LEGAL AID SOCIETY
OF SAN MATEO COUNTY
Phone | 650-558-0915
Fax | 408-517-8973
THE NATALIE LANAM JUSTICE CENTER
SOBRATO CENTER FOR NONPROFITS - REDWOOD SHORES
330 TWIN DOLPHIN DRIVE, SUITE 123
REDWOOD CITY, CA 94065
WWW.LEGALAIDSMC.ORG

PRIVACY & IDENTITY THEFT TIP SHEET

This tip sheet is for informational purposes only and does not constitute legal advice.

I. WHAT IS IDENTITY THEFT?

Identity theft occurs when someone takes your personal information without permission and commits fraud or other crimes using that information. For example, a person may use information such as your name, social security number, credit card number, address, etc. and then use that information to access your bank account, open other credit accounts, or even rent an apartment.

Identity theft is serious and its ramifications can last for many years into the future affecting your ability to get credit cards, loans, find places to rent, or even get jobs. As such, it is essential to protect yourself!

II. HOW DOES IT OCCUR?

Dumpster Diving. By searching your trash for bills or other paper with your personal information on them.

Skimming. Using a special storage device when processing your card to steal the card number.

Phishing. Thieves pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.

Changing Your Address. Thieves divert your billing statements to another location by completing a change of address form.

Old-Fashioned Stealing. Thieves steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and, new checks or tax information. Thieves steal personnel records, or bribe employees who have access.

Pretexting. Theives use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

III. HOW TO FIND OUT IF YOUR IDENTITY HAS BEEN STOLEN

Monitor existing financial accounts and bank statements for unauthorized activity and purchases
Regularly check your credit reports! If information on there is incorrect, call the credit bureaus to contest the information. Their numbers can be found in Part IV.
Identifying Information- The following may indicate that your identity has been stolen: if there are names, aliases or addresses listed that are not ones you have ever used; the social security number listed is not yours; the date of birth is incorrect, or the employers list includes employers you have never worked for.
Credit Accounts- Each credit account you have opened including credit cards, store credit cards, bank cards, loans, and mortgages should be listed. Watch out for accounts that you never opened or applied for as these are indicators of ID theft.
Credit Inquiries- In the inquiries section of your report it will contain a list of every institution that has requested your credit report within the last two years. Within that section is voluntary or authorized credit inquiries section. If in that section there are any companies that you never gave permission to have check your report, this could indicate that someone is trying to open accounts in your name.
Public Record and Collection Items- Bankruptcy, foreclosure, law suits, liens, wage garnishment, or judgments that you don't recognize as yours could indicate possible ID Theft.

In accordance with federal law under the Fair Credit Reporting Act, you are entitled to a free copy of your credit report once every twelve months and after placement of a fraud alert..
You can obtain all three credit reports for free by: calling 877-322-8228; **or** filling and mailing the Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 which can be printed out from ftc.gov/credit ; **or** by going online at www.annualcreditreport.com

IV. WHAT TO DO IF YOUR IDENTITY HAS BEEN STOLEN

Step 1- To prevent other accounts being opened in your name, call any one of the three credit bureaus to place a fraud alert on your account. That bureau is then required to inform the other two once the alert has been placed. Once you place an alert, it is active for 90 days and may then be renewed.
Transunion: 1-800-680-7289
Equifax: 1-800-525-6285
Experian: 1-888-397-3742

Step 2- Close accounts that you know or believe were opened fraudulently or tampered with by calling and speaking to someone in the security or fraud department of each company and asking that the account be flagged to show it was the result of ID Theft and ask that it be closed. Banks and credit card companies should be notified in writing. Keep copies of the letters and send them by certified mail, return receipt requested. A sample letter is available on our website.

Step 3: File an ID Theft complaint with the FTC at: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html; **or** by calling 1-877- ID THEFT (1-877-438-4338). Save the complaint reference number as it is necessary if you need to update the complaint information later

Step 4: File a Fraud Report with the police. The police report should contain specific details, so it is important to bring a printed copy of the FTC ID Theft complaint. The report can be used to permanently block fraudulent information that results from the identity theft from appearing on your credit report and prevent companies from collecting on debts that result from the ID theft or from selling them to a collection agency.

You can also request a credit freeze which makes it so that your credit report cannot be viewed by anyone unless you unfreeze the report. Note, there is a charge for this.

V. PREVENTATIVE MEASURES

Protect your Social Security Number- do not carry your card in your wallet or give out your number unless absolutely necessary. If unsure, ask why it is needed and if alternative forms of ID can be used.
Treat your trash and mail carefully- Shred anything with identifying information before throwing it away or recycling it. Deposit outgoing mail with identifying information directly in a post office box and empty your mailbox promptly. Also, delete files on your phone and computer that you no longer use and empty the recycling bin. Before tossing or selling electronics, erase all information on them.
Be Wary of the Internet- The internet can be a great resource but it can also leave you open to online scammers and ID thieves. Keep passwords private, limit the amount of information you share online, use strict privacy settings, and keep security software on your computer updated. For more information on how to protect yourself from online fraud, visit: www.OnGuardOnline.gov.
Protect your Passwords- Do not write them on your computer, debit cards, or anywhere that could be accessed by others. Combinations of letters, numbers, and characters make the strongest passwords. To increase strength even further, avoid using the same password for multiple accounts and avoid using personal information in the password such as birth date, mother's maiden name, etc.
Verify Sources- Don't give out information over the phone, internet, or mail unless you initiated the contact and you are sure of who you're dealing with. Verify websites by searching for them rather than cutting and pasting or clicking on a link. Verify callers by checking the phone directory or online.
Secure your Purse, Wallet, and Phone- Keep only absolutely essential cards and info in your purse/wallet. Keep your phone password protected. Keep all of these in secure locations.
Storage of Information- Put personal information in a secure place, especially if you have roommates, employ outside help, or are having work done on your house.

For More Information visit:
http://www.consumer.ftc.gov/