Information
and Privacy
Commissioner/
Ontario

Identity Theft:
Who's Using Your Name?

Ann Cavoukian, Ph.D.
Commissioner
June 1997

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of Peony Gandolfi in preparing this report.

Cette publication est également disponible en français.

Table of Contents

Introduction

Your new credit card fails to arrive in the mail. Months later, creditors you never heard of are repeatedly calling you and demanding payment for merchandise you never bought. Your credit history has always been perfect, but you are now being denied financing due to several delinquencies appearing on your credit report. Could this really be happening? Unfortunately, it could, and it has, to thousands of victims of a crime known as "identity theft."

As part of its mandate, the Office of the Information and Privacy Commissioner/Ontario (IPC) researches and comments on matters and trends relating to the issue of privacy protection. Identity theft, a crime resulting from the misappropriation and abuse of personal information, is a growing societal problem that deserves our attention. This report will look at what identity theft is, how it occurs, why people should be concerned, and what consumers and organizations can do to minimize their chances of being victimized. In particular, technological ways of protecting one's personal information will be explored.

A key underlying theme throughout the paper will be the idea that identity theft could be significantly reduced if more organizations adopt and follow fair information practices.[1]

What is identity theft?

Identity theft involves acquiring key pieces of someone's identifying information in order to impersonate them and commit various crimes in that person's name. Besides basic information like name, address and telephone number, identity thieves look for social insurance numbers, driver's license numbers, credit card and/or bank account numbers, as well as bank cards, telephone calling cards, birth certificates or passports. This information enables the identity thief to commit numerous forms of fraud: to go on spending sprees under the victim's name, to take over the victim's financial accounts, open new accounts, divert the victim's financial mail to the thief's address, apply for loans, credit cards, social benefits, rent apartments, establish services with utility companies, and more.

Why should I care?

Every year, thousands of people are victimized by identity thieves who steal millions from banks, retailers, and other creditors. In the United States alone, banks lost up to $90 million due to theft of identity in 1995.[2] Ultimately, every one of us must pay in the form of higher interest rates and service fees. U.S. officials are now describing identity theft as "the fastest growing crime in the nation," having identified it as "the leading form of consumer fraud."[3]

The theft of your identity can leave you with a poor credit rating and a ruined reputation which may take months or even years to correct. Meanwhile, due to your seemingly dreadful credit history, you may be denied jobs, loans, cheque-writing privileges, or the right to rent or buy accommodation. You may even risk false arrest and having your story viewed with suspicion.

A typical victim's financial losses alone due to identity theft have been calculated to be as high as $36,000. This includes telephone calls, notarized statements, loans, counselling fees, and lost wages resulting from time taken off work to deal with the problem. The figure does not include losses associated with paying off the thief's bills or being denied employment.[4]

On top of it all, victims are often surprised by the lack of co-operation from those they turn to for help. Police have at times denied that they are real victims and have even arrested them for the thief's crimes. Creditors and credit bureaus have accused victims of lying and dodging debts that they themselves had incurred. Credit bureaus have refused to remove false data from victims' records. In other words, if your identity gets stolen, you may essentially be left on your own to sort out the mess.

To make matters worse, many identity thieves are never caught, leaving them open to repeat this form of fraud again and again. What is really frightening, however, is how easy it is to steal someone's identity.

How can my identity get stolen?

Today's identity thieves are absconding with people's identifying data in much more sophisticated ways than through stolen wallets.[5] Some of these include:

- lurking around automatic teller machines (ATMs) and phone booths in order to capture PIN numbers (by watching through binoculars as the numbers are being entered, or more simply, by casting a watchful gaze over someone's shoulder). Travellers are a particularly favourite target;

- stealing mail from mailboxes or re-directing mail in an effort to collect credit cards, bank statements, credit card statements, pre-approved credit offers, tax information or other personal data. *Privacy Journal* has also pointed out "how automated credit bureaus freely accept an address change without confirming it or notifying the consumer who is the subject of the file. An imposter can easily have a retail store enter a change of address for a consumer whose identity the imposter has misappropriated, and that is what thousands of credit fraud perpetrators are doing …;"[6]

