Identity Theft and Fraud

Identity theft is a term that refers to crimes in which someone wrongfully obtains and uses another person's ***personal data*** (i.e., name, date of birth, social security number, driver's license number, and their financial identity – credit card, and/or bank account) in some way that invokes fraud or deception, typically for economic gain (to obtain money or goods/services). Criminals also use identity theft to fraudulently obtain identification cards, driver's licenses, birth certificates, social security numbers, travel visas and other official government papers.

Identity theft is one of the fastest growing crimes in America. The Federal Trade Commission (FTC) conducted a random telephone survey of 4,057 adults in the spring of 2003. Of those persons surveyed, 4.67% said they were the victims of identity theft in 2002. Applied to the entire U.S. population, this translates into 9.9 million victims. The FTC estimates there were 6.9 million identity theft victims in 2001 and 3.4 million victims in 2000.

How Identity Theft Is Committed

Identity theft occurs in a variety of both low and high tech means. The following are some of the ways it occurs:

- **Business Record Theft:** They obtain your personal data from businesses or institutions by stealing files from offices where you are a customer, employee, patient or student; or by bribing an employee who has access to your files; or even "hacking" into the organization's computer files. The use of temporary employees by many businesses contributes to the problem. Medical records are an abundant source of revealing personal data.
- **Shoulder Surfing:** In public places, the identity thief watches from a nearby location while you write a check at a checkout line, or use a telephone calling card or credit card. They are skilled at memorizing these numbers and information.
- **Dumpster Diving:** Some identity thieves engage in "dumpster diving" – going through your trash, or the trash of businesses or even landfills – to obtain copies of your checks, credit card or bank statements, or other records that typically bear your name, address or possibly telephone number.
- **Under the Color of Authority:** They fraudulently obtain credit reports by posing as landlord, employers or others who have a legitimate need/right to the information.
- **Skimming:** They steal your credit/debit card account numbers as your card is processed at a restaurant, store or other business, using a special data collection/storage device known as a "skimmer."
- **Steal Mail:** By stealing your mail, the identity thieves may obtain your bank and credit card statement, pre-approved credit offers, new checks, or tax information.
- **Theft of Wallets and Purses:** They may simply steal wallets or purses containing identification and credit and bank cards.
- **Diversion of Mail:** The identity thief may complete a "change of address form" to divert your mail to another location.
- **"The Information Highway":** Referred to as "the information highway," they may obtain information you share over the Internet.

- **"Scamming:**" Often through email, they scam information by posing as legitimate companies or government agencies.

How Do Identity Thieves Commit Fraud?

Having obtained someone else's personal data and information, identity thieves can employ numerous means to commit fraud. Such means include the following:

- They may go on spending sprees, using stolen credit or debit account numbers to buy "big ticket" items like computers, TV's or other electronic equipment.
- They may open a new credit card account, using the fraudulently obtained name, date of birth and SSN. When they use the credit card and don't pay the bills, the delinquent account is reported on the victim's credit report.
- Being in possession of a stolen credit card, they may call the credit card issuer and ask to change the mailing address on the account. The victim doesn't receive the bills and the identity thief uses the stolen or fraudulently-obtained card.
- They may establish cellular phone service in the victim's name.
- They may open a bank account in the victim's name and write bad checks on that account.
- They may purchase a motor vehicle by taking out an auto loan in the victim's name.
- Using a stolen debit card, they may drain the victim's bank account.

Identity Theft Prevention

- Minimize the number of credit cards and identification carried in a wallet or purse. Don't carry bank account numbers, PIN's, birth certificates or passports in a wallet or purse, except when needed.
- Avoid carrying more blank checks than actually needed. An identity thief can fraudulently use the sensitive information often pre-printed on checks (address, bank account number and telephone number). *Do not have your Social Security number pre-printed on personal checks.*
- Keep good backup information about your accounts, in the event your wallet or purse is stolen or lost.
- Memorize all your passwords. Do not record them on anything in your wallet or purse.
- When you go on vacation, take along a list of toll-free telephone numbers for your banking and credit card companies – not your card numbers – and keep the list in a safe place other than your wallet or purse.
- Consider canceling any credit cards you don't really need or haven't used in six months.
- Never provide personal information (Social Security number, credit card number, address, etc.) over the telephone unless you initiate the call and are familiar or acquainted with the business.
- Destroy – preferably shred – credit card applications you receive in the mail and don't use. Also shred credit card slips, cancelled checks, and telephone bills.
- Review your credit card bills and your checking account statements as soon as they are received, to ensure that no fraudulent activity has taken place.
- Obtain a copy of your credit report from each of the three major credit bureaus at least once a year to check for errors.
- Be careful at ATM's and using phone cards. "Shoulder Surfers" can obtain your "PIN Number" and get access to your accounts.

