If You Become a Victim of Identity Theft

Place a fraud alert on your files

Contact the three major U.S. credit reporting companies to report yourself as a victim of identity theft.

Order a credit report

By law, you are entitled to a free copy of your credit report once a year from all three companies. Prepare copies for the FTC and your local police. Order a free copy of your credit report by phone, toll-free at (877)322-8228, or online at **www.annualcreditreport.com.**

Notify the US Postal Inspector

if your mail has been stolen or tampered with: US Postal Inspection Service—Local Post Office (**877)876-2455 www.uspis.gov/report**

Contact the Federal Trade Commission (FTC)

to report the crime. The FTC provides information to help victims resolve problems that result from identity theft**:**
https://www.ftc.gov
Hotline: (877) 438-4338

You can report file a report with OPD online or by calling the non emergency number.

Include a copy of your FTC Identity Theft Affidavit; any other proof of identity; proof of your address; a government-issued photo identification.

Make a note of your OPD Case # (RD#) to refer to if needed by a debtor or law enforcement agency. Unfortunately not all cases will be assigned to an investigator if there are no significant leads to identify the suspect.

Oakland Police Department

455 7th Street
Oakland, CA 94607

www.oaklandca.gov/departments/police

Emergency

911

Non Emergency
(510) 777-3333

Text-To-911
Enter 911 without spaces or hyphens and text the reason for your emergency.

Report Online

You can file an Identity Theft report on the City of Oakland website

www.oaklandca.gov/services/report-a-crime-online

or by scanning the QR Code below

SCAN ME

Oakland Police Department

Identity Theft

Resource Card

Report Identity Theft
OPD Non-Emergency
(510)777-3333

This brochure is available in English, Spanish, Chinese, and Vietnamese. TF - 3168 (Sep 2022)

What is Identity Theft?

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Typical identity theft involves a thief stealing your personal information to pose as you in some way.

Synthetic Identity Theft

A newer and growing variety - synthetic identity is born when your personal identifiable information (PII) is combined with fake data to create a brand new, fake identity. PII, such as your date of birth, passwords, passport number, Social Security number or credit and bank account numbers, telephone number, birth and death certificates, medical ID number, and biometric data, like fingerprints and scans, is subject to theft and fraud.

A thief will combine your Social Security number with a different name or other fake credentials. Synthetic identity theft can be harder to detect - which will lead to more damage in the long run.

Statistics

One of the fastest growing crimes in America
The Bureau of Justice Statistics estimates that identity theft victimized close to 17 million people in 2012 alone. Identity theft has topped the U.S. Federal Trade Commission's ranking of consumer complaints for 15 years.

There are many ways to commit identity theft, including hacking, financial and social media account takeovers, credit card fraud, phishing, medical ID fraud, ransomware attacks, tech support fraud, and others.

How to Prevent Identity Theft

Because we use our personal information almost every day there is always a chance that someone could steal this data whenever we provide it. However, you can take simple steps to reduce the chance of identity theft.

Report all lost and stolen cards immediately!

Don't share your personal, financial or health plan information over the phone, through the mail, or over the Internet unless you have a trusted relationship with the requestor and you initiated the contact.

Limit what you carry.
Empty your wallet of extra credit cards and IDs. Leave your social security card and Medicare card at home – unless you are going to need them for a specific reason.

Use only one credit card for online purchases. Do not use a debit card.

Collect mail daily.
Identity theft isn't always high tech. One of the easiest ways a thief can steal your identity is simply to take your physical mail from your mailbox. Deposit outgoing mail in postal collection boxes or at your local post office. Do not leave mail in unsecured mail receptacles.

Shred Documents containing personal information before disposing of them, including receipts, credit offers, loan and credit applications, insurance forms, bank statements, and similar documents.

Securely Store Documents
Store financial documents, Social Security, Medicare and credit cards in a safe place at home and at work.

Remove all personal information stored on your laptop, computer or phone before you sell, give away or dispose of it.

Create different passwords for your accounts. Create a different, secure password that is long, complex, and unique for various accounts. Avoid using information related to your identity, such as the last four digits of your Social Security number, your birthday, your initials, or parts of your name.

Beware Shoulder Surfing
Shoulder Surfers observe your actions or eavesdrop to gain access to sensitive information. Shield keypads with your hand or body when entering your PINs and/or passwords. Avoid sharing personal info over the phone in public.

Monitor Your Credit Reports, Bank and Credit Accounts. Open and read your bank account and credit billing statements when you receive them. Check for unauthorized charges or withdrawals and report any immediately by phone and in writing. Contact the credit card issuer if replacement cards are not received prior to expiration dates.