- illegally obtaining personal credit reports;

- setting up telemarketing schemes to elicit account numbers from unsuspecting consumers;

- accessing personal information accidentally sent to the wrong fax number, e-mail address or voice mailbox;

- scavenging through the garbage in search of credit card or loan applications, employer's files, and identification/authentication data such as login IDs and passwords. Similarly, thieves can search erased disks for any retrievable data;

- sending false messages on the Internet (spoofing) in an effort to collect private information. For example, posing as travel agents or other service providers, identity thieves can make off with your credit card number once it has been entered to purchase a ticket or service;

- sending e-mail using someone else's computer or e-mail address;[7]

- using various software programs such as "signals analysis" and "sniffer" programs to intercept financial data, passwords, addresses or other personal information being sent over networks;

- breaking into computer systems and gaining access to personal data. For example, names, addresses and credit card or social insurance/security numbers (SINs/SSNs) located in the databases of governments, financial organizations, employers, creditors, and credit bureaus can be downloaded by employees, former employees or external hackers. They can then sell the information or use it to open fraudulent accounts.

One security expert found that nearly 70 per cent of the websites he surveyed in December 1996 had "security lapses." Surveyed sites included banks, credit unions and government agencies.[8] Even more recently, a 14-year-old boy faced multiple charges after making $3000 worth of fraudulent purchases using a collection of debit card numbers that he had downloaded from the Internet.[9]

Identity theft case files

To provide readers with some understanding of the stress and aggravation that identity theft victims must endure, this section will outline several actual cases.

- A young secretary spent years trying to clear her name after a tax evader got hold of her SIN card, which the secretary had never received. The imposter used the secretary's name and SIN to move from job to job and collect unemployment insurance, health benefits, and maternity benefits — all without paying any taxes. The secretary was continually harassed by the government to settle "her" unpaid income taxes. Revenue Canada even garnisheed her bank account and earnings. The victim had to travel to each of the thief's six former employers, pleading for written statements to prove to tax officials that she herself had never worked there.[10]

- Using someone else's birth certificate and SIN card, a Vancouver man managed to obtain a photo ID card from the British Columbia government. He later used these three pieces of identification to open fraudulent bank accounts. He then proceeded to steal over $170,000 from several banks. This was done primarily by depositing bogus cheques into the accounts and immediately withdrawing the money through ATMs.[11]

- A Parisian woman whose ID card had been stolen, later found records indicating, much to her surprise, that she had been "married" for four years to a man she had never met. Once her "husband" had obtained French citizenship, he divorced her.[12]

- In a multi-victim fraud case, a teacher opened fraudulent credit card accounts and stole $43,000 worth of merchandise using the names and SSNs of his students and colleagues. The thief took the personal information from a class list and from pay stubs stolen out of campus mailboxes. The victims had to persuade the three national credit bureaus to delete the fraudulent data from their credit reports permanently. They also asked that creditors be alerted not to extend credit in their names unless they first confirmed that the victims themselves were the ones opening the accounts.[13]

- When a disabled telecommuter received her credit report from TRW,[14] it was seven pages long and had over 15 past due fraudulent accounts. There was also a judgment against her from an eviction that had taken place from an apartment. Later, she also received notice that she had defaulted on a loan. When she went to file criminal charges against her identity thief, the local sheriff's department said that the case would probably never be looked at because there were only two detectives and "it was not as important as a murder." TRW required that she prove to the 15 creditors herself that she had filed a criminal report by sending them notarized statements (at a cost of $10 each). None of the creditors prosecuted the thief, however, because they said it was not financially worthwhile to do so.[15]

- A year after her SSN was stolen, a former Californian was denied a mortgage because of numerous delinquent accounts appearing on her credit reports. After months of struggle, she succeeded in getting TRW to delete the false entries, only to see them reappear half a year later. Both Equifax and Trans Union misplaced her files and failed to remove as many as nine of the original 12 false entries. Adding insult to injury, Trans Union even hinted that the victim herself was the perpetrator.

