What is Identity Theft?

Identity theft means the theft of a consumer’s personal identification and/or credit information, which the thief uses to gain access to the victim’s credit and bank accounts and takes over the victim’s credit identity. The perpetrator may use this information to obtain money, credit, goods, services and other things of value in the victim’s name.

WHAT TO DO WHEN IT HAPPENS TO YOU

• File a police report with your local police department. Request a copy of the police report for proof of the crime.
• Set up a folder to keep a detailed history of the crime.
• Keep a log of all your contacts including the case number from the police department, all names, dates, and times. Make copies of all documents that are mailed out to creditors. Use certified mail when sending information to creditors.
• Close all existing credit card accounts. Have the creditors note on the account that it was closed at the customer’s request, not lost or stolen. By saying the latter, it takes the blame off the victim.
• Some creditors may request for fraud affidavits to be notorized. A written statement and supporting documents should be sufficient to prove the identity theft.

• Contact all creditors, by phone and in writing to inform them of the problem.
• Notify your bank to verify any unusual activity. Request a change of PIN and passwords to your accounts. If any checks are stolen or missing report to the following companies:
  - Check Rite 800-766-2748
  - Chex Systems 800-428-9623
  - Cross Check 800-552-1900
  - Equifax 800-437-5120
  - National Processing Company 800-526-5380
  - SCAN 800-262-7771
  - Telcheck 800-366-2425
• For any license number misuse, contact your local DMV at 800-777-0133.
• For Social Security number misuse, contact 800-269-0271.
• Notify the US Postal Inspector if your mail has been stolen or tampered with. Call 916-263-7240. www.usps.gov/websites/depart/inspect

• Submit the following letter to any creditor that is requesting money. Do not pay any amount that the perpetrator created.

Dear (Creditor/Collection Agency Name):

On (Date), I received your letter demanding payment of (dollar amount). I did not open this account and incur this unpaid balance. Someone, other than myself, wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/services to someone, other than myself. Your company is a victim and should file a police report in the appropriate jurisdiction.

You are hereby notified that on (Date), I filed an identity theft report with the Sacramento Police Department. The case number is (report #). The report can be verified by calling the SPD Records Division at 916-433-0620.

Sincerely,

(Your name and address)

• Report the incident to the Federal Trade Commission (FTC) www.consumer.gov/idtheft

• Often times, victims are either criminally prosecuted for their perpetrator’s actions in identity theft cases or the creditors attempt to seek civil actions for their losses. If this occurs, contact the local court where the matter is being held. If prosecution is still being pursued, contact the California Department of Justice or the Federal Bureau of Investigations to see how to clear your name.

• Call the fraud units of the three credit bureaus and ask to have a “Fraud Alert or Security Freeze/Victim Impact” statement placed on your credit file.
  - Experian (formerly TRW) 888-397-3742
  - Equifax 800-525-6285
  - Trans Union 800-680-7289
Preventive Actions

- Activate the security freeze for $10 each with the three major credit bureaus (Experian, Equifax and Trans Union.) By utilizing the security freeze, a perpetrator cannot apply for credit in your name and the applicant will be rejected. Also request to opt out of pre-approved mailings for credit cards.

- Order your credit report from the three credit bureaus at least once a year to check for fraudulent activity or other discrepancies.

- Promptly remove mail from your mailbox after delivery. If you live in an area where mail theft is a problem, consider a post office box.

- Deposit outgoing mail in post office collection mailboxes or at your local post office. Do not leave it in your mailbox to be picked up.

- Notify credit card companies and financial institutions prior to a change in address or phone number.

- Shred pre-approved credit applications, credit card receipts, bills and other financial information.

- Empty your wallet of extra credit cards and ID’s, and cancel the ones you do not use.

- Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gas pumps.

- Never give personal information over the telephone. All legitimate financial institutions will already have this information.

- Do not carry any passwords or your social security card in your wallet or purse.

- Do not throw away old or unused checks. Shred them.

- Be on guard against fraudulent e-mails pretending to be from well known companies such as eBay or PayPal that attempt to get your personal information (credit card numbers, etc.).

- The less you write down your SSN, the better off you will be.

- Check your credit statements monthly for any suspicious activity.