- Do not put checks in the mail from your home mailbox. Drop them off at a U.S. Mailbox or the U.S. Post Office. Mail theft is common. It is easy to change the name of the recipient on the check with an acid wash.
- When you order new credit cards in the mail, or your previous ones have expired, watch the calendar to make sure you get the card within the appropriate time, If it is not received by a certain date, call the credit card granter immediately and find out if the card was sent. Find out if a change of address was filed if you don't receive the card or billing statement.
- Obtain a post office box, or locked mailbox, if you can.
- Consider making your telephone number an unlisted number or just use an initial instead of full first name in the directory.
- Obtain credit cards and business cards with your picture on them, whenever possible.
- If someone you don't know calls you on the telephone and offers you the chance to receive a "major" credit card, a prize, or other valuable item, but asks you for personal data –such as your Social Security number, credit card number, or mother's maiden name – ask them to send you a written application form, if they won't do it, tell them you are not interested and hang up.
- When you are traveling, have your mail held at your local post office, or ask someone you know well and trust to collect and hold your mail while you are away.
- If your monthly credit card or bank statements do not arrive at the normal time of the month, call the financial institution or credit card company immediately and ask about it.
- Always take credit card and ATM receipts with you. ***Never*** toss them in a public trash container.
- Remove your name from the marketing lists of the three major credit reporting bureaus; i.e., Equifax, Experian (formerly TRW) and Trans Union. This will limit the number of pre-approved offers of credit received.
- Do not carry your SSN card; keep it in a safe place.
- When creating passwords and PIN's, do not use the last four digits of your social security number, your birth date, middle name, mother's maiden name, address, consecutive numbers or anything else easily discovered by identity thieves.
- Order your Social Security Earnings and Benefits Statement once a year to check for fraud.
- When you order new checks, do not have them sent to your home. Have them sent to a post office box or arrange to pick them up at your bank.
- Pay bills with an electronic bill payment service.
- Sign up for Direct Marketing Association Mail Preference Service and the Telephone Preference Service. By doing this, your name is added to computerized name deletion lists used by nationwide marketers.

  Direct Marketing Association
  Mail Preference Service
  P.O. Box 908
  Farmington, NY 11735-9008

  This will put you in a "delete" file, which is sent to subscribing organizations (approximately 70% of direct marketers) four times a year. Your name remains on the delete list for five years. This should result in a significant reduction in catalogs, magazine offers, credit card solicitations sweepstakes and other national advertising mail.

- When you fill out a loan application, find out how the company disposes of them. If you are not convinced they store them in locked files and/or shred them, take your business elsewhere.
- Encourage businesses you patronize to truncate (no more than the last five digits of a credit card number appears on a transaction slip) credit cards or take your business elsewhere.

What to Do if You Are the Victim of Identity Theft

Persons who have been the victim of identity theft or fraud should take the following measures:

- In dealing with authorities and financial institution, do the following:

  - ✓ Act quickly and assertively to minimize the damage.
  - ✓ Keep a log of all conversations, dates, names and telephone numbers.
  - ✓ Confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.

- Report the crime to the appropriate local **law enforcement agency.** Provide them with as much documented evidence as possible. Obtain a copy of the police report. Obtain the telephone number of your fraud investigator and provide it to creditors and others who require verification of your case.
- Immediately contact the fraud units of the three **credit reporting companies –** Experian (formerly TRW), Equifax and Trans Union.