  The victim's bad credit report also affected her husband, whose Visa card was consequently not renewed. She ended up suing the three credit bureaus for their abusive practices, testifying in court that creditors were calling her "at all hours of the day and night," and did not stop doing so until she moved to another state. Trans Union argued that systemic improvements to ensure maximum accuracy were costly and that credit bureaus had no way to differentiate between genuine victims and consumers who themselves were committing fraud.[16]

- After years of turmoil, a Texas couple won a $1.45 million lawsuit against their identity thief for invasion of privacy, defamation, and a host of other charges. However, given the offender's paltry assets, this may have been a hollow victory. The offender was a former loans officer who had obtained the couple's personal information by using the bank's credit terminal to access their credit report. Using their SSNs, address, and financial account information, the thief opened 21 finance, gas and other credit accounts totalling approximately $50,000. In a separate action, the couple also sued 13 credit bureaus, collection agencies, banks, stores and other creditors involved in the case, for violations of privacy, defamation, and other charges.[17]

- After her military security clearance was suddenly suspended, an army employee discovered that a relative had stolen her identity and opened several fraudulent accounts. In an effort to clear herself, she paid off $30,000 in fraudulent debts. She then quit her job to go to a new one paying $30,000 a year, but the offer was subsequently withdrawn after the prospective new employer saw her credit report. As a result, she was left jobless and unable to hold on to her apartment. She was also unable to obtain any sort of government assistance or financial assistance from the credit bureaus involved. Ultimately, she had to leave the country because the only employment she was able to secure was in Korea.[18]

- From an organization perspective, in a 1994 case, more than $300,000 was stolen from financial institutions using signatures and other personal information extracted from bank dumpsters. It has also been found that most credit report database intrusions may be traced back to authorized terminals, not external hackers.[19]

Don't be an easy target

Personal information is now so readily available in the networked world we live in that it may be impossible to eliminate identity theft entirely. Broader systemic and legislative reforms and the co-operative efforts of many including creditors, credit bureaus, law enforcement agencies and government, will be essential to combat the problem. In the meantime, however, there are several preventative measures that one can take, which may help to reduce one's chances of becoming a victim.[20] These are discussed in the sections that follow.

Low-tech methods

- Always store cards and documents containing sensitive personal data in a secure place. Sensitive data may include: credit cards, social insurance number, driver's license, bank account numbers, pre-approved credit applications, address, date of birth, tax records, passports, utility and phone bills. Shred (or tear up) all such documents prior to their disposal. Consider installing a secure mailbox.

- Obtain a copy of your credit report regularly to check for fraudulent accounts, false address changes and other fraudulent information. Report all errors to the credit bureau and have them immediately corrected.

- Keep and carry as few cards as possible. After completing a credit card transaction, make sure that the card you get back is your own. Tear up the carbon copies. Cancel all unused credit accounts.

- Carefully review all bank and credit card statements, cancelled cheques, phone and utility bills, as soon as you get them. Report any discrepancies immediately. If any regularly expected statements do not arrive on time, contact both the post office and your creditors to ensure that your mail isn't being diverted to another location.

- If you applied for a new credit card and it hasn't arrived on time, call the bank or credit card company involved. Report all lost or stolen cards right away.

- Do not provide your address in conjunction with the use of your credit card. Your cheques should not have your driver's license preprinted on them. Also, avoid, unless legally required, writing your credit card number or SIN/SSN on your cheques.

