

- **Request** that the CCRBs place an extended fraud alert on your credit reports. They are free. They permit some creditors to get your report as long as they take steps to verify your identity, which may include contacting you in person.
- An alternative to an extended fraud alert is a security freeze. A freeze generally stops all access to your credit files, but like a fraud alert, it may not stop misuse of your existing accounts or other types of identity theft.
- **Contact** all your creditors by phone and in writing to inform them of the theft.
- If an identity thief has used your SSN to file a forged tax return in an attempt to get a fraudulent tax refund early in the filing season and you file your own return later, you will receive a notice or letter from the IRS that states one of the following: (1) More than one tax return has been filed for you, (2) You have to return the money paid out in your name to the identity thief, or (3) IRS records indicate you received wages from an employer not names on your return. In this case you will need to respond immediately and submit the Form 14039. You can also get help from the Taxpayer Advocate Service (TAS) by calling **(877) 777-4778**. For more information on the TAS go to **[www.irs.gov/advocate](http://www.irs.gov/advocate)**.
- **Call** the U.S. Secret Service at **(619) 557-5640** if the crime involves counterfeit credit cards or computer hacking.
- **Notify** the U.S. Postal Inspector if your mail has been stolen or tampered with.
- **Notify** your banks, library, and the SSA, IRS, and California DMV if you believe you may become a victim.
- In the case of medical identity theft, request a copy of your current medical files from each health care provider, and request that all false information be removed from them

and your insurance files. Enclose a copy of the police report with your requests.

- **Call** the Health Insurance Counseling and Advocacy Program’s Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to report any theft that involves Medicare.
- If you are contacted by a collector for a debt that resulted from identity theft, send the debt collector a letter by certified mail, return receipt requested, stating that you did not create the debt and aren’t responsible.
- **Include** a copy of the police report and a completed copy of the FTC’s Identity Theft Victim’s Complaint and Affidavit. It can be downloaded from its website at **[www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf](http://www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf)**.
- Also **write** in your letter that you are giving notice as a claimant under California Civil Code Sec. 1798.93(c) (5) that a situation of identity theft exists.
- **Call** the SDPD Economic Crimes Section at **(619) 531-2545** and talk to the investigator if you have any questions about your case, or have more information to provide.
- **Other things** you should do as a victim are in the Identity Theft Victim Checklist on the website of the California Department of Justice Office of the Attorney General at **[www.oag.ca.gov/idtheft/facts/victim-checklist](http://www.oag.ca.gov/idtheft/facts/victim-checklist)**. They will help victims clear up their records and limit the damage done by the thief.

## SDPD DIVISIONS

**For general information please contact your local police substation.**

<b>Central Division</b>	<b>(619) 744-9500</b>
<b>Eastern Division</b>	<b>(858) 495-7900</b>
<b>Mid-City Division</b>	<b>(619) 516-3000</b>
<b>Northeastern Division</b>	<b>(858) 538-8000</b>
<b>Northern Division</b>	<b>(858) 552-1700</b>
<b>Northwestern Division</b>	<b>(858) 523-7000</b>
<b>Southeastern Division</b>	<b>(619) 527-3500</b>
<b>Southern Division</b>	<b>(619) 424-0400</b>
<b>Western Division</b>	<b>(619) 692-4800</b>

**For more information, online visit:**

**[www.sandiego.gov/police/](http://www.sandiego.gov/police/)**

**Revised January 17, 2018**



**SAN DIEGO POLICE DEPARTMENT**

## Identity Theft Recognition, Response and Recovery

This brochure contains information that can be helpful on how to recognize if your identity has been stolen, how to respond to identity theft and how to recover from this theft.

