

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone pretends to be you. Then, pretending to be you, they apply for credit, buy cars, commit crimes, obtain a passport, or any number of things that you might or might not do or authorize.

IDENTITY THIEVES CAN ACCESS YOUR PERSONAL INFORMATION BY:

- Stealing wallets or purses.
- Rummaging through your trash (“dumpster diving”).
- Stealing mail (including pre-approved (credit offers).
- Completing a “change of address form” to divert your mail to another location.
- “Skimming” your credit or debit card through a special device that stores the account information.
- Taking your information from a business or institution.
- Stealing information from your home.
- Scamming information from you by posing as a legitimate person or government official.

IDENTITY THEFT IS A CRIME

Penal Code Section 530.5. (a) Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment pursuant to subdivision (h) of Section 1170.

RED FLAGS THAT YOU MAY BE VICTIM OF IDENTITY THEFT

- **M**istakes on your bank, credit card, or other account statements
- **M**istakes on the explanation of medical benefits from your health plan
- **Y**our regular bills and account statements don't arrive on time
- **B**ills or collection notices for products or services you never received
- **C**alls from debt collectors about debts that don't belong to you
- **A** notice from the IRS that someone used your Social Security number
- **M**ail, email, or calls about accounts or jobs in your minor child's name
- **U**nwarranted collection notices on your credit report
- **B**usinesses turn down your checks
- **Y**ou are turned down unexpectedly for a loan or job.

HOW CAN I PROTECT MYSELF FROM IDENTITY THEFT?

Any one of us can become a victim of identity theft. This is a crime that strikes all economic classes, all sections of the country, and all ages. Identity thieves will even steal the identity of someone who has died. Statistically, California is near the top in the nation for reported cases of identity theft.

The following are some ways to protect your identity:

- Do not carry extra credit cards, your Social Security card, passport, or birth certificate except when absolutely necessary.
- Install a locked mailbox at your residence or use a post office box to reduce the chance of mail theft.
- Pick up new checks at your bank.
- Do not leave paid bills in your mailbox for the postal carrier to pick up.
- Ask your financial institutions to add extra security protection to your account. Most will allow you to use an additional code when accessing your account.
- Protect your Social Security Number at all costs. Do not let merchants write your SSN on your checks. Request merchants to use other forms of identification.
- Never allow credit card numbers to be written on your checks.
- Do not use your birth date or mother's maiden name as PIN numbers or passwords.
- Be careful with passwords and PIN numbers. Do not use the same one for everything. Change your passwords and PIN numbers from time to time.
- Remove your name from the marketing lists of the three credit reporting bureaus - Equifax, Experian, and Trans Union. Do not give any OPT-OUT service your SSN, date of birth, mother's maiden name, or other personal identification information.
- Shred all paperwork with financial and personal information on it before throwing it in the garbage.
- Do not give out personal information over the phone, through the mail, or over the Internet unless you know who you are dealing with.
- Obtain a copy of your credit report at least once or twice a year. Check it for errors or possible fraudulent information. You can receive one free credit report a year. **Check with each credit bureau.**

You may be a victim of ID Theft if:

- Bills that do not arrive as expected.
- Unexpected bills or credit card statements arrive.

BE WISE ABOUT MANAGING YOUR PERSONAL INFORMATION:

- Do not carry your Social Security card or number. Minimize the number of credit cards and identification cards you carry.
- Shred discarded personal records and documents.
- Guard postal mail from theft. Deposit outgoing mail in post office boxes instead of from an unsecured mailbox. Remove mail from your mailbox promptly.
- If you get an e-mail that asks for personal or financial information, do not reply or click on the link in the message.
- Only shop at Internet sites you trust.
- If you are not interested in pre-approved credit offers, opt-out of receiving them. Call 1-888-5-OPT-OUT
- Review your bank and credit card statements carefully as soon as you receive them.
- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with.
- Order a copy of your credit report every year and review it carefully.
- Determine how your information will be used and safeguarded before giving it out.

DO NOT:

- Do not give out personal information in response to unsolicited offers by internet, phone, mail, or in person. Criminals may be posing as legitimate business people, charity workers or law enforcement to gain your trust and your money.
- Do not open email, files, hyperlinks or download programs from people or companies you do not know. You could unknowingly infect your computer with a virus or malware.
- Do not use automatic password log-in features on your computer. If your computer is stolen, your personal information could be compromised.
- Do not hesitate to notify authorities if you suspect you may be the victim of identity theft.

WARNING SIGNS OF ID THEFT

- Denials of credit for no apparent reason.
- Calls about purchases you did not make.
- Finding withdrawals in bank accounts you cannot account for.

TAKE IMMEDIATE ACTION: FIRST STEPS

A fast response to identity theft is the best way to minimize the damage to your name and financial health. The Oakley Police Department recommends that you immediately take the following steps:

- **Report fraud to creditors.** Check with credit card companies and banks to see if any new accounts have been opened in your name or if any unauthorized charges have been made. Work with these companies to stop further damage as quickly as possible. You may wish to close bank accounts immediately, but remember to make sure that all outstanding checks clear before you do so. Once you verify that all legitimate checks have cleared, talk to your bank about closing compromised accounts and setting up new, password-protected accounts. Once you have notified banks and credit card companies of the fraud, you should also alert your other creditors, including phone companies, utility providers, Internet service providers, and other service providers.

- **Place a fraud alert on your credit report.** Contact the toll-free number of any of the three consumer reporting agencies, listed below, to place a fraud alert on your credit report. A fraud alert notifies potential creditors to contact you and verify your identity before approving a credit request in your name. You only need to contact one of the three companies, because that company is required to contact the other two.

Equifax: 1-800-525-6285; www.equifax.com;

P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742);

www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289;

www.transunion.com; Fraud Victim Assistance Division,
P.O. Box 6790, Fullerton, CA 92834-6790

Once you place a fraud alert on your file, you are entitled to free copies of your credit reports. You will receive a letter telling you how to order your free copies. When you receive your credit reports, review them carefully and look for any suspicious activity.

- **File a police report.** California law requires police departments to accept and provide reports. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime.

- **Decide whether you want to place a security freeze on your credit report.** A security freeze is different from a fraud alert. It allows you to prohibit your credit report from being released to another person without your prior express

authorization. An identity theft victim requesting a freeze will need to provide a police report number with his or her application. To request a freeze, you must submit a written request via certified mail to each of the three credit reporting agencies above. Once the freeze is in place, you will be unable to obtain credit without first providing the consumer reporting company with your unique Personal Identification Number. The freeze allows consumers whose personal information has been compromised to take a proactive step to prevent identity theft.

How Do I Contact Agencies and Bureaus To Report Identity Theft?

Credit Bureaus (Open 24 hours)

Equifax 1-800-525-6285

Experian 1-800-397-3742

Trans Union 1-800-680-7289

Social Security Administration

1-800-269-0271

Federal Trade Commission

1-877-ID-THEFT

www.ftc.gov

California Attorney General's Office

www.oag.ca.gov

Your local postal inspection service

Check for listings under Postal Service in the "United States Government" section of your local phone directory's blue pages.

The Oakley Police Department

(925)-625-8855

OTHER USEFUL RESOURCES ON IDENTITY THEFT:

Federal Trade Commission (FTC)

www.consumer.gov/idtheft

U.S. Department of Justice (DOJ)

www.usdoj.gov

U.S. Postal Inspection Service

www.usps.com/postalinspectors

IDENTITY THEFT



Oakley Police Department

3231 Main Street

Oakley CA 94561

(925) 625-8855

*" A Place for Families in
the Heart of the Delta "*