- Avoid giving out your credit card number or other personal information over the telephone unless you have a trusted business relationship with the company and **you** have initiated the call. In particular, do not provide personal information over unencrypted wireless communications such as cordless or cellular phones. (Even baby monitors can broadcast your personal communications to eavesdroppers)

- Some card issuers call customers if they notice unusual charges on their cards. You should never give out any information about your account over the telephone except your confirmation of what has already occurred. If you have any doubts, hang up and contact the card issuer directly. Similarly, do not provide any personal information to unfamiliar callers claiming to be from your financial institution or brokerage firm. Ask for the person's name, hang up, and then call them back.[21]

- PINs and passwords should **never** be written down or revealed to **anyone**. Choose ones that cannot be easily guessed, and change them regularly. When conducting banking or investment transactions over the telephone, make sure that no one can hear you or be in a position to detect your PIN or password as it is being entered.

- If you should discover that your personal information has been placed in an online directory or a searchable database, try to have it removed. For example, one major U.S. database company has been selling names, addresses, birth dates, unlisted phone numbers and other data on millions of people over the Internet. Even SSNs were initially being offered until hundreds of people complained.[22]

- Do not create online profiles containing your personal information — it could be used by someone else to impersonate you.

- Beware of start-up software that asks for registration information including your credit card number and SIN/SSN, to upload "for billing purposes."

High-tech privacy-enhancing technologies

The world's expanding electronic infrastructure has enabled fraud to flourish exponentially. In our increasingly technology-driven world, the use of privacy enhancing technologies can be a critical complement to the safe information practices outlined above. Privacy-enhancing technologies, or "PETs" refer to technologies that transmit your personal information in encrypted form, or otherwise enable you to conduct electronic transactions in an anonymous manner by minimizing or eliminating the collection of personally identifying data. Encryption is a mathematical process of encoding information so that it cannot be read without possession of the correct "key" necessary to decode it.

When transmitting information via a communications network, you should assume that your communications are not private, unless that information is encrypted.[23] Without strong encryption, Personal Computer (PC) banking, online investing, online shopping, sending and receiving e-mails, and processing commercial or credit applications over the Internet can expose personal information to unauthorized disclosure, theft and alteration.

The most rapidly increasing area for the commission of identity theft is said to be on the Internet.[24] This should not be surprising in light of the opportunities the Net provides for the collection (and abuse) of personal information, on a scale not previously possible. It has been predicted that by the year 2000, 30% of all North American commerce will take place in cyberspace, and worldwide Internet commerce revenues could reach $200 billion U.S.[25] With this will come ever-growing opportunities for identity theft.

A wide variety of PETs are available today. The following section will discuss some of the key ones. Combining additional security features with PETs, such as passwords and encryption, will further increase security and privacy.

Identity protectors

Identity protectors, such as blind signatures and digital pseudonyms, are mathematical sequences based on encryption techniques that enable users to conduct electronic transactions in an anonymous manner, while at the same time, allowing the service provider to verify the user's authenticity and eligibility for benefits and services.

Digital signatures are the electronic equivalent of handwritten signatures. Like handwritten signatures, which are used to authenticate paper documents, digital signatures placed on electronic documents serve the same purpose. Digital signatures can protect against spoofing and message forgeries, but they offer little privacy since they are intended to identify the originating party. **"Blind" signatures**, developed by David Chaum of DigiCash,[26] go one step further and provide the same authentication as digital signatures, but do so without revealing

the originator's identity, thus rendering it "blind." The advantage of such a system is that it preserves the authenticating features of digital signatures, while protecting one's privacy at the same time.

A digital pseudonym is an alternative pseudo-identity that a user may choose to assume in order to engage in a particular transaction, communication or service in an anonymous manner. One can select a different pseudonym for every service provider, or for use each time that a particular service is used.

For a more in-depth discussion on these and other PETs, readers may wish to see the joint report by the IPC and the Netherlands Data Protection Authority entitled, *Privacy-Enhancing Technologies: The Path to Anonymity.* Released in the fall of 1995, this paper provides a detailed analysis of advanced encryption techniques that allow for authenticated yet anonymous transactions, such as digital signatures, blind signatures, digital pseudonyms and trusted third parties.

