SCAMMED! Will you be a victim of Identity Theft?

Identity Theft
The Fastest Growing Crime in Our Nation Today

What is Identity Theft?

Identity theft occurs when an imposter takes your personal data –usually your name, Social Security number (SS#), driver's license number, address and/or birth date - and uses it for his/her own financial gain. This person(s) may apply for telephone service, credit cards or loans, buy merchandise, lease cars or apartments and even use your identity to gain employment - working as you. They might even try to fool police into believing that they are you when being arrested or being given a ticket. Identity theft is a dual crime. Both the person whose identity has been used and the credit grantor are victims. Persons found guilty of this crime may be punished with a fine and/or imprisonment - (PC 529 and 530.5).

Can this happen to me?

Yes. Experts estimate there were 700,000 - 1 million new victims nationwide in 2001. The Federal Trade Commission has declared identity theft the fastest growing crime today and it is considered a national crisis. In 2001, California was second only to the District of Columbia in the number of identity theft reports per capita.
There are many ways that thieves can steal your identifying information. It can be as high tech as computer hacking or as low tech as digging through your trash. It can be an unknown store clerk or someone you know and trust. They possess the same motive, which is to use your name and good credit to purchase goods and services without paying the price. However, there is a price to pay - for the victim. It can take hours, weeks and even years to undo the damage caused to your credit and good name.

How can I prevent becoming an Identity theft victim?
While no one can totally prevent this crime from occurring to you, here are some positive steps to take which will decrease your risk:

1. Check your credit reports once a year from all three of the credit reporting agencies listed below. This is one of the best ways to find out if someone is using your information without permission. There may be a small charge for these reports unless you are a victim of financial crime or you are denied credit in the last 60 days.
2. Guard your Social Security Number. When possible, don't carry your social security card with you. That also includes any cards or badges that may include this number on it. Resist giving it out unless absolutely necessary. Question why a business has requested personal information if you think it is not appropriate. Ask how they protect you from lD theft.
3. Guard your personal information. Get credit cards with your picture on them. Be alert to shoulder surfers listening for information. Keep confidential information in a locked area in your home. Don't print your SS# or driver's license number on your checks.
4. Cancel credit cards you no longer use and carry as few as possible in your wallet. Add passwords to all your credit card and bank accounts. Use a random word rather than your mother's maiden name.
5. Don't store account numbers or passwords on your computer without firewall software protection.
6. Carefully destroy papers you throw out, especially those with sensitive or identifying information. A crosscut paper shredder works best. You can cut back on the number of pre-approved credit offers you get by calling 888-5OPTOUT.
7. Be wary of possible telephone and e-mail internet scams. Never provide information unless you have initiated the contact. lf you suspect a scam, call 877-FTC-HELP to check it out.
8. Keep an eye on your credit card when you give it to a store clerk or waiter. Carefully read your monthly statements and immediately report any unauthorized charges.

How do most victims find out about the crime?

Typically they find out when applying for a loan, a new credit card, when they receive a call from a collection agency or when a pre-employment criminal background check reveals a past record. An annual review of your credit bureau reports will minimize these impacts.

What should I do lf I become an identity theft victim?

1. Contact the governmental agencies and credit grantors involved-credit card companies, banks, utility companies, card merchants. California law requires that they provide victims with copies of the application form transaction information on fraudulent accounts upon request. (PC 530.8)

2 If telephone service with SBC California has been established in your name, contact SBC California at 1-877-2024558 (English) or at 1-888-615-0743 (Spanish).

3 Contact each of the three credit bureaus listed below and request a copy of your credit report. You should also place a fraud alert with each of these companies requesting that no one can be allowed to open an account without your express permission.

4 Contact the police where you live. In California, they must take a report and give you a copy of it. (PC 530.6) Make several copies of that report you'll need it to clear up your records.

5 Call the Federal Trade Commission at 1-877-IDTHEFT and record the crime. They are collecting statistics about ID theft crime and one of their databases are linked to law enforcement.

