Global Information Assurance Certification Paper

Dealing with Identity Theft

Abstract:
The purpose of this paper is to educate the public about Identity Theft, and help people who are the victims of this crime. There are four parts to this essay. Part One explains what identity theft is and the extent of the problem. Part Two explores how identity theft happens. Here we see some of the tools and trickery used to gather information. This encompasses both the high-tech and low-tech methods for gathering the personal information needed to assume someone's identity.

Part Three explains how to re-claim a stolen identity. This section contains an action plan you can use to restore your good name. And, the last section explains what you can do to prevent identity theft. This covers practical steps people can take to protect their personal information at home and at work. See the appendix for additional web links, phone numbers of organizations and government agencies.

Stephen Moran

GSEC Practical
Option 1, Version 1.4b
August 22, 2003

Dealing with Identity Theft

As the Data Security Manager for a bank, I conduct security awareness seminars several times a year for my employer. I am always amazed to discover that over 25% of the employees attending each seminar have family members that have experienced identity theft. Despite the computer security measures taken in the work place, we too will likely experience identity theft in our lifetime. People need to know how to protect their personal information, and what to do when they become a victim of identity theft.

In this essay, Identity Theft will be defined, and then it will be explained how it is committed. We will look at what is being done to protect citizens from criminals, and what people can do when they become identity theft victims. And finally, we will look at ways to protect your personal information. The Appendix contains many links to web-sites that have information about restoring your good name. Make sure you spend some time visiting these sites.

What is Identity Theft?

Identity theft is the unauthorized use of an individual's personal information by another person for the purpose of committing fraud. The fraud is committed by using another person's identity to obtain unauthorized credit cards and loans, making unauthorized purchases, or committing crimes in the victim's name.

The information needed to assume someone's identity is easy to obtain and use. Our identity can be based on a few personal statistics and facts: our name, address, social security number, fingerprints, parent's names, bank account code, PINS, photographs, and DNA. The United States government identifies people by their legal name, social security number, and date of birth. The Federal Trade Commission (FTC) documented over 161,000 cases of identity theft in 2002, and identity theft is the fastest growing fraud crime in our country today. This crime represented 43% of all fraud cases reported in the US.[1]

There are several indications that your identity has been stolen. You start receiving bills for items that you did not purchase, and bill collectors start calling and visiting you about past-due accounts. Your bank contacts you about bouncing checks or you are denied credit for a new purchase because your credit is bad. Let's look a real case of identity theft.

Mike, a fellow bank employee, shared his identity theft experience with me. Mike is an upstanding man in his early thirties. He has worked hard and established an excellent credit history over the past 14 years. Mike's outstanding credit history allowed him to purchase several cars and a home in the San Francisco Bay area. In October 2002, Mike's credit history was rated Excellent.

[1] Federal Trade Commission. National and State Trends in Fraud and Identity Theft, Jan. 22, 2003

In November, Mike was looking for employment in the Los Angeles area, and he applied for a security guard job at a Community College. He filled out a job application for the position, and submitted the paperwork to an HR department representative. Within weeks, someone had used his personal information and stolen Mike's identity. The identity thieves ordered a department store credit card, a gasoline charge card, and opened a charge account at a jewelry store in his name.

By the end of December the identity thieves were busy buying furniture, appliances, gasoline, and jewelry. The charges for the accounts at, Lowe's, Chevron, and Westerfield's Jewelry stores totaled $39,000 in four months. Mike was never aware of the mounting debt, because the thieves had opened new charge accounts and the bills were never delivered to his address. All of Mike's regular bills were being paid on time.

Mike's first indication of a problem surfaced in early May when he decided to purchase a new car. He negotiated a great deal on a new car. The salesman finally needed to run a credit check on Mike to approve the car's financing. To his disbelief, Mike was told that there was a BIG problem with his credit. Mike told me, "I thought he was joking, but he wasn't." "I was shocked and embarrassed; I couldn't believe what I saw on the credit report."