Data encryption

Several powerful encryption programs are readily available at no charge through Internet service providers as stand-alone programs or as part of packages providing file or e-mail encryption and digital signatures. For example, one powerful public key encryption system, PGP, (Pretty Good Privacy) developed by Philip Zimmermann[27], may be used to encrypt e-mail or computer files.

An alternative to PGP is the Kerberos authentication scheme, which may be used to secure specific messages or to protect the server's protocol level. Privacy Enhanced Mail (PEM) may also be used to encrypt sensitive data before sending it over the Net.

Various technologies for encrypting credit card numbers for use in making payments over the Internet are now being developed, such as the Secure Electronic Transaction (SET) standard. Internet communications and transactions may also be encrypted using Secure Hypertext Transfer Protocol (S-HTTP) and Secure Sockets Layer (SSL).

Anonymous remailers

When you send a letter through the regular mail, you can remain anonymous simply by not putting your return address on the envelope. On the Net, however, your address is automatically forwarded, unless you take steps to channel your e-mail through an "anonymous remailer." An anonymous remailer is a free service that strips the identifying header from your e-mail before sending it on its way. For a range of anonymous services on the Net, take a look at: www.anonymizer.com.

Anonymous payment mechanisms

Electronic payments can take place anonymously through the use of smart cards such as stored-value cards, pre-paid transponders for electronic toll roads, or electronic cash involving digitally encoded money. Developed to serve as the electronic equivalent of cash, digital cash systems are designed so that transactions cannot be traced back to the purchaser, yet the payee is still assured of the payment's authenticity.

Other PETs

- Computer security hardware and software, such as access control software and programs that prevent unauthorized online access to your computer, are available. Software that will turn an ordinary PC into a secure telephone can be downloaded from the Internet at no cost.

- Tokens are unique identification strings which may be stored on smart cards. Tokens may be used in combination with passwords/PINs, card readers, and at times, encryption.

- Special privacy enhancing printers have mailboxes and collators with several locking trays, each of which can be assigned a password. Users can send their print jobs to their own secure output trays.

- Other PETs involve anonymous one-time signatures, protected passwords, one-time passwords, tiered levels of entry, partitioned access according to file sensitivity, and call blocking. One Internet service provider even offers free, anonymous Internet accounts, pseudonymous servers and "Anonymizer" services that allow users to surf the World Wide Web "with complete anonymity."[28]

While privacy-enhancing technologies are available today, with new ones appearing on a regular basis, they are not yet widely known or used. Widespread implementation — throughout business, government and private industry — will only come about through consumer demand. By making yourself heard today, you can help to secure a more privacy-respectful electronic future for everyone.

What organizations can do

Organizations have an equal, if not larger role to play than consumers when it comes to preventing identity theft. *Privacy Times* reported that, "theft-of-identity cases are a direct response to criminals' increasing willingness to take advantage of inadequate security for personal financial data stored in credit bureaus and other large databases."[29] We make the following recommendations (especially applicable to financial and public sector organizations):

- When information systems are being designed or upgraded, consider how user-privacy could best be protected. Explore the application of PETs and ensure appropriate security measures are taken. Ask: How much personally identifiable information is actually required for this system to function? Once this has been determined, collect and retain only the minimum.

- Absent legislation, adopt a privacy policy for your organization and train all employees on responsible information handling practices. The Canadian Standards Association's *Model Code for the Protection of Personal Information* (CAN/CSA Q830-96) is an excellent code for use by private sector organizations.

- Exercise considerable caution when collecting, using, and disclosing SINs/SSNs. Do not ask for these numbers if not required by law. Stolen SSNs result in thousands of cases of identity credit theft each month. Persons lacking proper documentation may steal these numbers in order to obtain legal identities. A SIN/SSN can also be used to impersonate someone over the telephone or online in order to retrieve personal data about the individual, such as tax information. Avoid the use of SINs/SSNs as client/employee/student identification numbers.

