Kern County Sheriff's Office
Documentary Evidence

A Criminal Investigation can not be started until documentary evidence is submitted.

Documentary evidence are the record that most businesses keep, which provide useful leads (information) specific to the transaction AND that can be tracked.

Documentary Evidence includes;

- **Telephone caller ID information.**
- **Internet Protocol (IP) Address, time, date, and time zone of computer used to communicate over the internet.**
- **License Plates**
- **Signature Documents**
- **Business Notes documenting conversations, phone numbers, and names.**
- **Invoices, orders, other documents which show changes of address, telephone numbers, names, and ship to addresses or names.**
- **Bank account numbers, credit card or checking account numbers used in conjunction with the fraud.**
- **The purchase receipts and information which shows what was fraudulently purchased, where it was purchased and the date and time it was purchased.**

Although still important in a investigation, Documentary Evidence IS NOT;

- **Surveillance video (unless you know the person in the photograph).**
- **The bill by which you discovered the fraud.**
- **The notice of payments due or account collections notice.**
- **Or, your credit report.**

Documentary evidence must be requested by YOU from EACH business your account or personal information was used at. Some businesses will send the

information to you directly, while **others** will only send it to the Sheriff's Office.
Be sure to;

- **Clarify** with the business **where they will send** the information and when.
- **Write down** the name and direct phone number of the person you spoke to.
- **Write down** any reference number the business uses to track your claim.

To assist you, the Kern County Sheriff's Office has developed a Identity Theft Kit. This kit contains a form "A" which you can send to each business to request the evidence. The kit also serves as a crime report and is only available by reporting the crime and receiving a case number. Also in the kit is a form to help you keep track of who you have been talking to. Be sure to mention to the business that you need any records that may include;

- **Telephone caller ID information**
- **Internet Protocol (IP) Address, time, date, and time zone of computer used to communicate over the internet**
- **Invoices, orders, other documents which show changes of address, telephone numbers, names, and ship to addresses or names.**
- **Receipts**

I

BEFORE YOU INFORMATION IS STOLEN

As a first step in preventing unnecessary hassle**, lay out all the cards you carry on a photocopier and make a copy. Then turn your cards over and make another copy.** Keep these copies at home so if the cards are ever lost or stolen, you will know exactly what was in your wallet, and you will have instant access to contact numbers for notifying the appropriate agencies.

Identity theft and fraud crimes are perceived to be low-risk crimes that can have high payoffs for perpetrators. Advances in technology have made personal information more usable than ever, leading criminals to profit from sophisticated. It is easy to understand why identity theft is the fastest-growing.

Horror stories abound about fraud that can be committed using your name, address, social security number (SS#), credit cards, and so on after the loss or theft of a purse or wallet. You may also experience the misuse of your accounts through mail theft or theft of your ID in another way (stolen carbon slips, or from the Internet, for instance).

Nationwide, an estimated 500,000 to 700,000 people become victims of ID theft each year. An average victim spends $800 to clear up discrepancies related to the theft, and spends an average of 175 hours over 23 months to get things straight! The longer you delay, the more time and money it takes to fix the problem.

Protecting your private information

Knowing how an Identity Thief can get your information is one step to prevention

Here are some of the ways that have been used by identity thieves to get the information they need in order to do their dirty work.

- **Stolen mail and trash (dumpster diving)**

Curbside recycling in some neighborhoods means that all the "good stuff" for identity thieves is no longer mixed-in with the garbage. Consider using a shredder for your more sensitive information.

- Bank statements
- Credit card statements
- Pre-approved credit offers
- Telephone calling cards
- Tax information

- Pay stubs
- Credit card carbons
- Stolen trash of a business

Suspect often divert unsuspecting victim's mail by completing/forging a mail forwarding card. Resulting in your mail going where the thief wants it. If your mail suddenly stops coming, immediately contact the local post office to see why.

If a mailbox theft occurs, that's a Federal crime and you can get the Feds on your side. Contact your local postmaster, or see the U.S. Postal Inspection Service website.

To help prevent theft, deposit mail in post office collection boxes, not your own mailbox. Quickly remove mail from your mailbox after delivery, and request mail be held when you're gone.

- **"Pretext" calls**

Pretext calls are where the thief poses as your bank, internet service provider, or other organization with which you may or may not have had financial dealing and they call you to "verify your account information" because of a problem they had with their "records system."

- ***Fraudulently Obtained Credit Reports***

Your credit report is a gold mine of information. Fortunately, the credit reporting agencies have become much more careful about the information that is divulged, and more careful about the types of businesses eligible to get credit information.

Credit Reports Don't Tell All - But They Tell a Lot
Account numbers are normally disguised by asterisks in place of some of the digits, and your social security number is not revealed unless it is already known by the requestor of the report. Still, a credit report gives a lot of background information that would help an identity thief to impersonate you.

Your best defense is to check for suspicious inquiries on all three of your credit reports. A suspicious inquiry is one that is **not** the result of **you** applying for credit (or a job, or an apartment.)