Credit reporting Agency contact information

TransUnIon: 1-800-888-4213 www.tuc.com To report fraud: 1-800-680-7289
Experian: 1-800 EXPERIAN www.experian.com To report fraud: 1-888-397-3742
Equifax: 1-800-685-1111 www.equifax.com To report fraud: 1-800-525-6285

Are you a curious cat?

Important Resources and Internet Links

www.sbc.com
To find out more about Identity Theft and prevention tips relating to other types of telephone fraud.
www.idtheftcenter.org
The Identity Theft Resource Center website includes numerous self-help guides, scam alerts, fraud declaration forms and request letters.
www.privacyrights.org
www.consumer.gov/idtheft
or 1-877-IDTHEFT
www.ifccfbi.gov
The FBI and its Internet Complaint Center
www.privacy.ca.gov
California Department of Consumer Affairs, Office of Privacy Protection -1 866-785-9662 operates a hotline for consumers and victims of fraud.
866-658-5758 California DMV fraud hotline
www.corp.ca.gov/comp/complist.htm
California Department of Corporations complaint form
www.usps.com/postalinspectors

"Dialing for Dollars" Protecting Older Americans from Fraud
www.ssa.gov
Social Security Administration
www.consumer.gov/idtheft/
Federal Trade Commission
www.usa.visa.com/personal/secure_with_visa/identity_theft.html
Visa credit card company
www.mastercard.com/us/gateway.html
Master card credit card company

SCAMS!

If it doesn't look right-it isn't!

There are numerous variations, but only a few basic scams. The links below can fill you in.

INFORMATIONAL LINKS

www.nclnet.org/pressroom/fakechecks.htm
Advocacy group with lots of information
www.cbsnews.com/stories/2004/09/23/60minutes/main645313.shtml
CBS news report on Lottery Scams which target the elderly
www.crimes-of-persuasion.com/index.htm
Common Schemes, Scams and frauds
www.crimes-of-persuasion.com/Crimes/Telemarketing/Outbound/Minor/assistance.htm
Fake Grandson Scam
www.crimes-of-persuasion.com/Crimes/Telemarketing/Outbound/Minor/assistance.htm
Internet Fraud Complaint Center
http://www.msnbc.msn.com/id/6083986/
MSNBC Inside the dark art of phone fraud
www.fraud.org/welcome.htm
National Fraud Information Center

A COMMON SCAM

The following is a typical example of a "Nigerian Scam" Letter. This scam originated in Nigeria and, like all scams, appeals to avarice and gullibility in the belief of getting something for nothing. Like all scams the victim ends up the loser. There is a dedicated website named after the Nigerian law it violates-419. The link follows the letter.

Beware the friendly Wolf!

Tel: +27.72.606.4064
E-mail : moroka2@post. com

23'd Sept.,2OO4

Dear Webster,

This letter may come to you as a surprise due to the fact that we have not yet met. I thought about it long and hard before contacting you, it will benefit us both if you pay particular attention to this letter.

I am Mr. Morrison K. Moroka, Head of lnternal Audit Department with The Standard Bank of South Africa Limited. I managed to get your contact details through some research. A British oil Merchant and Contractor, Mr. Richard W. Webster, one of our Private Banking clients died intestate and has no nominated next of kin to inherit the title of investments made through our bank. The essence of this communication with you is to seek your assistance in claiming the funds. Since you have the same surname with the deceased and well suited for this confidential transaction, we will deposit the-Us$ 8,720,000 (Eight Million Seven Hundred and Twenty Thousand US Dollars) in your account and I will share the total proceeds with you.

Since Richard Webster died without writing a WILL and all attempts to trace his next of kin or heir has been unsuccessful; we have sent a routine notification to his forwarding address and home town but got no reply. I just returned from England, the bank paid for my travel to Europe to investigate and nominate a next of kin if possible, to whom the funds will be paid. So far, all investigation and records show that he did

not declare a next of kin or relations in any official documents, including his Bank Deposit documents in my Bank. This sum of US$ 8.7 million is still sitting in my Bank and the interest is being rolled over with the principal sum at the end of each year. It is becoming apparent that no one will ever come forward to claim the funds. Under South African Law, at the expiration of four years if nobody applies to claim the funds, the money will relocate to the ownership of the South African Government.

