

In dealing with the authorities and financial institutions, keep a log of all conversations, including dates, times, names, and phone numbers. Note the time spent and any expenses incurred. Confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents. Once you discover you are a victim of identity theft you should notify the following:

1. Credit Bureaus. Immediately contact the fraud units of the three credit reporting companies— Experian, Equifax, and TransUnion. Report the theft of your credit cards or numbers. The contact information is provided at the end of this brochure. Ask that your account be flagged or a credit freeze placed on your credit report. Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. The credit bureaus will provide you with a free copy once a year so you can monitor your credit report. Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened and for them to remove the inquiries that have been generated due to the fraudulent access.

2. Creditors. Contact all creditors immediately with whom your name has been used fraudulently— by phone and in writing. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

Creditor's Requirement to Report Fraud. You may be asked by banks and credit grantors to fill out and notarize fraud affidavit, statements or supporting documentation.

3. Law Enforcement. Report the crime to the law enforcement agency servicing your area. Give them as much documented evidence as possible. Get a copy of your police report or the report number issued by the agency. Keep the report number of your police report handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report to verify the crime.

January 1, 1998, California Penal Code Section 530.6 mandated California police agencies to take identity theft reports from victims who reside in their respective jurisdictions. Investigative jurisdiction will be determined by your law enforcement agency.

4. Stolen Checks. If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Password protect the account.

5. ATM Cards. If your ATM card has been stolen or is compromised, get a new card, account number, and password. Do not use your old password. When creating a password, don't use common numbers like the last four digits of your social security number or your date of birth? Always check the card reader for signs of tampering and never expose your password.

6. Fraudulent Change of Address. Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud. Find out where the fraudulent credit cards were sent. Notify the local Postmaster for the address to forward all mail in your name to your actual address. You may also need to talk to the mail carrier.

7. Social Security Number Misuse. Call the Social Security Administration to report fraudulent use of your social security number. Also order a copy of your Earnings and Benefits Statement and check it for accuracy.

8. Passports. If you believe your passport has been compromised, notify the US Department of State, passport office.

9. Phone Service. If you discover fraudulent charges on your bill contact the provider immediately. Request a password be placed on your account to protect it from being changed.

10. Driver license number misuse. You may need to change your driver's license number if someone is using yours as identification on bad checks. Contact the state office of the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Also, fill out the DMV's complaint form to begin the fraud investigation process. Send supporting documents with the complaint form to the nearest DMV investigation office.

11. False civil and criminal judgments. Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil or criminal judgment has been entered in your name for actions taken by your imposter, contact the court where the judgment was entered and report that you are a victim of identity theft.

Top 10 Ways to prevent **Identity Theft**

1. Use a secure Internet connection (no free wifi) when entering in your personal information.

2. Do not reply to unfamiliar emails or calls; also, do not click on any unfamiliar links or documents.

3. Shred documents/paperwork with personal information before discarding.

4. Check your mailed monthly statements or balances online.

5. Pull your credit report once a year from each credit bureau.

6. Record your doctor's visits, procedures, perscriptions and then compare to your insurance bills and explanation of benefits.

7. Follow up on any dental credit.

8. Notify creditors or financial institution of any unauthorized transactions.

9. Place a fraud alert or credit freeze.

10. If it seems too good to be true

IT PROBABLY IS!