in the name of the victim and issue bad checks.
- Subscribe to online pornography.
- Applying for employment under the victim's name and impose the tax burden on the victim.
- Withdrawing funds from the bank accounts of the victim.
- Filing for bankruptcy using the victim's name.
- Issuing counterfeit checks and bank cards in the name of the victim.
- Taking out auto loans using the victim's credit history.
- Stalking the victim by using the information.
- Committing crimes under the victim's name and using the victim's clear criminal record to obtain a low bond and once out of jail, fail to appear for court hearings at which time an arrest warrant will be issued for the victim.
- Purchase guns using the victim's clear criminal record.

The more subtle and more dangerous strategy is based on creating small charges to your credit card bills in the amounts of $5-20. While this may not sound like a big theft, taking a few dollars each month via credit card theft from a 100,000 people can be quite lucrative. Thanks to the internet, this is extremely easy for the cyber-thief. And, with any luck, most of the victims will not realize that their identity has been stolen for many months.

Self-Protection

While there isn't much that individuals can do to prevent theft from computer databases maintained by their banks, credit cards, employers, retailers, etc. there are a few things that individuals should do to prevent or to have early recognition of a problem:

- In your wallet or purse, keep only the identifying information and cards that you absolutely need for your day to day activities. Make photocopies of the information that you do carry and store it in a secure location. This information will allow you to promptly report account numbers of lost or stolen credit cards or bank accounts.
- Monitor your bank and credit accounts. Know when the statements usually arrive in the mail. If the statement is late contact the bank or credit provider. Most bank and credit card accounts can be monitored via the Internet. This should not dramatically increase the risk your information will be stolen because the information is already stored on a database of the company. However, if a thief hacks into your computer, he may be able to obtain your password to the accounts because of your Internet monitoring activity.
- Protect your mail from theft. Promptly retrieve delivered mail and make arrangements to have your mail held if you are going to be away for several days. Also, do not leave outgoing mail in your mailbox. Drop it off at a collection box or post office.

- Protect your computer from hackers. Install firewall programs to protect your computer. This is especially important for businesses that store identifying information on customers in databases. Even though firewalls can be penetrated, some protection is better than no protection. Use spyware and adware programs to eliminate programs that may monitor your computer use to external parties.
- Never give your identifying information over the phone to solicitors. An identity thief can pose as a bank representative, a pollster, or a government investigator. Legitimate organizations with whom you do business have the information they need and will not ask for it.
- Monitor your credit report. Order a copy from the three credit bureaus at least each year, if not more frequently. Monitoring your credit report can reveal new accounts that have been opened without your knowledge. Also, it can reveal inquiries about your credit history. Inquiries that were not made by you attempting to secure credit may be a signal that someone else is trying to obtain credit using your information.
- Destroy identifying information that you are discarding. Shred charge receipts, credit applications, insurance forms, bank checks, expired charge cards, credit offers, and statements that you are discarding. Before revealing any identifying information, find out how it will be used, how it will be secured and whether it will be shared with others. Ask if there are alternate methods for identification. If they want your social security number, ask why they need it. Offer another number as an alternative.
- Businesses should limit the number of employees who have access to identifying information on customers. Limiting the opportunity to access identifying information will limit the temptation of the employee to steal information and misuse it or sell it to a thief.

If you discover that your identity has been stolen, one should immediately view the government's web page www.consumer.gov/idtheft, notify your bank and credit card providers, and your local law enforcement officials. The identity theft crisis has arrived!

References

CNN Money "Time Warner Employee Data Missing" http://money.cnn.com/2005/05/02/news/fortune500/security_timewarner/index.htm?cnn=yes accessed 5/18/2005

Federal Bureau of Investigation, “Protecting Yourself Against Identity Fraud” (September 7, 1999).

Federal Trade Commission - Consumer Advice - Identity Theft www.consumer.gov/idtheft/

Lemos, Robert, "Perfect storm for New Privacy Laws?" CNET News.com http://news.com.com/2102-1029_3-5593225.html?tag=st.util.print

Morrison, Joanne"Bank Loses Card Data of Senators, U.S. Govt Staff" http://news.yahoo.com/news?tmpl=story&cid=1896&u=/nm/20050226/us_nm/financial_b Accessed 3/15/2005

Sullivan, Bob "Ameritrade Warns 200,000 clients of Lost Account Information, Including SSNs, on missing tape" MSNBC Technology and Science, http://www.msnbe.msn.com/id/7561268 accessed 5/18/2005.

Swartz, John "Terrorist Use of Internet Spreads" USA TODAY, http://www.usatoday.com/tech/news/2005-02-20-cyber-terror-usat_x.htm Accessed 3/15/2005.