Consequently, my proposal is that I will like you as a foreigner with the same surname to stand in as the next of kin for Mr. Richard Webster so that the fruits of his labour will not get into the hands of some corrupt government officials. The process is simple; I need you to make available your full details for a local solicitor to prepare the documentation that will establish you as a next of kin. Also, the solicitor will draw up letters to the probate registry in your favour for the transfer to be authorised. Then the money will be paid into an account nominated by you, to be shared in a ratio to be determined.

There is no risk at all. Our positions in the bank, both as Director and Manager guarantee the successful execution of this transaction. If you are interested, please reply via the private e-mail (Any time) or work Telephone number above (8:30AM - 6:00 PM). Once you indicate your interest to assist us, I will provide you with more details and relevant documents that will help you understand, and to prove the authenticity of this transaction. For now, observe utmost confidentiality until we make contact. Be rest assured that this safe and will be beneficial to us.

Sincerely,

Morrison K. Moroka

You gotta be kidding me? This stinks!

home.rica.net/alphae/419coal/
Nigeria. The 419 Coalition Website

How can I protect myself?

Not every smiling face is friendly!

1. Mail is a common source of information to thieves. Courtesy checks from credit card companies; your checks to pay bills; bank and credit card statements all contain the information needed to steal your identity or credit. Consider renting a Post Office box rather than an unprotected mail box. It's cheaper than being victimized!
2. ALWAYS shred personal information, bank statements, old checks, bills etc. when you are finished with them. NEVER just throw them in the

trash. REMEMBER those courtesy checks and applications from credit card companies? If you throw these away, even at the Post Office, someone will use them. Shred these also.

3. Scams are routine on the internet. If you receive them via e-mail, just delete without responding. Be prudent with the personal information you disclose on the internet, especially free E-mail accounts and subscriptions that require certain information.
4. Keep personal information locked up at home. Make a copy of the front and back of all credit cards and keep this locked up also. Don't leave personal information on an unsecured computer.
5. Don't leave unsecured valuables in your vehicle. EVERY thief knows that people often leave valuables under the front seat and in the glove compartment. The majority of stolen credit cards are taken from the glove box. A locking trunk is the only secure area of a vehicle, and then ONLY if there is no rear seat access into the trunk.
6. Question those businesses that don't check your ID when you present your credit card. If they don't check you, they won't check a thief!

Be a bear about protecting your name and credit!

I'm a small business owner. How can I protect my business?

1. CHECK ID, CHECK ID, CHECK ID!
2. Before accepting a check, recognize that it is extremely simple to create fraudulent / forged checks with computers. Obviously, don't accept third party checks. Try to be a business and not a bank, and consider the cost of cashing personal checks which later turn out to be fraudulent.
3. Have a written store policy for employees concerning checks. This should include the following: that the ID photo is checked against the customer; the information on the ID matches the check; the driver's license number be read and written down by the clerk. Consider thumb

printing the check. For prosecution purposes, no case can be made without the above.

4. Consider installing surveillance cameras. If you have surveillance cameras then change the tape regularly (or go digital). CLEAN the camera lens once in a while. Position the camera to record the face of the customer.
5. Consider the placement of window advertisements. If the view is obscured then Deputies cannot see in, and neither can the clerk see outside. Consider after hours lighting, both inside and out. Register the alarm and update the contact information (533-5855).
6. Train employees to detect counterfeit bills. Posters and training aids are available to you (694-2902 Det. Moses). This is a growing problem due to the quality of printers. Bills need to be checked for the following: Paper, color, strip, watermark and denomination. A pen marker is good to detect the paper, but a growing trend is to bleach the amount on a low denomination bill, and change it to a higher number (eg $5 to $100). Know your presidents!
   www.moneyfactory.com/newmoney

7. The best prevention policy, to avoid embezzlement, is to have a division of responsibilities. In most reported embezzlements the same person is responsible for accepting monies, paying bills, and accounting. Put in place checks and balances. Most reported embezzlements are not discovered for years. Remember, it's only your profit if you get to keep it!
8. Deposit your takings daily. Don't leave it in the store overnight / weekend.