- Consider storing the textual portion of a record (i.e., clinical encounter data in a health record) separately without any personal identifiers; retain identifying information (such as name, SIN, address, date of birth) in a separate database, preferably in encrypted form. Organizations can also separate the flow of personal data from other transactional data in their information systems.

- If you are a credit bureau, provide your customers with a free credit report annually, upon request, and notify customers whenever their credit reports have been accessed.

- Require proof of identity and check it carefully when a customer applies for credit or a change of address. Credit bureaus should not accept client address changes from creditors without first verifying them with the consumer involved.

- Make use of artificial intelligence programs to identify patterns of fraudulent use and notify consumers of any suspected fraudulent activity. Creditors have a responsibility to report fraudulent accounts to the police and ensure that they are deleted from a bona fide client's record.

- Do not use customers' personal information for "secondary purposes" such as adding it to mailing lists or selling/leasing it to third parties, without the explicit consent of the individual concerned.

- Store and dispose of personal information accurately and securely, especially credit and loan application forms.

- Avoid using date of birth or mother's maiden name as passwords for financial accounts. This type of information is often quite easy for others to acquire.

- Do not put scanned copies of anyone's signatures on your organization's website.

What if it happens to me?

Identity theft is a multi-faceted problem that is unlikely to go away. If you should become a victim, you will need to take action quickly:[30]

- Notify the police, banks, and creditors immediately. Obtain a copy of your police report (as evidence of the fraud having been perpetrated). Cancel all existing credit cards, accounts, passwords and PINs, and replace them with entirely new ones.
- Call the credit bureaus and ask each to attach a fraud alert and victim's statement to your report. Ask creditors to call you prior to adding any new items to your report. Have all corrections forwarded to anyone who has received your credit report within the past two years. Ask for a free copy of your report after three months.
- Contact the post office if you suspect that an identity thief has filed a change of address form for your name, and is diverting your mail to another address.
- Alert all utility companies that someone has been using your identity fraudulently and inform the appropriate authorities that someone may be abusing your SIN and/or driver's license number.
- Take action to have any criminal or civil judgments against you that may have resulted from your identity thief's actions, permanently removed.
- Keep a log of all your contacts and make copies of all documents. You may also wish to contact a privacy or consumer advocacy group.[31]
- In some cases, it may be advisable to seek the assistance of a lawyer.

Conclusion

The theft of your identity can pose a serious threat to your privacy and has the potential to make your life very difficult. This paper has provided a brief look at some of the factors contributing to this crime, as well as possible ways of preventing it, and failing that, dealing with it.

The problem of identity theft must be fought on several fronts. Applying fair information practices is a good place to start. Moreover, as computers and networks make it easier and easier to gather your personal information, technological methods of protecting privacy will become increasingly important. Organizations that can offer their clients greater informational privacy may well obtain a competitive advantage over those who fail to do so. If enough people demand it, we may find that in the future, anonymous transactions (which authenticate identity in a blind manner), will become the standard, as opposed to the identifiable transactions of the present day. De-identifying information may well pave the way to a future which includes privacy.

Notes

1. In 1980, the OECD (Organisation for Economic Co-operation and Development) developed a set of internationally-recognized principles for the responsible treatment of personal information commonly known as the Code of Fair Information Practices. The Code sets out several restrictions and standards concerning the collection, retention, use, disclosure and security of personal information. More recently, the Canadian Standards Association has developed an updated Code called the "Model Code for the Protection of Personal Information."

   OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* September 1980.

   Canadian Standards Association, CAN/CSA-Q830-96 *Model Code for the Protection of Personal Information*. A National Standard of Canada. March 1996.

2. U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August 1996, pp. 14-15.

3. Ibid., p. 14.

   "Scam Artists Await Unwary Travellers," *Toronto Star*, December 2, 1995, p. F19.

4. U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August 1996, pp. 15-16.

5. U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August 1996.

   Privacy Rights Clearinghouse, "Coping With Identity Theft: What to Do When an Imposter Strikes," Fact Sheet No. 17, May 1995.

