

DO....

- Shred all personal and financial information (bank statements, ATM receipts, credit offers, credit card bills etc.) before discarding.
- Keep your personal information in a secure location.
- Call the post office immediately if you do not receive your mail.
- Be aware of others nearby when entering your PIN number at ATM machines.
- Limit the number of credit cards and personal information you carry in your purse/wallet.
- Report lost/stolen credit cards immediately.
- Cancel all inactive credit cards.
- If you have applied for credit and have not received the card on time, immediately report it.
- Closely monitor the expiration dates on your credit cards. Contact the creditor if your replacement cards have not arrived.
- Review your credit report twice per year to safeguard your identity.
- Use non-standard passwords on your accounts.
- Avoid using maiden names, birth dates, children's names, and social security numbers.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.
- Avoid using your social security number for any identification purposes.

DON'T....

- Volunteer any personal information when using your credit cards.
- Give your social security number, credit card number, or bank account numbers over the phone unless you have initiated the call and know who you are speaking to.
- Leave receipts at ATM'S, bank counters or gasoline pumps.
- Leave envelopes containing your credit card payments in your home mailbox.
- Disclose bank account numbers, credit card numbers, or other personal information on any web site you have not initiated or have not authenticated from your service provider.

SAMPLE DISPUTE LETTER

Date

Your name, address, city, state, zip code
Institution name, address, city, state, zip code
Ref: account number

Law enforcement case number

To Whom It May Concern:

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

Enclosed are copies of (police report, documentation etc.) supporting my position. Please investigate this matter and correct the fraudulent charge as soon as possible.

FOR YOUR RECORDS

Credit Card Name	Account Number
_____	_____
Phone Number	Dept. Case Number
_____	_____
Credit Card Name	Account Number
_____	_____
Phone Number	Dept. Case Number
_____	_____

IDENTITY THEFT



KERN COUNTY SHERIFF'S DEPARTMENT

RESOURCE GUIDE FOR PREVENTING AND REPORTING IDENTITY THEFT

This brochure is a publication of the
Kern County Sheriff's Department
Crime Prevention Unit
(661) 391-7460

HOW THIEVES GET YOUR INFORMATION

- **Online Data** — On the simplest level, thieves access data that consumers share through phone listings, directories, memberships etc. Thieves can also purchase sensitive information about someone (name, address, phone numbers, Social Security number, birth date etc.) from an online broker.
- **Direct Access to Personal Documents in the Home** — Unfortunately, there are identity thieves who can gain legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends, etc.
- **Purse/Wallet Theft** — Stolen purses and wallets usually contain plenty of bankcards and personal identification. A thief can have a field day using this information to obtain credit under the victims name or sell the information to an organized crime ring.
- **Dumpster Diving** —Thieves rummage through trash cans searching for pieces of un-shredded personal information that they can use or sell.
- **Mail Theft** – Crooks seek out and steal from unattended/unlocked mail boxes to obtain pre-approved credit card offers, bank statements, tax forms, and checks.
- **Inside Sources** — A dishonest employee with access to personnel records, payroll information, insurance files, account numbers and/or sales records can wreak havoc.
- **Imposters** — Many identity theft victims have been taken in by individuals who posed as someone with legitimate or legal reason to access the victims personal information.

What Should I Do If I Become A Victim Of Identity Theft?

1. Make a single toll-free call to one of the national credit bureaus.

You only make a single toll-free call to any one of the three credit bureaus. That credit bureau will notify the other two of the crime.

Within 24 hours all three credit :

- Place a fraud alert on the victim's credit report.
- Opt the victim out for all pre-approved offers of credit for two years.
- Provide a free copy of the victim's credit report within three days.
- Verify with the victim all information on the

CREDIT BUREAU CONTACT INFORMATION

EQUIFAX

www.equifax.com

888-766-0008 (Fraud Hotline)

800-685-1111 (Report Order)

EXPERIAN

www.experian.com

888-397-3742 (Fraud Hotline)

888-397-3742 (Report Order)

TRANSUNION

www.transunion.com

800-680-7289

800-916-8800

2. File a police report.

Get a report number and/or copy of the report should anyone request proof of the crime.

3. Contact the fraud departments of your creditors.

(e.g., credit card issuers, phone companies, utilities, banks and other lenders). Describe your identity theft problem and follow up with a letter or affidavit. This is very important for credit card issuers, since the consumer protection law requires cardholders to submit disputes in writing.
4. File a complaint with the federal Trade Commission (FTC).

The FTC handles complaints from victims of identity theft, provides information to those victims, and refers complaints to appropriate entities, including the major credit-reporting agencies and law enforcement agencies.

The ID Theft Affidavit is a special tool developed to help simplify the ID theft reporting process for consumers. It is a standard form that can be used by victims to report the same information to different companies, such as the three major credit bureaus, and other banks or creditors where an account has been opened and/or used under the victim's name.

FTC CONTACT INFORMATION

www.consumer.gov/idtheft

877-IDTHEFT

877-438-4338

5. Take appropriate actions, depending on your identity theft circumstances.

If you suspect:

- Your mail has been stolen to obtain bank or credit card statements... File a report with the U.S. Postal Inspection Service Office.
- A thief has changed a billing address on a credit card account... Close all accounts that have been tampered with, request new PIN's and passwords.
- Your social security number has been stolen...Contact the nearest Social Security Administration Office to report the suspected abuse.