Identity Theft and Computer/Mail Fraud Schemes

ID Theft occurs when someone uses personal information such as your name, Social Security number, credit card number or other identifying information without your permission to commit fraud or other crimes. Put simply, ID Theft is a form of fraud. Identity thieves may use a variety of low and high-tech methods to gain access to your personally identifying information.

Common ways Identity Theft occurs:

Defrauding businesses or institutions.

Stealing records from their employer

Bribing an employee who has access to the records

Conning information out of employees

Hacking into the organization's computers

Rummaging through your trash, the trash of businesses, or dumps in a practice known as "dumpster diving."

Using a method called “pretexting” (on the phone) or “phishing” (over the internet) wherein a caller pretends to be a business with which you may have had some financial contact, or they are "performing a survey." They ask for information no legitimate business would ask for: bank account and credit card numbers, about your credit report, investments, savings, Social Security numbers, birthdates, etc.

Obtaining credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer or someone else who may have a legitimate need for and a legal right to the information.

Stealing credit and debit card account numbers as your card is processed by using a special information storage device in a practice known as "skimming."

Stealing wallets and purses containing identification and credit and bank cards.

Stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.

Completing a “change of address” form to divert your mail to another location.

Stealing personal information from your home.

Internet/e-mail Scams

Most scams, by phone or email, ask you to provide either credit card account information or your Social Security number. NEVER give out this information unless you initiate the call and you know that you are speaking to a true company representative. The list of scams below represent only a few of the scams currently being used.

Generic Scams:
Do not respond to any of these scams, not even to remove your name from the list.

Special VISA/Mastercard Scam Alert:
Should you get a phone call from a VISA or Mastercard “employee” trying to confirm unusual spending activity AND that person asks for code on the back of your credit card--- DO NOT give that number out. They will sound very professional but may not be from that company. They may even tell you how the scam works- for instance telling you that charges are always under $500. Then they will ask you for the code on the back of your credit card. DO NOT give that number to the caller. They often say that the charge is for an Anti-Marketing Device. Contact VISA or Mastercard Fraud numbers on your credit card to confirm that they made that call and deal with the situation that way.

Account verification or "phisher" scams:
For several years, individuals have purchased domain names that are similar to those of legitimate companies. It may be in a form such as: abccompany-accounts.net. The real company is abccompany but it does not have a "-accounts" in its domain. These con artists then send out millions of emails asking consumers to verify account information and even SSN. Prior to agreeing to do this, check with the company directly and see if the email originally was sent from them.

Sign-in Rosters:
There are some companies and governmental agencies that ask you to put your name and SSN on a sign-in roster. Please be aware that identity thieves may sign up toward the end of a page (purposely) so that they can copy and collect personal
identifying information. If you encounter a sign-in roster like this, the best way to handle the situation is to write the following instead of your SSN - "will provide in person."

Help move money from my country," aka Nigerian 419 Scam:
Everyone has received an email from a representative of a foreign government asking you to help move money from one account to another. Nigerian Money Offers now account for about 12 percent of the scam offers people have said they've received, according to a recent National Consumers League poll. However complaints about these offers increased 900 percent from 2000 to 2001. The latest versions of this scam include a dying woman, a soldier and emails other than from Nigeria.

Canadian/Netherlands Lottery- "You Have Won":
Unless you entered a lottery or bought a ticket to win a prize, these are scams. They originate from the Netherlands and other foreign countries. This scam can cost you more than $20,000. Many include: From: "Promotions Manager" : CONGRATULATIONS! WERKEN BIJ DE LOTTO, 41132, NL-1007 DB AMSTERDAM, THE NETHERLANDS. NEW- Via US Mail there is a new scam about a "Spanish Lottery."

"Free Credit Report" Emails:
Many of the "free credit report" emails you receive are scams. Either the person is trying to find out your social security number or will be billing you for a service later on. Do your homework and check out the company via the Better Business Bureau, US Attorney and Federal Trade Commission.

"You have won a free gift":
You may receive either a phone call or email about a free gift or prize. You just need to send your credit card info to take care of shipping and handling. DON'T. Free means free, there should be no charge. Also, you must consider if this is a group sending out a cheap gift in exchange for finding a "live" phone number or email address. Responding may result in hundreds of spans or telemarketing calls.

Tsunami and Hurricane Victim Aid Scams:
Consumers are urged to make donations directly to official web sites rather than respond to unsolicited requests.
Recently, many law enforcement agencies and consumer advocacy organizations issued warnings that con artists were using "phishing" attacks to prey upon the outpouring of generosity for victims of the Indian Ocean tsunami and hurricanes in the southern United States. In these attacks, fraudulent e-mails disguised as e-mails from seemingly legitimate relief agencies are sent to unsuspecting consumers, attempting to trick them into going to a fraudulent Web site designed to steal credit card and other personal information.

Protection and Prevention

If you catch ID Theft early, it can be easier to stop. Many people do not know that they have become a victim for a year or more. A victim may not find out until the day he or she tries to buy a house and the bank denies the loan. (85% of victims find out about the crime due to such an adverse situation; only 15% learn through a positive action taken by a business group that verified a submitted credit application.) By monitoring your credit report and being cautious with your personal information, you are protecting yourself.

1. Shred all financial documents before throwing them out.
2. Purchase a locking mailbox or route mail to a post office box.
3. Distrust e-mail links — instead, type addresses directly into the address box.
4. Protect your computer with a firewall and anti-virus software.
5. Don’t disclose social security numbers or other confidential information.
6. Download software with caution — avoid downloads from questionable web sites.
7. Create unique passwords, commit them to memory.
8. Don’t open e-mail attachments from unknown sources.
9. Don’t put personal information such as your SSN on checks.
10. **Purchase identity theft protection.**