



Identity Theft

February 2004

A nationwide survey released by the Federal Trade Commission in September 2003 found that more than 9.9 million Americans were the victims of identity theft last year alone, collectively losing more than \$5 billion. In addition, businesses lost more than \$50 billion as a result of identity theft. According to the Colorado Attorney General's newly launched Identity Theft Prevention web page, identity theft is the fastest growing crime in America.

Getting access to personal and financial information is easier than ever. Public records contain information about birth and marriage dates and property ownership, and legitimate companies collect and sell records relating to licenses, marriage and divorces, judgments, liens, bankruptcies, and more.

Identity thieves have numerous methods to acquire more social security numbers, bank or credit card numbers, calling card accounts, and other private and personal information:

- Stealing a purse or wallet
- Stealing mail left for pickup or delivered to your home
- Diverting mail to another mailbox using a false change-of-address request
- Digging through dumpsters or garbage cans looking for personal or financial information
- Watching over your shoulder as you enter your PIN or long distance calling card number
- Calling to "verify" account information or "confirm" an enrollment or subscription
- Using false or misleading Internet sites to collect personal or financial information
- Purchasing personal information from unscrupulous employees at companies where you do business
- Burglarizing businesses looking for computers or files clients' personal/financial information
- Hacking into business or personal computers to steal private files and financial information
- Sending email or programming popup messages that appear to come from your credit card company or Internet service provider and claiming that because of a problem with your account you must resubmit your credit card and/or other personal information

Preventing Identity Theft

Be careful about providing your personal or financial information to anyone. The Attorney General's office gives this advice:

- Never provide personal identifying or financial information over the phone if you did not initiate the call. This includes callers selling services as well as charitable solicitors. Banks, credit card companies, telephone companies, and other legitimate creditors do not call to "verify" account numbers.
- Never provide personal identifying or financial information over the phone to anyone claiming to represent a contest or sweepstakes promotion. It is illegal to market a foreign lottery in the United States.
- Never carry your social security card in your purse or wallet.
- Never have your social security number printed on your checks, driver's license, or other financial documents. If a bank, health care provider, or other entity uses your social security number for account or client identification (or prints these numbers on cards you must carry with you), call or write the company and ask that a different ID number be issued.
- Never respond to email or pop-up messages on your computer claiming some problem with a credit card or Internet, or other account. Promptly contact your credit card company or ISP to assure there are no problems with your account.
- Purchase a simple cross-cut shredder (the kind that creates confetti, not long strips) and get in the habit of shredding all personal and financial documents you discard. Shred all pre-approved credit card and loan applications (and any negotiable checks that are sometimes attached). Also shred bills and invoices after you have paid them, bank statements (including cancelled checks), investment or retirement account statements, medical statements of any kind, and any other documents containing information about you or your finances.
- Place password protection on all credit card accounts that allow it. Do not use common numbers or personal information (like birth dates or part of your social security number) or commonly chosen words (like a child's name, spouse's name, or pet's name) for passwords.

Corporate Office
3033 East First Avenue
Suite 600
Denver, CO 80206
303-321-1880
Fax 303-331-0272

Please visit our website
for a complete list of
office locations:
www.LTGC.com

- Control access to your credit history. Remove your name from mailing lists for pre-approved lines of credit by participating in the credit bureaus' "Opt-Out" program. Call 1-888-5-OPT-OUT (1-888-567-8688) to enroll. They will request your social security number to verify you are the one making the request, but this is a legitimate use of that information.
- Be careful with your incoming and outgoing mail. If you don't have a secure, locked mailbox, mail your bills from a curbside public mailbox or directly at your local post office. Never leave your outgoing mail in an unsecured mailbox overnight. If you are planning to be away from home on vacation, arrange for your post office to hold your mail.
- Arrange to pick up new checks at your bank. Never have boxes of new checks delivered to your home. (They do not fit in many mail slots, so your postal carrier may leave them on your doorstep.)
- Take all credit cards and ATM receipts with you after you pay for goods and services and destroy them in your cross-cut shredder when you get home.
- Write to your bank, insurance company, and other financial institutions you do business with and ask them not to share your customer information with unaffiliated third parties.
- Remove your name from national direct mail advertising lists by sending your name and address together with your written request to: DMA Mail Preference Service, Attn: Dept. 12059580, Direct Marketing Association, P.O. Box 282, Carmel, NY 10512.
- To dramatically reduce telephone solicitations, place your name on the Colorado No-Call List by calling 1-888-249-9097. You can also register online at <http://www.coloradonocall.com>. You can also participate in the national no-call registry by calling 1-888-382-1222 or registering online at <http://www.donotcall.gov>.

More tips to help prevent identity theft:

- When ordering checks, have only your initials and last name printed on them. That way, if someone steals your checkbook, they will not know how you sign your name—but your bank will know if they are signed incorrectly.
- When you write checks to pay your credit card account, do not write the complete account number in the "memo" line. Instead, note only the last four numbers. The credit card company will know the rest of the number, but anyone who handles your checks (or steals your mail) will not have a complete card number.
- Instead of having your home address printed on your checks, use a work address or P.O. num-

ber. If you have a work number, use that on your checks instead of a home number.

- Place the contents of your wallet on a photocopy machine and take a copy of both front and back of every card. This way you will know what you have in your wallet, including all account numbers and cancellation phone numbers in case your wallet is stolen. Keep the photocopy in a safe place.
- When in a restaurant or store, try to make sure you see the person swiping your card only one time on a legitimate approval system. Some thieves supply and second card reader designed to capture information and pay employees to scan customers' credit cards at the same time they run them through the normal card reader.

Limiting the damage

If lose your wallet or purse or are the victim of identify theft, there are some things you can do to limit the damage:

- Cancel all credit cards and bank accounts immediately. Make sure you have the toll-free numbers handy, along with the account numbers of every card you carry in your wallet. (This is where that photocopy of your wallet contents comes in handy.)
- File a police report immediately in the jurisdiction where your property was stolen. This proves to creditors you were diligent, even if law enforcement officials tell you there will probably be no official investigation. Give as much documented evidence as possible, including any fraud accounts. Get a copy of the report and give the phone number of your investigator to creditors or others who require verification of your case.
- Immediately report the situation to the fraud units of the three credit reporting agencies: Equifax (1-800-525-6285), Experian (1-888-397-3742, and TransUnion (1-800-680-7289). Effective April 2003, if you notify one bureau that you are a victim of identity theft, it will also notify the other two. Ask that your file be flagged with a fraud alert and include a victim's statement informing creditors to contact you via telephone to verify all applications.

For more information, visit the Colorado Attorney General's web page at <http://www.ago.state.co.us/idtheft/welcome.htm>.

Disclaimer: This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is distributed with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal or accounting advice or other expert assistance is required, the services of a competent professional should be sought.

Corporate Office
3033 East First Avenue
Suite 600
Denver, CO 80206
303-321-1880
Fax 303-331-0272

Please visit our website
for a complete list of
office locations:
www.LTGC.com

