Identity Theft Prevention

Check Washing/Counterfeit Checks:
You pay your bills on time every month. This past month you even sent them in early. However, the banks are now sending you late notices and charging you fees. They claim to have never received the payment.

This scenario plays out in many households throughout the U.S. each month. A thief takes an unsuspecting consumers bills left for pick up in their mailbox. They will then either "wash" the check or use the information to counterfeit a check.

How these frauds work:
Check washing is a process in which Identity Thieves use a combination of household products to erase ("wash") the hand written ink from a check. The thief can then make the check payable to himself or herself or someone else. They can also change the amount of the check to be hundreds if not thousands more than it was written for originally.
Counterfeiting checks has been made easier in recent years because of the technology that has been developed. All the thief needs is a software program, blank check stock, and a printer. These items can be found in many stores. With this technology the thief then only needs the account information from a consumers check. The account information is entered into the software program and a counterfeit check is created. It's that simple. The thief can now write checks payable for any amount they choose. The counterfeit checks are used until they have drained the money out of your account or you have noticed the activity and closed the account. Some preventative actions you can take to guard against this type of fraud are to:

- Mail your checks at the Post Office.
- Contact your Financial Institution to see what security features you have on your current checks. Is there a more secure check that you can be using?
- Use a regular Ballpoint ink pen when writing checks. Some companies warn that it is easier to wash checks that are written with a felt tip pen.
- Never leave your mail in the mailbox overnight.
- Keep good records of what checks you have written. These records should include who the check was written to, the date, and amount.
- Review your bank statements each month for any inaccuracies.

Review Your Statements!
Although no one ever really wants to receive these bills it is very important that you review them carefully. Many consumers just pay the bill without reviewing the statement. However, there is always a chance that someone has gained access to your account and is using it to make unauthorized purchases.

When reviewing your statements you should look for purchases that you did not authorize. If you are unsure about an item you should contact the company immediately to check to see if maybe you actually did make the purchase. If you are positive that you did not authorize the transaction you should contact the company that your account is with and have the item disputed. You

should also inform the company that you want the account closed immediately. This will ensure that your account cannot be used in the future.

Throughout the year you should continue to review your statements carefully. You should also keep track of when you are supposed to receive them. If they do not arrive around the expected time contact the company immediately to make sure that it was sent to the correct address. If the address was changed without your authorization close the account immediately.

Protecting Your Social Security Number
One of the most important things you can do to protect yourself from Identity Theft is to protect your Social Security Number (SSN). Your Social Security Number is the key to your personal information. By obtaining your SSN a thief can get access to many things including your Bank accounts and Credit cards.
Below are some steps you can take to protect your Social Security Number:

- Do not carry your Social Security Card in your wallet or purse. Keep this card in a safe place at home.
- Do not imprint your SSN on your checks.
- Many Department of Motor Vehicle's no longer require that your Social Security Number be your Driver's License number. If this is the case in your state be sure to have your License number switched.
- When asked to provide your Social Security Number, ask the individual why it is needed and how they will be using the number.
- Do not post your number in emails or chat rooms.
- When applying for something online make sure that the site is secure.
- Read the Privacy Policy of any website that you provide personal information to. This policy will let you know how they use this information.

Opt Out Information
Are you sick of those unwanted Pre-approved Credit Offers? Or all the Spam you receive in your inbox? If so, you may want to consider placing your name on the Opt out lists. We have provided information below as to how you can opt out. Keep in mind this does not opt you out of all mailings. If you are receiving something from a particular company you should contact them directly and ask to be removed from their list.

To opt out of receiving pre-screened credit card offers, call:
1-888-5-OPTOUT (1-888-567-8688)

To remove your name from many national direct mail lists, write:

DMA Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735-9008
For more information, visit http://www.the-dma.org

To remove your name from many national telephone marketers, write:

DMA Telephone Preference Service:
P.O. Box 9014
Farmingdale, NY 11735-9014
For more information, visit http://www.the-dma.org

To remove your name from many national direct e-mail lists,
visit: http://www.e-mps.org

Shopping Precautions
There are some things you should know that go beyond locking your valuables in the trunk of your car while at a shopping mall. Your identity and credit rating is probably the most important thing you own and you should be vigilant in protecting it. It is remarkably easy to obtain control over your finances with just a few pieces of information about you.