6. "Fraud Happens: Here's How," *Privacy Journal*, July 1996, pp. 5-6.

7. Marta Gold, "Easy E-mail Easy to Open — PC Privacy Just an Illusion," *Southam Newspapers*, February 15, 1997.

8. "Web Security Studied," *Globe & Mail*, January 1, 1997, p. B6.

9. "Cops Bust Kid Who Found Credit Numbers on 'Net' Site," *Privacy Times*, January 16, 997, p. 3.

10. Geoff Baker, "Imposter Makes Life Hell for Secretary," *The Gazette (Montreal)*, November 5, 1992, p. A1.

11. Bob Stall, "He Conned His Way Into Hearts," *The Province (Vancouver)*, November 5, 1995, p. A8.

12. "Marriage Was Surprise to Her: Wed 4 Years to Unknown Man," *The Province (Vancouver)*, November 10, 1995, p. A43.

13. "'Theft of Identity' Rises to Thousands a Day," *Privacy Journal*, February 1996, pp. 1, 4.

14. TRW is one of the three major American credit bureaux (Equifax and Trans Union are the other two). TRW changed its name to Experian in the summer of 1996. See Robert Ellis Smith, "Privacy: The Untold Stories," *Wired*, February 1997, p. 96.

15. U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August 1996, pp. 3-5.

16. "Going Against All Three," *Privacy Journal*, May 1996, pp. 4-5.

    "L.A. Jury Identifies With 'Theft of Identity' Victim," *Privacy Journal*, August 1996, pp. 1, 4.

17. "Biggest Yet! Texas Couple Wins $1.45 Million for 'ID Theft'," *Privacy Times*, October 5, 1995, pp. 1-3.

18. The Consumer X -Files pp. 6-7

19. "Flap Forces Connecticut Banks to Review Data Security Policies," *Privacy Times*, July 20, 1995, p. 2.

    U.S. Public Interest Research Group, *Theft of Identity: The Consumer X-Files*, August 1996, p. 31.

20. Privacy Rights Clearinghouse, "Coping With Identity Theft: What to Do When an Imposter Strikes," Fact Sheet No. 17, May 1995.

    Privacy Rights Clearinghouse, "What to Do When Your Wallet is Stolen," Fact Sheet No. 13, June 1994.

    PIRG Consumer Watchdog Fact Sheet: "What Can Consumers Do to Avoid Becoming Theft of Identity Victims?"

21. Royal Bank Consumer Information brochure: "Straight Talk About Safeguarding Against Financial Fraud."

    An impersonator can also cause problems by sending you a false message using someone else's e-mail address. It is a good idea to confirm e-mails with a reply to ensure that they are genuine.

22. "SSNs For Sale On-Line," *Privacy Journal*, June 1996, p. 4.

    "Lexis-Nexis Spin: Did it Work?" *Privacy Journal*, September 1996, p. 7.

23. Note that while encryption can significantly enhance security and privacy, it cannot guarantee it.

24. "Scam Artists Await Unwary Travellers," *Toronto Star*, December 2, 1995, p. F19.

25. Patrick Brethour, "Is This the Year for Internet Commerce?" *Globe & Mail*, January 15, 1997, p. B12.

26. David Chaum*: "Achieving Electronic Privacy,"* Scientific American, August 1992.

27. Steven Levy, "Crypto Rebels," Wired, May/June 1993.

28. Sandy Sandfort, "Making Privacy Pay," *Wired*, January 1997.

29. "Biggest Yet! Texas Couple Wins $1.45 Million for 'ID Theft'," *Privacy Times*, October 5, 1995, p. 2.

30. PIRG Consumer Watchdog Fact Sheet: "A Checklist For Theft of Identity Victims."

    Privacy Rights Clearinghouse, "Coping With Identity Theft: What to Do When an Imposter Strikes," Fact Sheet No. 17, May 1995.

31. For example, California's Privacy Rights Clearinghouse (619-298-3396) or Public Interest Research Group (310-397-3404).