Identity Theft and Fraud

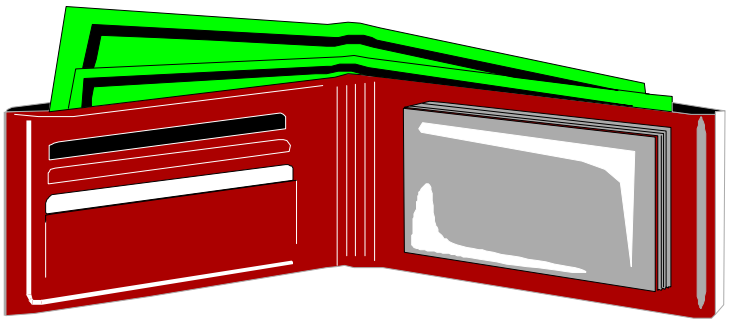
Identity theft and **identity fraud** are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Identity theft is one of the fastest growing crimes in America, affecting approximately 500,000 new victims each year.

How Identity Theft or Fraud is Committed

- In public places, criminals may engage in "shoulder surfing" – watching you from a nearby location as you punch in your telephone calling card number or credit card number.

- Some criminals engage in "dumpster diving" – going through your garbage cans or a commercial dumpster or trash bin – to obtain copies of your checks, credit card or bank statements, or other records that typically bear your name, address or even your telephone number.



- Criminals may simply steal your wallet or purse.

- If you have received applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge.

- Criminals may open up a new credit card account, using your name, date of birth and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on *your* credit report.

- They may establish a cellular phone service in your name.

- They may open a bank account in your name and write bad checks on that account.

- Criminals may pilfer bank statements, credit card statements, pre-approved credit card applications, etc., from your mailbox.

Prevention of Identity Theft or Fraud

- Limit the amount of confidential or personal information you carry in your wallet or purse. Do not carry bank account number, personal identification numbers (PINs), passports, birth certificates or Social Security cards.

- Avoid carrying more blank checks than you actually need. A criminal can fraudulently use the sensitive information often pre-printed on you checks (address, bank account number, and telephone number). *Do not have your Social Security number pre-printed on your checks.*

- Keep good backup information about your accounts, in case your wallet or purse is lost or stolen.

- 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.

- 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 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.

- Do not put your telephone number on your checks.

- 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.

What to Do if You Are the Victim of Identity Theft or Fraud

Those persons who have been the victim of identity theft or fraud should take the following measures. In dealing with authorities and financial institutions, they should keep a log of all conversations, including dates, names and phone 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 –** Eperian (formerly TRW), Equifax and Trans Union.

  ✓ E**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 your 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.