Since May 2003, Mike has been calling creditors, credit reporting agencies, and the police, trying to restore his good name. Some progress is being made, but it is painfully slow. Mike never did purchase his new car, and it may be years before he can undo the damage that was committed in his name.

A person's identity may have been stolen for one of many reasons including financial gain, extortion, revenge, security access, political embarrassment, or to hide other crimes. The rising popularity of this crime is due to its low risk of being caught. Here is a sobering report from a Gartner study:

> "…Seven million U.S. adults … were victims of identity theft during the 12 months ending June 2003, according to a new survey by Gartner Inc." "This represents a 79 percent increase over the 1.9 percent rate reported in a Gartner consumer survey concluded in February 2002. Because this crime is often misclassified, the thieves have better than a one in 700 chance of being caught by the federal authorities. "[2]

The identity thief is able to work in secret, and the victim is unaware of the crime until his or her financial records finally indicate something is very wrong. North Carolina Attorney General Roy Cooper said, **"**Businesses are losing billions of dollars to this crime." " Most of the time the Bank loses the money, and the customer loses their good name."[3] According to the American Banking Association, nearly 40% of the banks participating in the last year's fraud survey ranked identity theft as the No. 1 threat to the banking industry**.** [4]

---

2 Pettey, Christy. Gartner Inc. July 21, 2003

3 Gadwa, Tess. Charlotte Business Journal, June 16, 2003

How did the thief obtain my information?

Computers have been making identity theft easier by enabling thieves to quickly collect massive amounts of personal information from databases and public records. High tech surveillance and hacker tools have enabled some thieves to sniff network traffic and log keyboard strokes revealing user names and passwords to financial accounts. Many companies have inadequate security systems in place to protect customer information from theft and hacking activity. A few examples bring home the point:

- Republic Bank – In 2002, the bank's firewall was breached and a hacker stole the personal data of 3,600 online-banking customers. [5]

- The State of California – In April 2003, a hacker compromised the payroll information for 265,000 state employees. [6]

- TriWest Healthcare Alliance is a managed care contractor for the Pentagon. The thieves broke in and stole computer hard drives containing the names, addresses, phone numbers and social security numbers of more than 562,000 military personnel.[7] After this incident, TriWest's CEO wrote a public letter of apology to the stockholders for the break and theft of company information. [8]

- Data Processors International handles transactions for catalog and direct marketing companies. The Secret Service reported that a hacker accessed over 10 million credit card numbers. [9]

When was the last time you used a computer in Kinko's? Last year, in a court case in New York City, Ju Ju Jiang was convicted for installing a keyboard logger on Kinko's store computers in thirteen locations around the city. For the past two years, he collected over 450 online banking user names and passwords, and used the information to take money from the accounts and to open new ones.[10]

Company computers are not the only source of information. There is a great deal of personal information available in the public records and vital statistics, and Internet search engines make it very easy to obtain this information. The Internet phonebook and reverse directory are handy ways to find a friend in another part of the country.

> According to Kevin Mitnick: "…your personal information is not private at all. Anyone with Internet access and an anonymous prepaid phone card can, in just a few minutes, obtain your driver's license number, Social Security number and

---

4 Gadwa, Tess. Charlotte Business Journal, June 16, 2003
5 InfoSec Briefs. Information Security Magazine, April 22, 2002 - Vol. 4, No. 31.
6 Hayes, Frank. Computerworld, June 03, 2002.
7 Mientka, Matt. U.S. Medicine, February 2003
8 McIntyre, David J. Jr. TriWest, Announcement
9 Ho, David. The Associated Press April 3, 2003
10 Poulsen, Kevin. SecurityFocus, July 18, 2003

> mother's maiden name and the names of your spouse, children and pets. Much of this information is readily available on the Internet or through one or two telephone calls." [11]

There are many commercial investigative databases that can be used to locate people in the United States. One such database is Peopledata at www.peopledata.com. For just a few dollars, this site provides the following information on a selected person: address, phone number, date of birth, background check, and a satellite photo. Or, for $19.95 you can purchase CyberDetective and use this computer program to help discover information about anyone that you choose. The site boasts having 750,000 happy customers using their product. You can find CyberDetective at the following URL: http://cyberpi.info/CyberDetectivePIToolBox.htm.

