Identity Theft: A Tutorial

By
Robert J. Boncella

WASHBURN UNIVERSITY
SCHOOL OF BUSINESS
WORKING PAPER SERIES
Number 48

July 2005

Washburn University
School of Business
1700 SW College Ave.
Topeka, KS 66621
785-231-1010, extension 1308
www.washburn.edu/sobu

*Robert J. Boncella is professor of computer information systems at the School of Business at Washburn University, Topeka, Kansas. Comments should be directed to Robert J. Boncella, School of Business, Washburn University, 1700 SW College Ave. Topeka, Kansas 66621, 785-231-1010, extension 1839, bob.boncella@washburn.edu.

Identity Theft: A Tutorial

Dr. Robert J. Boncella School of Business, Washburn University
bob.boncella@washburn.edu

ABSTRACT

This tutorial will provide the reader sufficient information to understand what is identity theft, how it occurs, what is the effect, and how to recover when it has occurred.
In addition information will be provided on how to prevent identity theft. The purpose of this work is to bring together the relevant sources of information on identity theft and present them in concise and coherent manner. The relevant information will include data on the frequency of identity theft, the overall cost, and current legal processes in place to minimize identity theft.

Keywords: Identity Theft, Frequency of Identify Theft, Cost of Identity Theft, and Prevention of Identity Theft

INTRODUCTION

History

Identity theft is not new is has been occurring for a number of years. One only needs to recall the story of Isaac and his sons Jacob and Esau as told in Genesis 27.

Definition of Identity Theft

Today the common definition of identity theft is when someone possesses or uses your name, address, Social Security number (SSN), bank or credit card account number, or other identifying information without your knowledge with the intent to commit fraud or other crimes.

HOW DOES IT OCCUR

Acquire Personal Information

For identity theft to occur the perpetrators gain access to your personally identifying information. They attempt to do this using a variety of methods both high tech and low tech.

High-tech methods include obtaining personal information by: stealing records from your employer, bribing an employee who has access to your records, social engineering information from employees, or hacking into the organization's computers.

Low-tech means are "dumpster diving" which is rummage through your trash, the trash of businesses, or dumps in an attempt to acquire personal information.

Other techniques are obtaining access to credit reports by posing as a landlord, employer or someone else who may have a legitimate need for and a legal right to your personal information.

It is easy to obtain credit and debit card account numbers from your credit or debit card by using a special information storage device in a practice known as "skimming." This is basically a card reading device that reads and decodes the information encoded in the magnetic strip on the back

of credit or debit cards. It should be noted that hotel "keyless cards" might contain personal information encoded in the magnetic strip and should be destroyed after use.

More overt methods include stealing wallets and purses containing identification and credit and bankcards. Stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information. Perpetrators may complete a "change of address form" to divert mail to another location. They scam information from you by posing as a legitimate businessperson or government official.

Use of Personal Information

Once identity thieves have your personal information, they may use your credit and debit card account numbers to buy "big-ticket" items they can easily resell for cash.

Or open a new credit card account, using your name, date of birth and SSN. In addition they may change the mailing address on your current credit card account. They will run up charges on the account. Since the bills are being sent to the new address it may take some time before you realize there's a problem.

Other fraud that can happen: auto loans in your name; establish cell phone service in your name; open a bank account in your name and write bad checks on that account.

In general, id theft allows the perpetrators to do anything that you can do financially but they are not responsible.

IF I'M A VICTIM OF IDENTITY THEFT HOW CAN I DETECT IT?

In general being aware of your financial transaction will allow you to detect if you are a victim of identity theft. For example when a new credit account is opened in your name, these accounts are likely to show up on your credit report. So you should periodically request a credit report. In addition, read your financial account statements promptly and look for any unauthorized debits or charges.

If you fail to receive bills or if they don't arrive on time can be a sign of identity theft. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover the identity theft.

Other indications are: receiving credit cards for which you didn't apply; being denied credit, getting calls or letters from debt collectors or businesses about merchandise or services you didn't purchase.

HOW TO RECOVER FROM IDENTITY THEFT

- If you suspect you are the victim if identity theft the first step is to report the fraud to the three major credit bureaus: Equifax, Experian, and Trans Union.
- Report the crime to the police and call creditors.
- Request a credit report, if possible from all three credit bureaus. Review your credit reports carefully and request information on fraudulent accounts
- Write to the credit bureaus.

