



What to do if it happens to you

Prevention Guidelines and Resources

IDENTITY THEFT OVERVIEW

The purpose of this article is to provide information on how to protect yourself from identity theft and to provide help for those who have been a victim of this crime.

The United States General Accounting Office's 1997 report states that 750 million dollars was lost to identity theft alone.

As a result of the popularity this type of crime, California legislators passed Penal Code section 530.5 and 530.6. These sections make it easier for identity theft victims to make a police report.

530.5 PC allows the person whose identity was used to be named as a victim. Prior to this law coming into effect, only the stores that lost money were considered victims.

530.6 PC requires the law enforcement agency that has jurisdiction over and identity theft victim's residence, take an identity theft report, when requested by the victim. The law enforcement agency must take a report, even if the identity theft occurred in another jurisdiction. The law enforcement agency is also required to provide the victim with a copy of the police report. If the identity theft did not occur in the law enforcement agencies jurisdiction, they are required to refer the matter to the law enforcement agency where the identity theft occurred.

INTERNET SAFETY TIPS

The Internet is a very convenient way to order merchandise. Remember there is a greater chance of being the victim of identity theft, if you give your personal information out over the Internet.

If you choose to make Internet purchases, utilize Internet banking or obtain a loan follow these basic safety rules:

1. Check the website certificate to verify that it is valid. For more information check your web browser's help file.
2. Know the companies you are dealing with. Just because they have a certificate on file does not mean they are reputable company.



3. Updating your browser to a 128-bit encryption mode, makes your transactions extremely difficult to crack. Visit www.microsoft.com for Internet Explorer or www.netscape.com for Netscape information on how to get this done.
4. Remember use caution when giving your personal information over the Internet, because no system is 100% foolproof.

PREVENTION GUIDELINES

Don't carry information with you that you don't need. This includes you Social Security number, birth certificate or credit cards that you will not be using.

Be careful with credit card receipts once you have made a purchase. If you do not need them, shred them, if you need them; keep them in a safe place at home.

When mailing bills or important correspondence, use the post office. Do not allow you fail to sit in a street side mailbox.

Shred all credit card applications that you do not plan on using or any personal information you do not need.

Review your credit card bills and bank statements as soon as you get them to ascertain if the transactions are known to you.

Review your credit report at least once a year. If you have been the victim of identity theft review your credit report monthly to ascertain the possibility of continuing fraud.

Always sign the back of your credit cards. Some people believe if they write "see ID" instead of their signature the back of their credit cards this will protect them. Most credit card companies will not reimburse you for fraudulent charges if your credit card was not signed on the back.

If you have not received credit card bills in a normal fashion, confirm that no one has placed a change of address request with the [United States Post Office](#).

Do not pre-print your driver's license or Social Security numbers on your checks.

Never give out personal information, such as Social Security number, to anyone over the telephone or on the Internet.

Guidelines for Victims of Identity Theft

The most frustrating aspect of this crime is the work the victim has to do to restore their credit history. These guidelines should assist you.

- Call all three credit reporting bureaus and obtain a copy of your credit reports. Have a fraud alert placed in your credit file.
- Maintain a list of everyone you contact. List names, positions, dates, and times.
- Cancel all fraudulent accounts in your name and do not pay the bills that you are not responsible for, even if you are threatened with collections.



- Get a copy of your credit report every six months to make sure no fraudulent accounts have been opened.
- Notify all involved creditors or banks both by telephone and in writing.
- Contact the [Department of Motor Vehicles](#), if your driver's license was used.
- Contact the [Social Security Administration](#) if your Social Security number has been compromised.
- Do not pay for Notary services, if requested to do so by a victim company. Notary services are expensive and not necessary for criminal prosecution. Tell the requesting company to pay for the notary services, if they want a notarized affidavit.
- Contact the police department that has jurisdiction where you live, if you want to make a police report. Your local police department is required by law (530.6 PC), to forward the report to the police department that has jurisdiction in the area where the identity theft occurred.

RESOURCES

Credit reporting bureaus:

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

Social Security Administration:

To report fraudulent use, call (800) 269-0271

To order a statement, call (800) 772-1213

For more information contact:

Union City Police Department (510) 471-1365