Other sources of personal information for identity theft are stolen wallets and purses, stolen mail, company trash, lost laptop computers and Personal Digital Assistants (PDAs), and social engineering. Dumpster diving, is the practice of rummaging around in a company's trash. This is a quick and easy way of finding information about customers and products. Old computer printouts containing customer data are still valuable to a thief. Your personal trash at home may also contain discarded bank statements and other financial information. An account number and a customer name are enough information for a social engineer to start impersonating a real customer. However, the most disturbing facts about the cause of identity theft are dishonest and irresponsible employees stealing or losing company information.

> According to Judith Collins, Department Head of ID-theft prevention at Michigan State University, "About 70 percent of the (identity theft) cases start as inside jobs -- employees stealing customer information, such as credit card numbers, Collins said. Some theft comes from stolen wallets and purses, while a small number comes from stolen mail or trash."[12]

> John Leyden wrote, "The PDA Usage Survey 2003 found that PDA owners commonly download the entire contents of their personal and business lives onto their hand-held computers." "More than 40 per cent of people surveyed have lost a mobile phone, and a quarter have lost a laptop or PDA or both."[13]

Another source of personal information for the thief is your Mail. Most people are immediately aware that they have lost their wallet or purse, but stolen mail is hard to detect. The thief files a change-of-address notice with the U.S. Post Office, which diverts mail to a post office box before the victim finds out what's happening. By the time the victim becomes aware that they are not getting their bills and checks, the thief has already cashed your checks and made fraudulent charges on your accounts.

So, with all the information sources available, which one is the identity thief most likely to use?

---

[11] Mitnick, Kevin. The Mercury News, January 30, 2003
[12] Gadwa, Tess. Charlotte Business Journal, June 16, 2003
[13] Leyden, John. The Register, August 2, 2003

> "The greatest vulnerability for computer security doesn't come from technological flaws in hardware and software but from the weakest link in the security chain: People. And not just dishonest employees, trusted insiders can be duped or deceived into giving away the keys to the kingdom." Kevin Mitnick [14]

Social engineering is the art of tricking people into giving away information that allows the thief unauthorized access to accounts and computer systems for the purpose of committing fraud. The social engineer assumes a fake identity and uses it to steal your trust. Social engineers are bold crooks, and Kevin Mitnick was a master at this. Usually, they call people and ask a series of seemingly innocent questions, posing as a company or government representative, hoping that you will tell them something about yourself they can use against you. Here is an example:

A social engineer calls someone and might pretend that he was from a collection agency. In the conversation, the thief would tell the victim that they have a past-due account with the Phone Company for $82.14. He would threaten that if the victim didn't pay the bill immediately their phone would be disconnected, and then there would be a $250 charge to re-connect the phone service. Naturally, the customer would become flustered and protest that the bill was in error. At this point, the social engineer offers his help to verify the account record and clear up the problem. Now he begins to subtly question the victim about his account. The victim is usually willing to cooperate to clear up the misunderstanding, so he gives his name, address, account number, the name of his bank, and the check number he used to pay the bill.

In this case, you should insist that a copy of the phone bill be mailed to you immediately. Then you can examine the bill and call to the Phone Company and clear up any real problems. Be careful about what you say on the phone! Social engineers are really deceptive crooks. You must verify the identity of the person on the phone before giving them any personal information.

What do you do when your identity has been stolen? Reclaim Your Identity!

Internetweek reported that companies are not spending any more on information security even with today's increased threats.[15] So, it is up to each of us to prepare for the worst. Unfortunately, many people don't know what to do if they have their identity stolen. Here is an action plan that you can use to reclaim your identity and start restoring your good name.

