City of Monterey

IF YOU ARE A VICTIM OF ID THEFT

You must act quickly after learning you are a victim of identity theft or fraud. Even if there is no direct loss, fraudulent use of your information can devastate your credit file. This can prevent your use of your own credit or access to bank funds and accounts. Take steps to reduce future loss.

- Keep a log or chronology of the date, time and substance of all correspondence, people, companies and telephone conversations related to your identity theft or financial fraud.
- File a police report. Keep the report number and obtain a copy of the report. You may need both to verify the crime for creditors.

CREDIT BUREAUS

Only one call is needed to report fraud to all three bureaus. However, it's best to call all three and ask that your file be flagged with a fraud alert and add a victim's or consumer statement to your report. You can get one free report per year.

 www.Equifax.com
 800-525-6285

 www.Experian.com
 888-397-3742

 www.Transunion.com
 800-680-7289

- Ask the credit bureaus for the names of credit grantors where fraudulent accounts are opened. Ask that the related inquires be removed due to the fraudulent access.
- Ask the credit bureaus to notify anyone that has received your credit report in the last six months and alert them to any disputed or fraudulent information.
- Opt out of pre-approved credit offers by contacting www.the-dma.org or calling 888-567-8688. You can request to be removed from offer mailing and calling lists.

CREDITORS

Contact all creditors immediately where your name has been fraudulently used and accounts opened. Dispute any charges in writing. You may need to fill out a fraud affidavit and other forms.

CHECKS

If your checks or account information have been stolen or your bank account information used fraudulently, report it to the bank. Put a stop on the checks in question and have the bank close your accounts and open new ones. Have the bank set up a password for the new accounts.

SOCIAL SECURITY NUMBER

Call SSA and report the fraudulent use. Only as a last resort have your SSN number changed. Log on at www.ssa.gov or call 800-772-1213.

DRIVER LICENSE

If someone uses your driver license info to write fraudulent checks you may need to change your number. Contact the DMV and put an alert on your number (www.dmv.ca.gov). You may need to go to your local DMV office and file a complaint form so an investigation can be authorized.

POSTAL FRAUD OR CHANGE OF ADDRESS

One method of identity theft is to send your mail to another address. This allows the thief to intercept your personal information as it arrives in the mail. If this happens call the local Postmaster. Find where your mail is going and notify Postal Inspectors of the related office. Visit the Web for more info www.usps.com/postalinspectors

ONLINE CONTACTS & RESOURCES

- > CA Dept. of Consumer Affairs www.privacy.ca.gov
- > CA Atty General <u>caag.state.ca.us/idtheft/index.htm</u>
- > Federal Trade Commission www.ftc.gov
- > Monterey Police Department www.monterey.org/mpd

Monterey Police Dept.

351 Madison St. • Monterey, CA 93940
831-646-3830 • www.monterey.org/mpd

This pamphlet is provided to inform the public about identity theft. The Monterey Police Department makes no warranty or accepts any liability associated with its use. The information contained in the pamphlet was current at the time of printing. Special thanks to Menlo Park Police Department for providing material for this pamphlet.

Protect yourself from IDENTITY THEFT



A guide to keep your personal information safe and secure. Inside, find tips to protect yourself in the information age.

www.monterey.org | City TV cable Ch. 25

CITIZEN'S GUIDE TO PROTECTING AGAINST IDENTITY THEFT

Each day, Monterey Police Officers work to protect the lives and property of those who live and work in our community along with those who come to visit. The information age and advanced technologies have presented new challenges: protecting people from the theft of their identity.

Identity theft occurs when someone willfully obtains the identity of another and uses it for unlawful purposes. Most often, that purpose involves economic gain for them and results in severe hardships for the victim. Each year, approximately 10 million people in the United States are victims of identity theft. Losses run into the \$50 billions for businesses and consumers. It is one of the fastest growing crimes in the world, and law enforcement is positioning itself to meet the challenge.

