IDENTITY THEFT – WHAT IF IT HAPPENS TO YOU?

- Immediately contact the three major credit bureaus (Experian, Equifax, and Trans Union). Ask that your credit account be "flagged" for fraud. (This will require your prior notification if any credit accounts are to be opened using your personal information).
- Go through the required procedures of challenging any fraudulent account on your credit report.
- Directly contact the financial institution that issued the fraudulent account and file a fraud report.
- File a police report with your local jurisdiction. (You will need a police report number to challenge the fraudulent accounts).
- Change all of your financial account numbers (credit cards, bank accounts, new checks etc). Assume that all of your personal information has been compromised.
- Notify the Postal Inspect if someone changed your address without your consent. Notify the Postal Inspector of any fraud that was committed by using the mail system.

WHAT IF ITHAPPENS TO YOU? (CONTINUED):

- Notify the Social Security Administration of any fraudulent use of your social security number. Request a copy of your Earnings and Benefits statement and check it for accuracy.
- If your passport becomes stolen, or you suspect that it has been illegally used, contact the U.S. Department of State.
- Notify your telephone service provider if you discover fraudulent charges or calls that you did not make.
- If someone illegally used your driver's license, report it to the DMV immediately.

IMPORTANT RESOURCES

Equifax	800-525-6285
Experian	888-397-3742
Trans Union	800-680-7289
DMV (Fraud)	866-658-5758
Social Security	800-269-0271
US Postal Inspector	415-778-5800
Passport Fraud	202-955-0430
SFPD Fraud Detail	415-553-1521

SAN FRANCISCO POLICE DEPARTMENT

IDENTITY THEFT

QUESTIONS AND ANSWERS

San Francisco Police Department
Fraud Detail
850 Bryant Street, Room 419
San Francisco CA, 94103

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone uses your personal information to obtain credit, services, or goods without your permission.

The most common form of identity theft is when your social security number is used without your consent. However, there are cases where a person's driver's license, bank account numbers, telephone number, address, and name may be used for illegal purposes as well.

Why is my social security number so important?

Your social security number is your credit history "D.N.A.".

The major credit reporting bureaus use this number to keep track of your credit history. Banks and other financial institutions use your social security number to issue you credit or loans.

The IRS uses your social security number for your taxpayer identification numbers. Other institutions use this number as a customer identification number (gyms, libraries, department stores, insurance companies, doctor's offices, colleges, professional organizations etc.).

HOW CAN I PREVENT IDENTITY THEFT?

- Consider purchasing a shredder and shred all documents that contain personal information before throwing them in the garbage.
- NEVER place outgoing mail in your curbside mailbox. Try to find a nearby "blue" U.S. Postal Service Box to place your outgoing mail into.
- Consider getting a P.O. Box or receiving your mail at a work address. (The primary way thieves obtain your personal information is by stealing your mail).
- If you must have a curbside mailbox, consider purchasing a lockable mailbox (once the postal employee deposits the mail, only you can get it out with a key).
- Never carry your social security card in your wallet.
- Scrutinize anyone requesting your social security number. If an institution requests it, ask if it is a requirement.
- Never write your social security number on your checks.
- Do not use your social security number as a P.I.N. number for your ATM card (not even your last four numbers).
- Avoid using your mother's maiden name as a security question.
- Limit the amount of open lines of credit issued to you. Close open accounts that are inactive.
- Run a routine credit check on yourself and your spouse at least once every six months. Identify any questionable accounts and take action.
- Remember, sending your personal or financial information to anyone via email or fax is not secure.
- Be wary and suspicious of any solicitations of your personal or financial information.

Vigilance is the key to prevention.

While it is impossible to completely insulate yourself from becoming the victim of identity theft, you can take steps to significantly decrease your chances. Your personal and financial information is readily available to many people. It is up to you to monitor your credit, shred your documents, question those people who request information from you, and report suspicious and illegal activity.