Report the Crime and file a Police report within 24 hours.
By filing a police report, you are reclaiming your identity and letting everyone know you are a victim of a crime. The police report is an important document that will help you settle disputes with your creditors. Therefore, it is very important that the crime be reported as quickly as possible to minimize the damage done in your name. Keep a journal about your activities, and whom you called and wrote. Document everything you

---

[14] Mitnick, Kevin. The Mercury News, January 30, 2003

[15] Hulme, George V. InternetWeek, Monday July 28, 2003

can about the extent of the identity theft, then file a police report about the crime as soon as possible.

Contact the Credit Reporting Agencies: Call Experian, Trans-Union, and Equifax immediately and have them place your credit on Fraud Watch. Order copies of your credit history from each credit bureau. See the resource section for samples of Dispute Letters and contact information for each of the credit agencies. These agencies communicate with each other, and notifying one will result in all having the fraud alert placed on your records. Credit Bureau Resources:[16]

Trans Union -- www.tuc.com
Credit report: 1-800-916-8800
Fraud Line: 1-800-680-7289

Experian -- www.experian.com
Credit report: 1-888- 397-3742
Fraud Line: 1-888- 397-3742

Equifax -- www.equifax.com
Credit report: 1-800-685-1111
Fraud Line: 1-800-525-6285

Contact your Bank and have them place you on fraud watch. The Bank has procedures on how to handle Identity Theft cases. They will have you talk with their security department for information about the crime. If the thief accessed your bank account, then close all of your bank accounts and re-open new accounts. You must do this quickly to show that you took reasonable care of your account(s) to minimize fraud**. You are NOT responsible for any checks written by the thief.** The Bank is responsible for verifying your signature on every check! The law is on your side, and you will not pay for any fraudulent charges! Ask the Bank to help you contact your creditors and clear your name.[17]

If your Bank isn't helpful in resolving your identity theft issues, then inform the bank that you are going to contact the Bank Commissioner. They are the regulators for the Bank. You can contact the FFIEC at: http://www.ffiec.gov/nic/default.htm. You may need to conduct an Institution Search to determine which Federal agency has jurisdiction over your bank. The Regulators are agencies such as the FDIC, FED, and NCU. Contact the appropriate Regulator and ask for help.

Contact the Federal Trade Commission and report the crime. There are many documents about Identity Theft available at their web-site: http://www.consumer.gov/idtheft. This is a very good resource for information. The FTC tracks all fraud in the United States. Another must see web-site is: http://www.compleatprofessional.com/idtheft1.html#IDTheft. This has terrific information and documents you can use to inform creditors about your identity theft.

---

16 Wright, Chris. CPP, "Identity Theft" ASIS Virtual Seminar, June 11, 2003
17 Wright, Chris. CPP, "Identity Theft" ASIS Virtual Seminar, June 11, 2003

Call Social Security and have them place you on fraud watch. You may request a new Social Security Card. These folks are very helpful and they will provide additional information about reclaiming your identity.

Contact your Post Office and make sure your address information is correct. Check and see if your mail is being forwarded to another address. The police can use this evidence to track down the crooks.

Tell your family and friends about your troubles, and warn them to watch their financial accounts for signs of fraud. The thieves may have collected the names of family members and their personal information, (names, birth dates, and SSN) when they stole your identity.

Call your Creditors. Contact Department Stores, Utilities, Phone Company, City, Insurance carriers, and anyone else who may be affected by your misfortune. See the Appendix for web-links to sample Dispute Letters and contact information. Watch your credit card statements for signs of abuse. Cancel any misused credit cards immediately. Check your credit report for errors at least twice a year.

Your employer should be informed that your identity was stolen, and that you are actively working with the police and credit agencies to clean up your record. Arrange to have your paycheck automatically deposited into a new bank account.

Call the Department of Motor Vehicles and report the crime. You may need to have your driver's license canceled and reissued.

Contact the FBI, Secret Service, and the IRS. Why? Terrorists are assuming stolen identities and committing crimes. Your information reported to these agencies may help prevent another 9-11 disaster. The FBI investigates identity theft at the local level. The Secret Service generally investigates cases when monetary losses are large, or when your information provides evidence of a larger pattern of fraud.