- **Internet transactions on unsecured sites**

Transactions on unsecured sites or with illegitimate companies **posing** as a reputable "safe" business with which you may do business. They pretend to be conducting a transaction but are only collecting information.

- **Responding to links in unsolicited e-mails**

Never use the links sent to you in a e-mail that you did not solicit. These links will spoof a legitimate web site (make it look like the real site) so you enter information they want. The e-mails will **pretend** to be concerned with the security of something you MAY have utilized, (Ebay, your bank, a order from a large company, a membership) asking you to verify you personal information. **If you "verify"** the information via the link, you are giving your personal information to the thieves, not the company they are pretending to be. The best defense against this kind of attack to NEVER use the link in a e-mail, to use the companies normal web sites, AND/or to telephone the company for verification.

Old-Fashioned Theft

- Stolen wallet
- Stolen purse
- Burglarized Vehicle
- Burglarized gym locker
- Burglarized home or office
- Stolen car
- Stolen briefcase
- Stolen computer

On the bright side, if a physical theft has occurred, you'll find it easier to get help from the local police department. Still, there are important steps you should take after a theft (and important things you should do before a theft has occurred, if possible.)

Other Dangers

- Dishonest but trusted **employees** with access to your records.
- Dishonest **care giver** for elderly or infirmed.
- Dishonest workers with access to your home. (Don't leave your information open to view, even at home.)
- Dishonest **family** members and friends

  In the Kern County Sheriff's Office jurisdiction the predominant common denominator in identity theft and fraud cases is DRUG USE/ABUSE. (If you know a drug user/abuser; illegal, recreational or prescription, be particularly careful.)

- Information carelessly divulged by you. (Never email your social security or credit card number.)
- Information stolen (or "hacked") from a legitimate business or website.

- Email, instant messages, or rogue websites that trick you into divulging your personal information
- Misdirected emails and faxes you may have sent

If you have good credit, and many times, even if you don't, you are the target market of some group of financial institutions. As a result, you may often get "pre approved" offers for credit cards and other kinds of loans in the mail.

You may think that if they're not filled-out, they're useless to an identity thief -- so you toss them into the trash.

What can you do/ Protecting Yourself

Knowing how the thieves get the information, it is now clear how best to protect that information: you should begin immediately to practice these simple steps:

1. Protect your Social Security number, credit card numbers, account passwords and other personal information.

Use common sense, and be suspicious when things don't seem right. Never divulge your information over the phone unless you initiated the phone call. If personal information is requested ask questions. It is your right to know why it's needed, how it will be used, and who needs it.

If you get an unsolicited offer that sounds too good to be true it probably is! If a caller claims to represent your financial institution, the police department or some similar organization and asks you to "verify" (reveal) confidential information, hang up fast and consider reporting the incident. Real bankers and government investigators don't make these kinds of calls.

2. Minimize the damage in case your wallet gets lost or stolen.

Don't carry around more checks, credit cards or other bank items than you really need. Limit the number of credit cards you carry by canceling the ones you don't use. Don't carry your Social Security number in your wallet or have it pre-printed on your checks. Pick passwords and Personal Identification (PIN) numbers that will be tough for someone else to figure out-don't use your birth date or home address, for example. Don't keep this information on or near your checkbook, ATM card or debit cards. Also, don't leave your wallet unattended in a store, restaurant, office or other public place even for a few minutes.

3. Protect your incoming and outgoing mail.

Promptly remove mail from your mailbox after it has been delivered. If you're going on vacation have your mail held at your local post office or ask someone you *know and trust* to collect your mail. Deposit outgoing mail in the Postal Service's blue collection boxes, hand it directly to a mail carrier or take it to a local post office. Do not deposit mail in a full mail box and do not send it from your home mail boxes, including the large community boxes.

According to Postal Inspector, when writing checks use "gel-ink" pens. Currently they have found that checks written using "gel" ink are unable to be chemically erased and therefore more difficult to forge or counterfeit.

4. Keep thieves from turning your trash into their cash.

"Dumpster divers" pick through trash looking for pre-approved credit card applications and receipts, canceled checks, bank statements, expired charge cards and other documents or information they can use to counterfeit or order new checks or credit cards. To keep these from happening use a "cross-cut" shredder and shred any document that contains any part of or all of your personal information. "Cross-cut" shredding makes confetti out of the documents and makes it virtually impossible for the thief to paste them back together.

5. Practice home security.

Safely store extra checks, credit cards, bank statements, or other financial documents. Consider using a document safe for these items. Don't advertise to burglars that you're away from home. Use timers on your lights and temporarily stop delivery of your newspaper *and mail* or ask a *trusted* neighbor to pick up any items that may arrive unexpectedly at your home.