The following are just a few actions that we recommend in order to protect your information:

- When traveling, bring your cell phone for those calls you need to make while sitting in airports, train stations, or while on the streets. If you do not have a cell phone and must use a credit or calling card at a public phone, purchase a prepaid calling card. Many crooks will watch you from a distance and steal your credit card number as you enter it on the keypad. They will then turn around and charge hundreds or thousands to your card before your bank or you realized what happened.
- While shopping, leave your checks at home-especially if they have your social security number on them. Use a credit or debit card instead as there is much less information about you on them. If lost or stolen, the information on your checks could be all a sophisticated crook needs to assume your identity. Credit cards have far less information on them and your liability for unauthorized use is limited by law to $50.
- Many people are inclined to donate to charity during the holidays. This is a great way to help those less fortunate, but be careful whom you give your money to. As a general rule, do not give out money or personal information to those that solicit directly to you by mail or phone. When telephoned always ask for the name of the organization, the name of the individual on the phone, and a call back number. If they are legitimate, they will readily give you this information. If you would like to donate to an organization, you should initiate the contact. You can get the phone numbers and addresses from your local phone book. Do not let a crook take advantage of your generosity!
- When getting money from an ATM be on the lookout for Shoulder Surfers. These are people who look over your shoulder when you enter your PIN number. To protect yourself, stand directly in front of the machine and cover the number pad with your hand when entering the PIN. Keep an eye out for anyone suspicious.
- Leave your Social Security Card at home!
- Whenever possible do not pay cash. There are thieves that lurk in malls and watch to see who has paid cash for an item. They will then follow that individual and steal the shopping bag with the receipt in it. The thief will then go back to the store where the merchandise was purchased and "return" it for the cash. This scam is especially popular during the Holiday Season.

Credit Cards or Debit Cards?
Should I use my Debit Card or Credit Card? Many consumers ask this question when standing in line to make a purchase. Which card provides more protection for consumers?

One drawback of using a Debit Card is since the money is taken directly from a linked account, such as a checking account, the damage can be more devastating. If someone steals your card and makes a fraudulent purchase, the financial institutions are not required to credit any disputed money to your account until an investigation has been completed. An investigation could take weeks. In the meantime, you may not have the money in your account to pay your mortgage, car bill, or any checks you had written. As you can imagine this can cause many problems. A fraudulent purchase with a Credit card, on the other hand, can be disputed and the payment may be able to be withheld.

If you make a purchase with a Debit card and later find that the item is defective it may be harder to get your money back from the company. If you had used a credit card you again have the right, under the Fair Credit Billing Act, to withhold payment until the problem is fixed.

Both the Credit card and Debit card provide protection for consumers. The Fair Credit Billing Act provides protection for the use of credit cards and the Electronic Funds Transfer Act provides protection for the use of Debit cards. You can find information about each of these acts at the Federal Trade Commission's website http://www.ftc.gov.

Dumpster Diving: Just Plain Trash or An Identity Thieves Treasure?
Unless you're a celebrity you would probably never imagine that someone would want to go through your trash. You are probably thinking, "There is nothing valuable in my trash". Well unless you take precautions there very well may be enough information in your trash to take over your identity.
Dumpster diving is a way identity thieves get the information to steal someone's identity. They rummage through garbage cans looking for anything that might contain personal information. Here are some examples of what a dumpster diver may be looking for and what they may be able to do with the information.

Pre-approved credit card offers - Millions of consumers receive those pre-approved credit card offers every month. Many just discard these applications without shredding them. If an identity theft comes across one while dumpster diving they could complete the application and attempt to have the card sent to them at another address.

Bank Statements - If a thief comes across a discarded bank statement they now have your account numbers. They may try to impersonate you and have your address changed at your bank or create bogus checks with your account number.

Checks - If you discard voided checks or copies of checks, the thief could easily create duplicate bogus checks. There are many programs out there that make this procedure simple.
These are just some of the things an identity thief looks for when rummaging through trash. The most important thing you can do to protect yourself is to shred all documents with personal information on them. If you do not have a shredder cut or tear the documents into little pieces.

How to pick a good password
Picking a memorable password is a tedious task in itself. Always use a password that is going to be easy to remember but would still be hard for someone that knows you very well wouldn't figure out.