Talk to legal counsel and clear your name in the courts! You may need legal help to resolve the credit problems and restore your good name. Call the State Bar Association, and ask for a referral to an attorney that specializes in Identity Theft cases.

Things you can do to stop identity theft at work and at home

- You must be careful when sharing sensitive information with someone on the phone. Make sure you know the person before you give away details about yourself or your family.

- **Never share your system user id and password!** Use strong passwords and force everyone to change them regularly. Good passwords are words not found in a dictionary. A Strong password is at least 8 characters long, a combination of upper and lowercase letters, numbers, and symbols. A Pass-phrase is usually easy to

remember. Use the first character of each word to form your password. Here is an example of a strong password:

(**T**ake **M**e **O**ut **T**o **T**he **B**all **G**ame**!** -- **Tm0ttBg!**)

- Install and use a current anti-virus program and personal firewall software before browsing the Internet. Remember to update your anti-virus patterns frequently, and keep the operating system patches current.

- Be careful with sensitive information while in public areas. While traveling, always be aware of who is around you. Social engineers will eavesdrop on conversations, and shoulder surf for information. You must be more security conscious when you are outside of your home and office.

- If you travel with a laptop, then you need to encrypt your hard drive and data files. Many encryption software packages can be purchased for under $75.00. Be very careful with your laptop when traveling. The Airport and Taxis are the most common places to lose your PC.

- If you have a Personal Digital Assistant (PDA), then use the password feature to lock your device. Remember to choose a strong password, so if you lose your PDA you won't give away your personal information to a thief. The only way to use the stolen PDA is to reset it and erase all the information on the device.

- Physical security and building access controls are mandatory. Employees must have visible identification to enter the building, and have it checked by a guard or electronic sensor. Using both biometric devices and personal PIN codes are especially good as physical security controls. The buildings must be segmented into secure zones to prevent non-company personnel from wandering into sensitive areas. This limits the opportunities for property theft.

- Network access needs to be controlled and monitored. Unused computer workstations are Prime targets for social engineers to install unauthorized wireless access points. Example:

  A social engineer waits outside the company door with a box of equipment in his arms. An employee sees the person struggling with the door and opens it for him. The social engineer wanders around until he finds an open data jack and plugs in his wireless access point. Then the thief goes out to the parking lot and uses a wireless sniffer on his laptop to monitor the company network for passwords and sensitive information.

- Logical access controls are applied to computer systems to limit access to critical systems and data. Only those people with a "need to know", should be given access to sensitive information. The principle of least privilege should be enforced with vigilance.

- Limit the number of remote users working away from the secure building. Encrypt sensitive data on their home PCs and laptops. Use a Virtual Private Network (VPN) to connect back to the company with some form of two-factor authentication.

- Purchase a small fireproof safe for protecting your personal documents at home. Make photocopies of your credit cards and other personal information and keep the documents locked in a safe. Lock up your Social Security Card.

- Purchase a crosscut shredder. Use it to destroy any discarded documents with your account information or any personal information about your family. Shred OLD bank statements, credit card information, utility bills, insurance policy information, or medical information.

- Carry only necessary personal information in public and leave the rest at home in a safe.

- Protect your mail. Use a locking residential mailbox, or a post office box. Use security envelopes. Mail checks at the post office or a mailbox away from your home. Use direct deposit for regular income checks. [18]

- Protect your checks. Don't pre-print personal information on them. (Drivers license number or phone number) Don't share your account number with people you do not know.[19]

- Order a credit report at least twice a year and verify its accuracy. Correct any mistakes on your credit report IMMEDIATELY.