6. Pay attention to your bank account statements and credit card bills.

ALWAYS check into discrepancies in your records or if you notice something suspicious, such as a missing payment or an unauthorized withdrawal. Also, contact the appropriate institution if a bank statement or credit card bill doesn't arrive on time because that could be a sign someone has stolen account information and changed your mailing address in order to run up big bills in your name from another location.

7. Review your credit report approximately once a year.

Monitor your credit report for accuracy, looking for unauthorized bank accounts, credit cards, purchases, etc. Look for anything suspicious in the section of your credit report

that lists who has received a copy of your credit history. This may be an indication a thief is trying to obtain fraudulent benefits, or is merely casing you as a viable victim.

To order your report, call the three major credit bureaus at these toll-free numbers: Equifax at (800) 685-1111, Experian at (888) 397-3742, or Trans Union at (800) 888-4213. By law, the most you can be charged for a copy of your report is $8.50. To be safe, consider getting a copy from each of the three companies.

8. Practice "on-line" or internet safety.

Be suspicious of web offers that "seem to good to be true." Ensure the web site you are using is legitimate, or has been formally examined and certified secure and reliable by a legitimate certifying agency such as the Better Business Bureau or the like.

Use your credit card and social security number only when absolutely necessary. Only use websites who you believe are using secure communication links that are encrypted (scrambled). Again, keep your PIN numbers and passwords confidential, and DON'T write them down and leave them next to, on or near your computer. (prevention information paraphrased from the FDIC Consumer News - Summer 2000)

Credit Report

- Request a copy of your credit report every year or so. It tells you whether anyone has applied for credit in your name, and may reveal accounts being used without your knowledge, with the bill being sent to a different address.

Credit Cards

- Sign new cards immediately.
- Store them safely - They are money!
- Only carry the cards you will use.
- Don't write your PIN # on your card.
- Shred documents that show your account number before discarding.
- Don't give your card number over the phone, unless you initiated the call.
- Remember to get your card and receipt after a purchase, and double check they are yours.
- Notify the credit card company immediately if your bill is incorrect, or your card is lost or stolen.
- Check your bill carefully, and notify the credit card company if you don't receive it on time.

Mail

- Don't write your credit card number or social security number on a postcard or the outside of an envelope.
- Collect your mail promptly.
- Have your mail held if you'll be out of town or on vacation.
- Use collection boxes or the post office for outgoing mail if your home mailbox is unattended.
- Opt-out of receiving pre-approved credit offers

Internet

- Never e-mail your credit card number or social security number.
- Check carefully that you are on the page you intend, and not an impostor's page.
- Use only secure web pages for online ordering. (You should see the padlock on the status bar of Microsoft Internet Explorer pages where a credit card number is requested.)
- Online credit applications which request a social security number should also be on secure web pages. (Look for the padlock.)
- Use anti-virus and personal firewall software, and keep it updated.

Do you know what PMB Means?

Private post office box services have sometimes been a tool for fraudulent activity, including identity theft. The thief would change the victim's address so bills for the credit opened in the victim's name would go to the bogus mail drop. Now the U.S. Postal Service is requiring that, for delivery, **PMB** (private mail box) be indicated on in the address (or return address), and that two forms of identification be used (including photo ID) when opening accounts at mail box services.

Social Security Numbers

"Social Security numbers often represent the entry point for rip-off artists and identity thieves."

To an identity thief, your social security number is perhaps the most important piece of information about you.

Your SSN is important because a credit check is generally required to get new credit in your name. When a financial institution or business runs a detailed credit check on you, credit bureau policies commonly dictate that the inquiry cannot be made without a social security number.

What Social Security Says

The Social Security Administration says they will not help you restore credit that has been damaged by an identity thief. They recommend working with each credit bureau, creditor, employer and government agency involved to remove inaccurate information from your records, and then to watch for suspicious activity on an ongoing basis.

"You should continue checking your credit report annually for inaccuracies." Says the SSA.

Keep copies of your correspondence, records of your telephone calls and other documents verifying your efforts to correct the problem.

See Also: How to find out if someone stole your Social Security number to get a job...

Can You get a new SSN?

It is quite likely that a new social security number **will not resolve** your problems related to identity theft. In most cases, changing your SSN is not recommended. The SSA, only in certain cases, will issue a new number. Their yardstick for making the decision is...

"...if, after making all efforts to resolve the problems caused by someone else's misuse of your Social Security number, you are still being disadvantaged by the misuse."

A new Social Security number will be issued only if you can **prove** that someone else has stolen your number **and is using it** illegally.

If your card has been lost or your number has fallen into the wrong hands, that's generally not enough. You must provide evidence that the number is actually being misused, and that the misuse is causing you harm.

Of course, the Social Security Administration will not give you a new SSN to aid in avoiding legal responsibility, or in hiding bad credit or a criminal record.

How to get a new Social Security Number

To get a new SSN, you must visit your local Social Security field office. There is no fee.

Warning: People or companies offering to obtain a Social Security number for a fee are usually scams. If they supply a fraudulent number, your use of it could constitute a crime