- If your checks or bank account information were stolen close your bank account and open a new one with a new account number.
- If a debt collector contacts you tell the debt collector that you are the victim of identity theft and you dispute the validity of the debt. State that you did not create the debt and are not responsible for it.
- If your driver's license or DMV-issued ID card was stolen contact your local DMV office to report the theft. If available in your state ask for a fraud alert on your license.
- If your mail was stolen or your address changed by an identity thief notify the Postal Inspector.
- If you are wrongly accused of a crime committed by an identity thief check to see if your state has database of criminal identity theft cases. If so make sure your case is in that database.
- If someone uses your Social Security number to claim unemployment benefits or to work contact the Social Security Administration. If someone uses your social security number to work that will show up on earnings record maintained by the Social Security Administration.
- Contact the Federal Trade Commission and file a complaint. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps them learn more about identity theft and the problems victims are having so that we can better assist you.

The effects of identity theft may some time to be resolved. Resolution depends on many factors: the type of theft; if the thief sold or passed your information on to other thieves; was the thief is caught, and difficulties encountered in correcting your credit report.
Monitoring your credit report and other financial records for several months after the discovery of the crime is a wise strategy. Credit reports should be checked frequently in the first year of the theft, and periodically thereafter.

HOW TO PREVENT IDENTITY THEFT

The most effective method to reduce the chance of identity theft is to manage your personal information wisely,

- Unless you've initiated the contact or are sure you know whom you're dealing with don't give out personal information on the phone, through the mail or over the Internet. Identity thieves will pose as legitimate representatives of organizations in order to get you to reveal your SSN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing
- Leave you social security in a secure place there is no need carry your social security card.
- Use a home safe or strong box to secure personal information in your home.
- Guard your mail from theft: Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured home mailbox. Remove mail from your mailbox as soon as possible.
- Tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mailto thwart "dumpster diving".

- Carry the minimum identification information. Also only those credit and debit cards that you'll actually need.
- Password protect your credit cards, bank cards and phone accounts.
- Avoid using information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers as passwords.
- When requested use a password instead of your mother's maiden name.
- Give your SSN only when absolutely necessary. Avoid using your SSN as primary identification number. For example driver's license id number or student id number.
- Know your billing cycles. If your bills don't arrive as expected check with creditors. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work.
- When ordering new checks, pick them up at the bank, rather than having them sent to your home mailbox.

Computer use, the Internet, and Identity Theft

Don't store personal information on your PC or Laptop. However if you're storing personal information such as SSNs, financial records, tax returns, birth dates, or bank account numbers in your computer make sure your computer is secure. To do this the following is advised.

- Use virus protection often
- Virus protection software should be updated regularly
- Patches for your operating system and other software programs should be as soon as they are available
- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know.
- Be careful about using file-sharing programs. These effectively share your PC with the whole Internet.
- If you use a high-speed Internet connection like cable or DSL that leaves your computer connected to the Internet 24 hours a day use a firewall program to control access to you machine.
- Use a secure web browser software that encrypts using SSL information you send over the Internet to guard your online transactions.
- Try not to store financial information on your laptop unless absolutely necessary.
- Use a strong password - a combination of letters (upper and lower case), numbers and symbols. A good way to create a strong password is to think of an easily remembered phrase or book title and use the first letter of each word as your password. For example, "The Old Man and the Sea" would become "TOMATS".
- Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished

- Before you dispose of a computer, wipe all the personal information stored on the drives. This is not the same as deleting files using operating system commands. Purchase a utility program to overwrite the entire hard drive with a single character.
- Look for website privacy policies. They will answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties.

CURRENT LEGAL PROCESSES TO MINIMIZE IDENTITY THEFT

Federal Laws

Criminal Laws

Identity Theft and Assumption Deterrence Act

http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html. In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) to address the problem of identity theft. Specifically, the Act amended 18 U.S.C. § 1028 to make it a federal crime when anyone:

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.

Violations of the Act are investigated by federal investigative agencies such as the U.S. Secret Service, the FBI, and the U.S. Postal Inspection Service and prosecuted by the Department of Justice. Section 5 of this Act, Pub. L. No. 105-318, 112 Stat. 3007, makes the FTC a central clearinghouse for identity theft complaints. The Act requires the FTC to log and acknowledge such complaints, provide victims with relevant information, and refer their complaints to appropriate entities (e.g., the major national consumer reporting agencies and other law enforcement agencies).

Identity Theft Penalty Enhancement Act

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h1731enr.txt.pdf. This Act establishes penalties for aggravated identity theft.

Credit Laws

Fair Credit Reporting Act

http://www.ftc.gov/os/statutes/031224fcra.pdf. The Fair Credit Reporting Act establishes procedures for correcting mistakes on your credit record and requires that your record only be provided for legitimate business needs.

Fair Credit Billing Act

http://www4.law.cornell.edu/uscode/15/ch41schIpD.html. The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts. It also limits a consumer's liability for fraudulent credit card charges.

Fair Debt Collection Practices Act

http://www4.law.cornell.edu/uscode/15/1692.html. The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection.