- You can opt out of any pre-approved credit cards by calling. (888) 567-8688

- Block your name from Marketing Lists. Opt out of Mass marketing mailings by contacting the Direct Marketing Association and have them remove your name. www.the-dma.org[20]

- **Most Importantly, Don't trust people you meet online. Teach your family never to give personal information about family members on the Internet.**

What's being done to prevent this crime? The Law

Identity theft is a relatively new type of crime. Prior to 1998, there were no Federal laws against assuming someone's identity. However, it has become the focus of many laws in the past five years. Just recently Congress passed the Privacy Act, Gramm Leach

[18] Wright, Chris. CPP, "Identity Theft" ASIS Virtual Seminar, June 11, 2003
[19] Wright, Chris. CPP, "Identity Theft" ASIS Virtual Seminar, June 11, 2003
[20] Wright, Chris. CPP, "Identity Theft" ASIS Virtual Seminar, June 11, 2003

Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and the Patriot Act. The Patriot Act has a provision going into effect October 1, 2003. The Customer Identification Program (CIP) requires all financial companies to verify the customer's identity when they open a new account. The company must examine and record the customer's name, address, driver's license number, and date of birth.

In California, new privacy laws went into effect in July 2003: California's Data Security Disclosure Law - Cal Civ Code 1798.82, SB 1386, and AB 1773. These laws mandate that companies protect customer information. Companies must ask permission of their customers prior to releasing or selling information to other companies, and that all customers must be notified in writing if a computer system containing unencrypted personal information is breached. This means that any unauthorized access to information, employee or crook, could trigger the need to notify all of the company's clients in writing.

The privacy laws are targeted at companies and government agencies to force them to practice information security due diligence. All personnel must follow established security policies to ensure the confidentiality, integrity, and availability of all systems containing customer non-public information. The penalties for companies violating these laws can be severe. The Gramm Leach Bliley Act, for example, can assess companies up to $100,000 per violation. The Directors and Board members can be fined $10,000 each and face prison terms of five years for non-compliance.

Individuals are also being prosecuted for identity theft. Kevin Mitnick was sentenced and served five years in prison for identity theft. Ju Ju Juiang was just convicted of a similar crime in New York, and he faces jail time and fines for stealing people's on-line banking information.

Conclusion

Identity theft is an insidious crime that can ruin lives for years and it is growing rapidly. Everyone must take action now to protect themselves and their families from its miserable consequences. Has the Law required enough controls to safeguard our information? Yes. Are the penalties for companies severe enough to insure compliance? Yes. Do you feel secure about the companies managing your information? No. Why? There is an inverse relationship between the usability of a computer system and its security. If you make the computer more secure, it becomes harder to use and interferes with the user's productivity. Or, if you make the computer more user friendly, then the security of the data is placed at risk.

Companies have implemented the security measures mandated by the Law, but the information accessed from the computer is only as secure as the person using it. Therefore, identity theft will not be completely mitigated by passing Laws, or installing elaborate computer security. The final piece needed to solve the security problem is people. "We must have trusted company employees trained properly to do the right

things with the sensitive information they access." Mitch Kabay, PhD, CISSP [21] Companies need to be very careful in the hiring process, and treat their employees fairly so that they do not become disgruntled and misuse sensitive information. Security training must be conducted regularly to keep security awareness high. Only when all three elements are fully implemented and enforced will there be a dramatic decrease in identity theft. We must vigilantly guard our personal information, and look for the early signs of identity theft so we can act quickly before it gets out of control.

[21] Kabay, Mitch. Ph.D., CISSP, Network World Newsletter, 08/12/03

Appendix Resources that provide information about Identity Theft

Credit Bureau Contacts:

Trans Union -- http://www.transunion.com/index.jsp
Credit report: 1-800-916-8800
Fraud Line: 1-800-680-7289

Experian -- www.experian.com
Credit report: 1-888- 397-3742
Fraud Line: 1-888- 397-3742

Equifax -- www.equifax.com
Credit report: 1-800-685-1111
Fraud Line: 1-800-525-6285

GOOGLE, search on "Identity Theft"

"The Compleat Professional's Guide to Consumer Protection",
http://www.compleatprofessional.com/ConsumerProtectionGuide.html

"The Compleat Professional's Identity Theft Pages",
http://www.compleatprofessional.com/idtheft2.html

Sample Dispute Letters (Credit Bureau, Credit Card, Stolen Checks)
http://www.compleatprofessional.com/idtheft3.html

