Keep a log of all conversation with the authorities and financial institutions, including dates, names, and phone numbers. Note time spent and any expenses incurred. Confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.

1. Credit bureaus. Immediately call the fraud units of the three credit reporting companies—Experian (formerly TRW), Equifax and Trans Union. Report the theft of your credit cards or numbers. The phone numbers are provided at the end of this brochure. Ask that your account be flagged. Also, add a victim's statement to your report, up to 100 words. ("My ID has been used to apply for credit fraudulently. Contact me at 760-123-4567 to verify all applications.") Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. *These measures may not entirely stop new fraudulent accounts from being opened by the imposter. Ask the credit bureaus to provide you with free copies every few months so you can monitor your credit report.*

Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove inquiries that have been granted due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers.)

2. Creditors. Contact all creditors immediately with whom your name has been used fraudulently – by phone and in writing. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request." (This is better than "card lost or stolen," because when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

Creditors requirements to verify fraud. You may be asked by banks and credit grantors to fill out and notarize fraud affidavits, which could become costly. The law does not require that a notarized affidavit be provided to creditors. A written statement and supporting documentation should be enough (unless the creditor offers to pay for the notary).

3. Stolen checks. If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies (see next page for names and phone numbers). Put stop payments on any checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account.

4. ATM cards. If your ATM card has been stolen or compromised, get 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.

5. Fraudulent change of address. Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud. (Call the local Postmaster to obtain the phone number.) Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier.

6. 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 number. The SSA will only change it if you fit their fraud victim criteria. Also order a copy of your Earnings and Benefits Statement and check it for accuracy.

7. Passports. If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.

8. Phone Service. If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password, which must be used any time the account is changed.

9. Drivers license number misuse. You may need to change your driver's license number if someone is using yours as identification on bad checks. Call the state office of the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Fill out the DMV complaint form to begin the investigation process. Send supporting documents with the complaint form to the nearest DMV investigation office.

10. Law enforcement. Report the crime to the law enforcement agency within the jurisdiction where you live (530.5 PC). Give them as much documented evidence as possible. Get a copy of your police report.

11. False civil and criminal judgments. Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgment has been entered in your name for actions taken by your imposter, contact the court where the judgment was entered and report that you are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the Calif. Department of Justice and the FBI. Ask how to clear your name.

12. Legal help. You may want to consult an attorney to take legal action 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. Call the local Bar Association to find an attorney who specializes in consumer law and the Fair Credit Reporting Act.

13. Dealing with emotional stress. Psychological counseling may help you with the stress and anxiety commonly experienced by victims. You are not alone.

14. Sample "Courtesy Notice"

(Date)

Dear (Creditor Name/Collection Agency Name):

On (Date) I received your letter demanding payment of (amount). I did not open this account and incur this unpaid balance. Someone, other than myself, wrongly used my personal information to obtain a line of credit/service. Your company extended a line of credit/services to an imposter. Your company is a victim and should file a police report in the appropriate jurisdiction.

You are hereby notified that on (Date), I filed an Identity Theft Report with the Escondido Police Department. The case number is (report number). This can be verified by calling the Escondido Police Department's Records Bureau at (760) 839-4721.

Closing,

(Your Name and Address)

RESOURCES

Credit reporting bureaus:

Equifax: 11601 Roosevelt Blvd. St. Petersburg Fl 33716-2202

Information Service Center: (800) 525-6285

Order credit report: (800) 685-1111 (CA residents only)
Opt out of pre-approved offers of credit: (888) 567-8688
www.equifax.com

Experian: (formerly TRW): P.O. Box 1017, Allen, TX 75013.
Report fraud: Call (800) 311-4769 and write to address above.
Order credit report: (888) 397-3742.
Opt out of pre-approved offers of credit and marketing lists: (888) 567-8688
www.expewrian.com

Trans Union: P.O. Box 6790 Fullerton, Ca 92634.
Report fraud: (800) 680-7289 and write to Fraud Victim Assistance Division, P.O. Box 7690, Fullerton, Ca 92634.
Order credit report: (800) 916-8800
www.transunion.com

Remember, if you have been denied credit, you are entitled to a free credit report. If you are a victim of fraud, be sure to ask the credit bureaus for free copies. They will often provide them. Starting October 1997, free annual credit reports for victims of identity theft will be required by law.

Social Security Administration:
Report fraud: (800) 269-0271.
Order your Earnings and Benefits Statement: (800) 772-1213.

To remove your name from mail and phone lists:
Direct Marketing Association

- ❑ Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735
- ❑ Telephone Preference Service, P.O. Box 9014, Farmingdale, NY 11735.

To report fraudulent use of your checks:

- ❑ Global Payments: (800) 766-2748
- ❑ Chexsystems: (800) 428-9623
- ❑ Certigy/Equifax Check Service: (800) 437-5120
- ❑ SCAN: (800) 262-7771
- ❑ Telecheck: (800) 710-9898
- ❑ CrossCheck (800) 843-0760
- ❑ International Check Services (800) 526-5380

Other useful resources:
- ❑ Federal Government Information Center: Call (800) 688-9889 for help obtaining government agency phone numbers.

Contact the Federal Trade Commission to report the problem:
www.ftc.gov - The FTC is the federal clearinghouse for complaints by victims of identity theft. The FTC helps victims by providing the information to help resolve financial and other problems that could result from identity theft. Their hotline number is 1-877-IDTHEFT (438-4338) or: www.consumer.gov/idtheft

Laws
Federal
Identity Theft and Assumption Deterrence Act Public Law 105-318, 112 Stat. 3007 (Oct, 1998)
www.ftc.gov/os/statutes

State of California
Unauthorized Use of Personal Identifying Information
530.5 PC

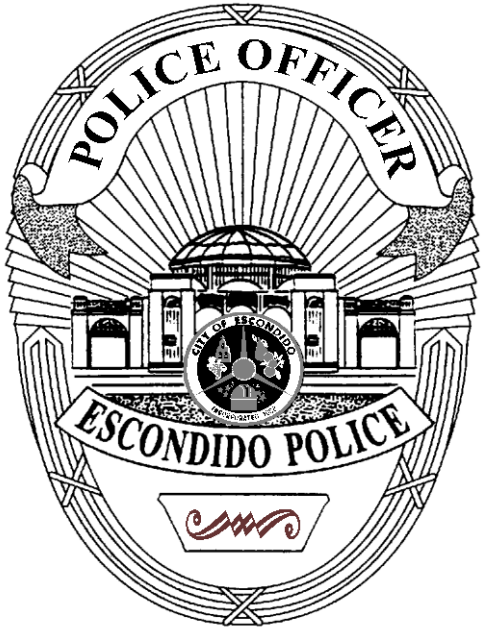
Useful Internet Locations
California Department of Consumer Affairs
www.dca.ca.gov

www.privacyrights.org
www.identitytheft.cor

IF SOMEONE IS USING YOUR PERSONAL INFORMATION TO OBTAIN FRAUDULENT CREDIT AND/OR BANK ACCOUNTS, YOU ARE THE VICTIM OF…

Identity Theft

What to Do If It Happens To You



Craig Carter
Chief of Police
Crimes of Property Unit
(760) 839-4717

This guide provides victim of identity theft with the major resources to contact. It is important to act quickly and assertively to minimize the damage.