Electronic Fund Transfer Act

http://www4.law.cornell.edu/uscode/15/1693.html. The Electronic Fund Transfer Act provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers.

Privacy and Information Security

Driver's Privacy Protection Act of 1994

http://www4.law.cornell.edu/uscode/18/2721.html. This law puts limits on disclosures of personal information in records maintained by departments of motor vehicles.

Family Educational Rights and Privacy Act of 1974

http://www4.law.cornell.edu/uscode/20/1232g.html. This law puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funding.

Gramm-Leach-Bliley Act

http://frwebgate.access.gpo.gov/. The relevant sections requires the FTC, along with the Federal banking agencies, the National Credit Union Administration, the Treasury Department, and the Securities and Exchange Commission, to issue regulations (to be codified at 16 CFR Part 313) ensuring that financial institutions protect the privacy of consumers' personal financial information. Such institutions must develop and give notice of their privacy policies to their own customers at least annually, and before disclosing any consumer's personal financial information to a nonaffiliated third party, must give notice and an opportunity for that consumer to "opt out" from such disclosure.

Health Information Portability and Accountability Act of 1996, Standards for Privacy of Individually Identifiable Health Information

http://aspe.hhs.gov/admnsimp/bannerps.htm#privacy. The privacy rule regulates the security and confidentiality of patient information. It took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct certain financial and administrative transactions electronically) having until April 2003 to comply.

State Laws

National Conference of State Legislatures

http://www.ncsl.org/programs/lis/privacy/idt-01legis.html

Cost and Frequency of Identity Theft

On September 3, 2003 the Federal Trade Commission released the results of a survey, which stated that 27.3 million Americans were victims of identity theft within the last five years. This included 9.9 million people in 2002. According to the survey, 2002's identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses. See http://www.ftc.gov/opa/2003/09/idtheft.htm for more detail.

Table 1 below is the most recent summary of identity thefts complied for the United States by the FTC. See http://www.consumer.gov/idtheft/stats.html for more FTC statistics regarding identity theft.

Rank	Victim State	Victims Per 100,000 Population	Number of Victims	Rank	Victim State	Victims Per 100,000 Population	Number of Victims
1	Arizona	142.5	8,186	26	Ohio	60.7	6,956
2	Nevada	125.7	2,935	27	Connecticut	57.1	2,000
3	California	122.1	43,839	28	Minnesota	57.0	2,905
4	Texas	117.6	26,454	29	Oklahoma	56.0	1,973
5	Colorado	95.8	4,409	30	Tennessee	55.0	3,246
6	Florida	92.3	16,062	31	South Carolina	51.2	2,148
7	New York	92.0	17,680	32	Arkansas	50.8	1,397
8	Washington	91.1	5,654	33	Hawaii	50.7	640
9	Oregon	87.8	3,156	34	Rhode Island	50.6	547
10	Illinois	87.6	11,138	35	Louisiana	49.9	2,254
11	Georgia	84.3	7,440	36	Alabama	48.9	2,216
12	New Mexico	83.4	1,588	37	Wisconsin	48.0	2,646
13	Maryland	83.0	4,612	38	Mississippi	46.5	1,330
14	Utah	76.6	1,831	39	Nebraska	45.1	788
15	New Jersey	75.1	6,530	40	Idaho	43.1	600
16	Michigan	72.3	7,307	41	Wyoming	42.2	214
17	Indiana	68.5	4,274	42	New Hampshire	41.8	543
18	Missouri	67.9	3,905	43	Kentucky	40.1	1,662
19	Delaware	66.6	553	44	Montana	39.3	364
20	Alaska	66.1	433	45	Iowa	34.8	1,028
21	North Carolina	65.8	5,623	46	West Virginia	34.2	621
22	Virginia	63.6	4,742	47	Vermont	33.5	208
23	Kansas	61.3	1,677	48	Maine	32.2	424
24	Massachusetts	61.1	3,921	49	North Dakota	29.6	188
25	Pennsylvania	61.0	7,563	50	South Dakota	23.2	179

*Per 100,000 unit of population estimates are based on the 2004 U.S. Census population estimates (Table NST-EST2004-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2004). Numbers for the District of Columbia are 922 victims and 166.6 victims per 100,000 population.

Federal Trade Commission
Created February 1, 2005

Table 1 Identity Theft Victims by State (Per 100,000 Population)

CONCLUSION

The preceding has allowed the reader to understand what is identity theft, how it occurs, what is the effect, and how to recover when it has occurred. We have summarized the current legal processes in place to minimize the effects and possibility of identity theft. In addition the cost and frequency of identity theft has been stated. For more details the reader is referred to http://www.consumer.gov/idtheft.