Federal Resources – Federal Trade Commission
http://www.ftc.gov or www.consumer.gov/idtheft

Identity Theft Data Clearinghouse
http://www.ftc.gov/bcp/conline/pubs/general/idtheftfact.htm

Privacy Rights Clearinghouse
www.privacyrights.org

Banking Agencies
FDIC – Federal Deposit Insurance Corporation, http://www.fdic.gov
Consumer Call Center (800) 934-3342

List of References

"National and State Trends in Fraud and Identity Theft", Federal Trade Commission, January 22, 2003.URL: http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf

Pettey, Christy. "Gartner Says Identity Theft Is Up Nearly 80 Percent", Gartner Inc., July 21, 2003. URL: http://www4.gartner.com/5_about/press_releases/pr21july2003a.jsp

Gadwa, Tess, "Identity theft hurts both bankers and customers", Charlotte Business Journal, June 16, 2003. URL: http://www.bizjournals.com/charlotte/stories/2003/06/16/focus2.html

InfoSec Briefs, "Florida Bank Breach Nets Online Banking Data". Information Security Magazine, April 22, 2002 - Vol. 4, No. 31. URL: http://infosecuritymag.techtarget.com/2002/apr/digest22.shtml

Hayes, Frank. "California Steamin'" Computerworld, June 03, 2002. URL: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,71657,00.html

Mientka, Matt. "Theft at Tri-West Exposes Patient Data", U.S. Medicine, February 2003. URL: http://www.usmedicine.com/article.cfm?articleID=589&issueID=47

McIntyre, David J. Jr., "Important Communications Concerning Information Theft", TriWest, April 2003. URL: http://www.triwest.com/announcement/

Ho, David, "Former hacker warns lawmakers about dangers to personal financial information", The Associated Press April 3, 2003 4:03 PM. URL: http://www.securityfocus.com/printable/news/3704

Poulsen, Kevin. "Guilty Plea in Kinko's Keystroke Caper", SecurityFocus, July 18, 2003. URL: www.securityfocus.com/news/6447

Mitnick, Kevin D., "Kevin Mitnick: Consumer vigilance can thwart high-tech crooks", The Mercury News, January 30, 2003. URL: http://www.siliconvalley.com/mld/siliconvalley/5070983.htm

Shain, Andrew. "Identity theft soars in U.S., Carolinas" The Charlotte Observer, January 23, 2003. URL: http://www.charlotte.com/mld/charlotte/news/columnists/mr_watchdog/5010346.htm

Leyden, John. "PDA security slackers, the lot of you" The Register, August 2, 2003. URL: http://www.theregister.co.uk/content/68/31621.html

Mitnick, Kevin D., “Kevin Mitnick: Consumer vigilance can thwart high-tech crooks”, The Mercury News, January 30, 2003. URL: http://www.siliconvalley.com/mld/siliconvalley/5070983.htm

Hulme, George V. “Companies Not Spending More on Security, Even with Increased Threats”, InternetWeek, Monday July 28, 2003 URL: http://www.internetweek.com/security02/showArticle.jhtml?articleID=12803291

Wright, Chris. CPP, “Identity Theft” ASIS Virtual Seminar, June 11, 2003

Kabay, Mitch. Ph.D., CISSP, “Insider attacks are a thorny problem.” Network World Newsletter, 08/12/03

“The Compleat Professional’s Guide to Consumer Protection”, URL: http://www.compleatprofessional.com/ConsumerProtectionGuide.html

“The Compleat Professional’s Identity Theft Pages”, URL: http://www.compleatprofessional.com/idtheft2.html

Sample Dispute Letters (Credit Bureau, Credit Card, Stolen Checks), URL: http://www.compleatprofessional.com/idtheft3.html

Federal Resources – Federal Trade Commission, URL: http://www.ftc.gov or www.consumer.gov/idtheft

Identity Theft Data Clearinghouse, URL: http://www.ftc.gov/bcp/conline/pubs/general/idtheftfact.htm

Privacy Rights Clearinghouse, URL: www.privacyrights.org