WHAT SHOULD I DO IF I AM A VICTIM OF IDENTITY THEFT?

- Close all accounts that have been tampered with, established fraudulently or are associated with lost or stolen information. [https://www.consumer.ftc.gov/features/feature-0014-identity-theft](https://www.consumer.ftc.gov/features/feature-0014-identity-theft)

- Contact the three credit bureaus (Equifax, Experian, and TransUnion) to inform them of the fraud and to place a “Fraud Alert” on your credit report files. [https://www.consumer.ftc.gov/features/feature-0014-identity-theft](https://www.consumer.ftc.gov/features/feature-0014-identity-theft)


- Contact the California Attorney General’s Office to obtain useful information and forms including an ID Theft affidavit for submission to merchants. Additionally, contact the Federal Trade Commission to report the fraud and obtain a recovery plan. [https://oag.ca.gov/idtheft](https://oag.ca.gov/idtheft)

Alameda County Identity Theft Council
A free resource created to provide direct help for residents of cities across Alameda County who believe they are victims of identity theft. [http://identitytheftcouncil.org/alameda](http://identitytheftcouncil.org/alameda)

The DOJ Privacy Enforcement & Protection Unit focuses on California’s various privacy laws. The unit provides information related to Identity Theft, first steps if you believe that you have been victimized and ID Theft related forms, which include an Affidavit of Fraud. [https://oag.ca.gov/idtheft](https://oag.ca.gov/idtheft)

California Office of the Attorney General ID Theft Registry
California has established an Identity Theft Database to help victims of identity theft who have been wrongfully accused or associated with crimes. [https://oag.ca.gov/idtheft](https://oag.ca.gov/idtheft)

This publication was supported by funding awarded by the 2018 federal grant fund Increased Access to Services Award KU19010010 through California Governor’s Office of Emergency Services (Cal OES).
What is identity theft?

Identity Theft is the use of another person’s personal information without consent to do something that is illegal, such as opening a credit account in another’s name. 

https://www.consumer.ftc.gov/topics/privacy-identity-online-security  
https://www.equifax.com/personal/identity-theft-victim-assistance  
https://www.transunion.com/identity-theft

How thieves obtain your personal information:

- Auto and residential burglary.
- Theft of wallets and purses.
- Theft of mail: credit card and bank statements, checks, pre-approved credit offers and various other documents.
- Dumpster diving: sorting through garbage to collect documents containing personal information such as old bills and tax returns.
- Phishing & Smishing scams: phony emails or text messages requesting that you forward your information to them for an alleged legitimate purpose.
- Accessing your credit report by posing as a landlord, employer or loan officer, and ordering a copy of it.

How can I prevent identity theft?

- Obtain a “Security Freeze” with the three credit bureaus.  
  https://www.transunion.com/credit-freeze  
  https://www.experian.com/freezecenter.html  
  https://www.equifax.com/personal/credit-report-services/credit-freeze/
- Frequently review your bank statements, credit card statements and credit reports for fraud.
- Install a locking mailbox.
- Cross-shred your financial documents and paperwork before discarding them.
- Protect your Social Security number: never carry it in your wallet; if your health plan card uses your Social Security number, ask the company for a different number; do not give it out unless absolutely necessary.
- Do not give personal information over the Internet, by telephone or by mail unless you know exactly with whom you are dealing.
- Stop pre-approved credit offers by having your name removed from the credit bureau marketing list.
- Protect your personal information on your home computer. Use “strong” passwords with at least eight characters, including a combination of numbers and symbols. Use firewall, virus and spyware protection. Don’t click on links in pop-up windows or in spam e-mail.
- Be alert to “fake” ATMs and cash dispensing machines.

Signs that you may be a victim of identity theft:

- Your bills do not arrive as expected.
- You have been denied credit for no apparent reason.
- You receive unexpected credit cards or account statements.
- You receive calls or letters about purchases that you did not make.

Scam alert:

Be aware of scams and price gouging.  