Fortunately, there is a lot that each of us can do to protect ourselves from identity theft. This brochure is designed to provide you with facts and tips to help prevent you from becoming a victim.

We strongly encourage you to take the time to read this brochure and to follow the suggestions. The actions you take now may help keep you from becoming the victim of one of the most destructive of all property crimes – identity theft.

- Carlo Cudio, Chief of Police

IDENTITY THEFT DEFINED

Identity theft is the crime of acquiring all or pieces of someone else's identifying information and using it to commit fraud. This can include your name, address, date of birth, social security number (SSN), financial account numbers and other information. With this information a criminal can commit numerous forms of fraud both against you and others while using your identity.

The California law PC 530.5 was enacted in 1998 making identity theft a crime.

COMMON METHODS OF IDENTITY THEFT

- Stealing mail from mailboxes to obtain credit cards, written and blank checks, bank and credit card statements, pre-approved credit offers, financial or tax information.
- Stealing wallets, purses or portable computers.
- "Dumpster diving" in your trash for receipts, forms, applications and personal information.
- Obtaining names, SSNs and account numbers from personnel, medical or customer files in the workplace (e.g., open files, applications or payroll stubs).
- Posing as a landlord, employer, or loan officer to get a copy of your credit history.
- "Shoulder surfing" at ATM machines and phone booths for PIN and phone numbers.
- Searching internet sites that list public records or use fee-based research services.

PREVENTION TIPS & TECHNIQUES

While you cannot completely prevent identity theft, you can reduce the risk of fraud by taking a few precautions every day. This may mean a change in handling your bills, accounts and personal information.

One of the most important things you can do is check your credit report at least once a year (see other side for details). You can catch fraud early by checking your credit report regularly. Below are some other easy steps to consider.

- Do not carry your social security card, birth certificate, or passport with you unless you need it for a specific reason. Leave them home.
- Do not share your social security number over the phone unless you are certain about the company or government agency you are speaking with.
- Do not print your driver license or social security number or let others write it on your checks.
- Do not carry more than two credit cards. Always take credit /debit card receipts with you. Never throw them in a public trashcan.
- Reduce the number of personal checks you write. Use cash, credit or debit cards and online banking services.
- Make a list or photocopy of all your credit cards and keep this is a safe, secure place.

- Shred unused pre-approved credit card offers and applications, all receipts, bills, statements and other financial records. Secure records in a locked location.
- Do not leave bill payments or checks in your home mailbox for the postal carrier to pick up, especially with the little red flag up. This is an invitation to a thief. Mail bills and checks only at a post office.
- If you are missing a credit card or other bill, or it appears overdue, a thief may have filed a change of address with the post office or the creditor. Call the creditor to verify your address with them. Ask the creditor to check if additional cards were requested. Call the post office to check on any change of address request.
- Cancel your unused credit cards. Limit the number of open credit accounts you have.
- Never give out personal information over the phone unless you initiated the call and have a trusted business relationship with the person.
- Never reply to email messages or Internet Web sites linked from an email asking you for account, personal or credit card information.
- Delete unsolicited email "spam" as many are scams to get a reply or to get your info and IP address. Do not click "unsubscribe;" just delete it. Many Internet services now provide email filters that block spam mail. Make sure these filters are installed.
- If you shop online, only use a secure browser connection (look for https in the browser address) or place your order by phone or mail.
- Check your Social Security Earnings and Benefits statement once a year to confirm no one else is using your number.
- Consider getting an unlisted home phone number and, if listed, avoid using professional titles which make you a target (e.g., Dr., M.D., Atty., Ph.D., etc.).
- When making new passwords, avoid using easily guessed ones, like your birthday or social security number or your name. Never carry a list of passwords with you.
- When ordering new checks, pick them up at the bank instead of having them mailed to your home.
- Shield the keypad when at an ATM, POS terminal or when using a phone calling card.