IMPORTANT INFORMATION

Date Crime Discovered: _____

Date Crime Reported: _____

Officer: _____

Report No. _____

NOTES

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Pleasanton Police Department

Physical: 4833 Bernal Avenue

Pleasanton, CA 94566

Mail: P.O. Box 909

Pleasanton, CA 94566

Phone: (925) 931-5100

Fax: (925) 931-5480

(Rev. 02-2013)

IDENTITY THEFT

A Resource Guide From the Pleasanton Police Department

WHAT IS IDENTITY THEFT?

Identity Theft is defined by California Penal Code section 530.5 as any person who unlawfully obtains personal information of another and willfully uses that information for any unlawful purpose, such as to commit fraud.

In short, identity theft occurs when someone obtains your personal information without your knowledge or permission to commit fraud, theft or for any other unlawful purpose. Your personal information can be anything that identifies you; such as your name, social security number, credit card information, or other identifying information.

Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data, especially your social security number, bank account or credit card number, your telephone calling card number, and other valuable identifying data can easily be obtained by criminals and used so that criminals can profit at your expense.

For victims of identity theft or other fraud, this guide will assist you by providing contact information and steps you can take to clear your good name.

If you are not a victim, this guide will help you better protect your information and provide you with additional steps to prevent the fraudulent use of your personal information and the ruining of your good credit. Whether or not you are a victim, take the ID theft test on the back resource page to evaluate your vulnerability.

PREVENTIVE ACTIONS

How Thieves Get Your Personal Information And How To Prevent It

- They go through your garbage looking for un-shredded papers. ***SOLUTION:*** Always shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want, before placing it in the trash.
- They steal your mail. ***SOLUTION:*** Quickly remove mail from your mailbox or use a P.O. box. Deposit outgoing mail at the post office or in another secure receptacle.
- They listen in on conversations you have in public. ***SOLUTION:*** ALWAYS be aware of your surroundings.
- They buy your information either on the Internet or from someone who might have stolen it. ***SOLUTION:*** Regularly check your credit report for unauthorized accounts.
- They obtain your information from loan or credit applications, from files at hospitals, banks, schools, car lots or businesses that you deal with. They may have obtained it from dumpsters outside of such companies. ***SOLUTION:*** Ask questions of businesses you deal with as to how your information will be used and disposed of once it is no longer needed. Be aware of Assembly Bill 2246 (2000) , which requires all banks and businesses to destroy paperwork containing customer's personal and financial information. The business must destroy it by; 1) shredding 2) erasing 3) or modifying it in such a manner that it is unreadable or undecipherable. Customers can initiate civil action against the bank or business if they are the victim of identity theft or fraud as a result of businesses not destroying paperwork properly.
- They get it from your computer, especially those without firewalls. ***SOLUTION:*** Always use a firewall and virus protection on your computer when connected to the Internet. Keep all programs updated, including your operating system (i.e., Windows 98 , XP , etc.)
- They may be a friend or relative or someone who works for or with you who has access to your information. ***SOLUTION:*** Do not allow anyone you don't fully trust access to your computer or personal information.

Additional Ways of Reducing Access to Your Personal Data

To reduce the amount of personal information that is out there, consider the following:

- Remove your name from the marketing lists of the three credit reporting bureaus -- Equifax, Experian (formerly TRW) , and Trans Union. This will limit the number of pre-approved credit offers that you receive. These, when tossed into the garbage, are a potential target of identity thieves who use them to order credit cards in your name. Call 1-888-567-8688 for more information or go to www.optoutprescreen.com.
- Sign up for the Direct Marketing Association's Mail Preference Service and the Telephone Preference Service. Your name is added to computerized name deletion lists used by nationwide marketers.

Credit Cards

DO NOT USE any credit card linked to any of your bank checking and/or savings accounts (i.e., MC/VISA debit cards). You are not afforded the same protections as a credit card (MasterCard, Visa, American Express). Do not toss credit card receipts into a public trash container.

Reduce the number of credit cards you actively use to a bare minimum. Carry only one or two of them in your wallet. Cancel all unused accounts because the cards are unused, the account numbers are recorded in your credit report, which is full of data that can be used by identity thieves.

Keep a list or photocopy of all your credit cards, the account numbers, expiration dates, and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your cards have been stolen. Do the same with your bank accounts.

Passwords and PINS

When creating passwords and PINS (personal identification numbers), do not use the last four digits of your social security number, your birth date, middle name, pet's name, consecutive numbers, or anything else that could easily be discovered by thieves.

Memorize all your passwords. Don't record them on anything in your wallet or purse.

Shield your hand when using a bank ATM machine or making long distance phone calls with your phone card. "Shoulder surfers" may be nearby.

Never give out your credit card number or other personal information over the phone unless you have a trusted business relationship with the company and you initiated the call.

Social Security Numbers

Your social security number (SSN) is the key to your credit and banking accounts and is the prime target of criminals. Protect your SSN. Release it only when necessary (i.e. tax forms, employment records, stock and property transactions). Do not carry your SSN in your purse or wallet.

Do not have your SSN printed on your checks. Don't let merchants write it onto your checks because of the risk of fraud.

Request your Social Security Earnings and Benefits Statement once a year to check for fraud.

Responsible Information Handling

Carefully review your credit card statements and phone bills including cellular phone bills, for unauthorized use.

Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including the account number, your phone number and driver's license number. Never permit your credit card number to be written onto your checks. It's a violation of California law (California Civil Code 1725) for retailers to do this and puts you at risk of fraud.