## Recognition

### Signs That Your Identity May Have Been Stolen

- ✓ Your credit card and bank statements, and other mail with personal information doesn't arrive when expected
- ✓ You start getting bills from companies you don't recognize
- ✓ Collection agencies try to collect debts that don't belong to you
- ✓ Charges you didn't make start appearing online and your monthly card and bank statements
- ✓ You are told that another address is on your credit card or bank account
- ✓ Your credit card or bank calls or texts you to ask about an unusual charge that you didn't make
- ✓ An account you didn't open shows up on your credit report
- ✓ You see withdrawals from your bank account that you can't explain
- ✓ Merchants refuse to cash your checks
- ✓ Medical providers bill you for services you didn't receive
- ✓ Your health plan rejects a legitimate claim because their records show that you have reached your benefits limit
- ✓ The IRS notifies you that a tax return has already been filed in your name and SSN
- ✓ You receive a letter from the IRS asking you to verify whether you sent a tax return bearing your name and SSN. The IRS holds suspicious tax returns and sends taxpayers letters to verify them
- ✓ You receive income information at tax time from an unknown employer

## Checking for Possible Identity Theft

- Obtain free copies of your credit reports from Equifax, Experian, and TransUnion, the three Consumer Credit Reporting Bureaus (CCRBs) at [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling **(877) 322-8228**. Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit.
- ✓ Check your medical bills and health insurance statements to make sure the dates and types of services match your records. If you see a doctor's name or date of service that isn't familiar, call the doctor and your insurer.

If you're denied credit, make sure the creditor's decision is based on your identity and personal credit information, and not someone else's.

## Response

### If You Believe You Are a Victim

- ✓ If you believe your information has been compromised or if your purse, wallet, or anything else with your personal information in it is lost or stolen, don't wait until you become a victim to report it. Do the following as soon as possible.
- ✓ File a police report in the jurisdiction where your loss occurred. Get a copy of the report. You may need to send copies elsewhere.
- ✓ Report the loss to one of the CCRBs and request that an initial fraud alert be placed on your credit files.

- ✓ Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

- ✓ If you're on active duty in the military you should contact one of the CCRBs and place an active duty fraud alert on your credit files.
- ✓ If any bank checks, cards, or account numbers were lost and could be used by an identity thief in the future, call the banks and request new account numbers, checks, ATM or debit cards, PINs, and passwords. Do the same for credit or charge cards that were lost and could be used by the thief in the future.
- ✓ If your Social Security card or any other card with your SSN on it was lost, contact your local the Social Security Administration (SSA) at **(800) 772-1213** to request a replacement card. You should consider blocking electronic access to your Social Security record. Authorize the IRS to put a marker on your account that will help it protect you from identity theft and resolve future issues.
- ✓ If your Medicare card or any other card with your Medicare number on it was lost, call the SSA at **(800) 772-1213** to request a replacement card. Or to obtain one online, you need to first create a My Social Security account.
- ✓ If your driver's license was lost, contact the California DMV Fraud Hotline at **(866) 658-5758** to report the loss, request a replacement license, ask that a stolen/lost warning be placed in your file, and check that another license has not been issued in your name.
- ✓ If your library card was lost, contact the library immediately.
- ✓ Consider buying identity theft protection.

- ✓ If you get a security breach notice or otherwise believe elements of your personal information such as SSN, driver license or California identification card number, medical or health insurance information, and financial account, credit card, or debit card numbers have been compromised, you should take the measures suggested above. And if multiple elements are involved as in the Equifax breach in September 2017, place security freezes on your credit reports with each of the three CCRBs.

## Recovery

### If You Become a Victim

- ✓ File a police report as soon as possible if you become a victim of identity theft and used it for an unlawful purpose. Call the SDPD at **(619) 531-2000** and give the dispatcher a description of the theft. An officer will call to take a full report and give you a case number. **Then do the following:**
  - Set up a folder where you can keep copies of all your reports and supporting documents, and a log of contacts and their phone numbers. You will need to refer to this case number.

- ✓ **Report** the theft to the FTC at [www.IdentityTheft.gov](http://www.IdentityTheft.gov) to get help in recovering from it. The FTC is the federal clearinghouse for complaints of victims of identity theft. This website is a one-stop resource to help you report and recover from identity theft. Information provided includes checklists, sample letters, and links to other resources. After answering some questions about your situation, you'll be told what to do right away, what to do next, and what other possible steps to take to create a personal recovery plan. Then you can create an account and be walked through each recovery step.