  Ex**perian** (formerly TRW)
  P.O. Box 2104
  Allen, TX 75013-2104
  Fraud # (800) 525-7195
  Web site: www.eperian.com
  Equifax
  P.O. Box 105873
  Atlanta, GA 30348
  Fraud # (800) 525-6285
  Web site: www.equifax.com
  Trans Union Corporation
  P.O. Box 34012
  Fullerton, CA 92834
  Fraud # (800) 680-7289
  Web site: www.tuc.com

- **Contact all creditors** immediately with whom your name has been used fraudulently – by phone and in writing. Obtain replacement cards with new account numbers for those that have been fraudulently used. Ask that old accounts be processed as "account closed at consumer's request." Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report such fraudulent activity immediately to credit grantors.
- If you have had **checks** stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks you are unsure of. Cancel your checking and savings accounts and obtain new account numbers.

- If your **ATM card** has been stolen or compromised, obtain a new card, account number and password. Do not use your old password. When creating a password, don't use common numbers like the last four digits of your Social Security number or your birth date.
- **Social Security Number Misuse**. Call the Social Security Administration to report fraudulent use of your social security number. As a last resort, you might want to change your Social Security number. The SSA will only change it if you fit their fraud victim criteria. Order a copy of your Social Security Earnings and Benefits Statement and check it for accuracy.
- If you have a **passport**, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.
- If an identity thief has stolen a victim's mail or has falsified change of address forms, the victim should contact the local postal inspector. The local post office will have the telephone number of the nearest postal inspection services officer or it can be found at the postal service website at www.usps.gov/websites/depart/inspect.
- You may want to change your driver license number if someone is using your license as identification to pass bad checks. Call the Department of Motor Vehicles (DMV) to see if another license has been issued in your name. Place a fraud alert in your DMB records. Go to your local DMV office to request a new driver license number.
- You may want to consult an attorney to determine legal action to take against creditors and /or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor.
- Immediately contact the fraud unit of one of the three credit reporting bureaus.

  - ✓ Equifax
    800-525-6285
  - ✓ Experian (formerly TRW)
    888-397-3742
  - ✓ Trans Union
    800-680-7289

  In the spring of 2003, these three major credit-reporting companies initiated a fraud alert sharing service in which a single fraud notification to one will be shared with the two others.

  Report the theft of your credit cards or numbers. Ask that your account be flagged. Ask the credit bureaus in writing to provide you with free copies every few months so you can monitor your credit report. In 1999, a law became effective requiring credit reporting bureaus to provide credit reports free of charge to victims of identity theft.

Federal Trade Commission

The Federal Trade Commission (FTC) is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not prosecute criminal cases, it helps victims of identity theft by providing them with information to help resolve the financial and other problems that can result from identity theft. The FTC may refer victim complaints to other appropriate government agencies or private organizations for assistance.

If someone has been the victim of identity theft, they can contact the FTC to file a complaint via the following:

FTC Toll-free Telephone Identity Theft
Hotline: 1-877-IDTHEFT (438-4338)

By Mail: Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Internet: www.consumer.gov/idtheft

The FTC produces a number of good identity theft related publications:

- *Avoiding Credit and Charge Card Fraud*
- *Credit and ATM Cards: What To Do If They Are Lost or Stolen*
- *Identity Crises: What To Do If Your Identity Is Stolen*
- *Identity Thieves Can Ruin Your Good Name: Tips for Avoiding Identity Theft*

The FTC has published an excellent comprehensive booklet about identity theft entitled, "When Bad Things Happen in Your Name." This downloadable booklet can be found in the FTC's Internet website (www.ftc.gov).

Possible Identity Theft Crime Prevention Initiatives

The primary deterrent to identity theft is public information and awareness. Citizens need to be aware of the extent of the problem, how identity theft is committed, steps or measures they can take to minimize the chance of being victimized and what they should do if they are the victim of identity theft.

The following are possible identity theft crime prevention initiatives local law enforcement agencies can adopt:

- Work with local media (newspapers, radio and TV) to publicize the problem and appropriate preventive measures.
- Provide information about identity theft on the law enforcement agencies' Internet website.
- Develop an identity theft training bulletin for law enforcement officers.
- Work with local financial institutions to develop an identity theft brochure for them to distribute to their customers.
- Speak about identity theft to local civic organizations – Rotary, Optimists, Lions Clubs, etc.
- Work with the local Better Business Bureau to disseminate identity theft information.
- Suggest that School Resource Officers teach identity theft prevention.