Request a copy of your credit report and review it for any discrepancies. If you notice any discrepancies, contact the credit bureau to dispute the discrepancies.

Starting December 1 , 2004 the **Fair Credit Reporting Act** allows you to get one free comprehensive disclosure each year of all of the information in your credit file from each of the three major credit bureaus.

www.annualcreditreport.com

Internet and On-Line Services

Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any web site or on-line service location unless you receive a secured authentication key from your provider. Look for the security features on the Internet browser you are utilizing when entering personal information or login information.

When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don't give them out!

Avoid responding to or clicking on emails that advise you that you need to provide your personal information or risk the closure of your account. These emails are known as "phishing" emails , they are designed by fraudsters to obtain your personal information.

WHAT TO DO IF I BECOME A VICTIM?

Contact all creditors, by phone and in writing, to inform them of the problem. Use the following letter format to dispute fraudulent charges to your credit history or accounts.

Sample Dispute Letter — Credit Bureau

Date

Your Name, Address, City, State, Zip Code

Institution Name, Address, City, State, Zip Code

Ref: (Account number if known)

To Whom It May Concern:

I am writing to dispute a fraudulent charge (or debit) attributed to my account in the amount of $_____. I am a victim of identity theft, and I did not make this charge (or debit). I am requesting the charge be removed (or the debit reinstated), that any finance or other charges related to the fraudulent amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as police report) supporting my position. Please investigate this matter and correct the fraudulent charge (or debit) as soon as possible.

Sincerely,

CREDIT BUREAUS	
Trans Union	**Order Credit Report: 800-888-4213** **Report Fraud: 800-680-7289**
Experian	**Order Credit Report: 888-397-3742** **Report Fraud: 888-397-3742** **www.experian.com**
Equifax	**Order Credit Report: 800-685-1111** **Report Fraud: 888-766-0008** **www.equifax.com**

Contact each of the three credit bureaus' fraud units to report identity theft. Ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts. Request that a copy of your credit report be sent to you.

An "Initial Fraud Alert" lasts 90 days and requires creditors to follow certain procedures before issuing credit.

An "Extended Fraud Alert" lasts 7 years and requires ID Theft Police Report.

Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Request a free copy of your credit report every few months so you can monitor any new fraudulent activity.

Advise your bank to flag your accounts and contact you to confirm any unusual activity. Request a change of PIN and a new password.

If you have any checks stolen or bank accounts set up fraudulently, report it to one of the following companies:	
National Check Fraud Service	**843-571-2143**
Shared Check Authorization Network	**800-262-7771**
TeleCheck	**800-710-9898**
CheckRite	**800-766-2748**
International Check Services	**800-526-5380**

Contact the Social Security Administration's Fraud Hotline at 1-800-269-0271.

Contact the state office of the Department of Motor Vehicles to see if another license was issued in your name. If so , request a new license number and fill out the Department of Motor Vehicles' complaint form to begin the fraud investigation process.

- Obtain a description of the suspect (if known)
- Obtain witness information
- Keep a log of all your contacts and make copies of all documents
- What is your financial loss? Attach all supporting documents

Make note of this case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report. Depending upon the location (jurisdiction) of where the crime occurred (goods or services obtained or delivered), an investigator may or may not be assigned to this case.

If the crime occurred in our jurisdiction and there are workable leads, such as witnesses and suspect information, an investigator will be assigned to the case. Unfortunately, all cases will not be actively investigated if significant leads are not present.

WEB RESOURCES	
Federal Trade Commission	**ww.ftc.gov** **www.ftc.gov**
ID Theft Center	**www.idtheftcenter.org**
Privacy Rights Clearinghouse	**www.privacyrights.org**
Social Security Administration	**www.ssa.gov**
U.S. Postal Service	**www.usps.gov**
Direct Marketing Association	**www.the-dma.org**
CA Dept. of Consumer Affairs	**www.dca.ca.gov**
CardCops	**www.cardcops.com**

ARE YOU AT RISK FOR IDENTITY THEFT?
Test your "Identity Quotient"

I receive several offers of pre-approved credit every week. **(5 points)** Add 5 more points if you do not shred them before putting them in the trash.

I carry my Social Security card in my wallet. **(10 points)**

I do not have a P.O. box or a locked, secured mailbox. **(5 points)**

I use an unlocked, open box at work or at my home to drop off my outgoing mail. **(10 points)**

I carry my military ID in my wallet at all times. **(10 points)**

I do not shred or tear banking and credit information when I throw it in the trash. **(10 points)**

I provide my social security number (SSN) whenever asked, without asking questions as to how that information will be safeguarded. **(10 points)** Add 5 points if you provide it orally without checking to see who might be listening.

I am required to use my SSN at work as an employee or student ID number. **(5 points)**

I have my SSN printed on my employee badge that I wear at work or in public. **(10 points)**

I have my SSN or driver's license number printed on my personal checks. **(20 points)**

I am listed in a "Who's Who" guide. **(5 points)**

I carry my insurance card in my wallet and either my SSN or that of my spouse is the ID number. **(20 points)**

I have not ordered a copy of my credit reports for at least 2 years. **(10 points)**

I do not believe that people would root around in my trash looking for credit or financial information. **(10 points)**

Each one of these questions represents a possible avenue for an ID theft.

100 + points — More than 500 ,000 people will become victims of ID theft this year. You are at high risk. We recommend you purchase a paper shredder, become more security conscious in document handling, and start questioning people need your personal data.

50-100 points — Your odds of being victimized are average, or higher if you have good credit.

0-50 points — Congratulations. You have a high "IQ." Keep up the good work and don't let your guard down.