- Some tips to use when choosing your password:
  Choose a password with at least 8 characters. Mix up the password with different characters such as letters and numbers.
- Be sure to change your password regularly and use different passwords for different services.
- If you a going to keep a written reminder of your password, keep it far away from your computer.
- Never use a password that is too easy for anyone to find out. Passwords that hackers first attempt are "blank", "password", and "administrator."
- Never use a password that would be easy for someone who knows you could figure out. Easy passwords to find are: birthdays, children's names, maiden name, favorite team, last name, place of birth, model of car, vacation spot, or a pet's name.
- Never share your password with anyone, even family members or people that you can trust. Encourage family members to get their own accounts.
- Never use your login as your password!

Protecting Your Identity During Summer Vacation
Many of us are preparing to take our summer vacation. Our vacations may include going to the beach, taking a cruise or taking the family to Disneyland. No matter where we end up this summer we should always take precautions to avoid becoming the victim of identity theft.

- The following are just a few precautions we recommend you take to protect yourself:
- Contact your local Post Office to request that your mail delivery be stopped during the time you will be on vacation. Or ask a trustworthy neighbor if they will pick up your mail daily.
- Carry only the checks and/or credit cards that you need. Travelers Checks are always a good idea since they can usually be replaced within 24 hours.
- Keep a list of what items you have in your wallet or purse. You should keep the list in a safe place where you are staying. Do not include account numbers on the list. Do include the name and phone numbers of the companies in case you need to contact them. This list will be very helpful in the event your wallet or purse is stolen.
- Put any documents that contain your personal information in a secure place in your home while you are away.
- Do not leave documents containing personal information lying around the hotel room. Ask the front desk if they have a secure vault or location and what type of security they have.
- Do not keep your Personal Identification Number (PIN) with your ATM card. This just makes it easier for the criminal to use your ATM card if it is stolen.
- As always, never carry your Social Security Number with you.

Back To School Protection
Attending college is a right of passage for many high school graduates. For the first time in their lives they are going to be living life on their own terms. No sooner than their parents drop them off at their dorms, do these young people get bombarded with offers for credit cards and other pay services. Credit card companies set up tables on college campuses across the country and offer bottles of soda, novelty pens, and t-shirts just for filling out an application. Inevitably, thousands of students sign up every year and are granted large credit lines despite having no proof of income.

All you really need to obtain a credit card is a name and a matching Social Security number! It is that easy. So as you can imagine, there is a great deal of importance for students to protect all of their documents with identifying information. We recommend the following tips for students to better safeguard their vital information:

- Always keep your credit cards, checkbook, bank statements, Driver's License, and especially your Student ID under lock and key. Most colleges use your Social Security number as your student ID number and many people will have access to it, such as your teachers and all of their staff. You should request another identifying number from your institution instead of using your Social Security number.
- If you leave your dorm room or apartment for any length of time, LOCK your door. It only takes someone a few seconds to steal something out of your residence. This kind of thing is very common.
- Get a private mailbox. Many colleges distribute mail by room or apartment rather than by name. Everyone living with you has access to your statements and letters. Your campus post office should be able to sell you a private box for a nominal fee.
- Never leave your purse, wallet, or backpack unattended in a public area such as the library or cafeteria. If it is not nailed down, it will probably disappear quickly.

Keeping Hackers off your PC
All of us are concerned about Hackers. Businesses, government agencies, and individual users all have reasons to be concerned. Hackers have stolen employee's personal information as well as customer information from numerous companies and agencies. Individual users have also been targeted in an attempt to obtain their personal information.

The following precautions should be taken to stop someone from hacking into your personal computer:

- The most important thing you can do to keep your information secure is to install firewall software so that you can restrict incoming traffic. Keep information such as your passwords and user ID's to yourself. Never give them out under any circumstances.
- Your software, both browsing (i.e. AOL, Netscape) and Operating Systems (i.e. Windows 2000, Windows XP, etc.), should always be kept up-to-date so that hackers cannot enter into known "back doors". Be certain to download security patches as they become available. This will ensure that your security is up-to-date.

- When submitting information for an e-commerce transaction such as account number, or credit card number, make sure that the Internet connection is secure. When a connection is secure, a small padlock usually appears in the lower right hand corner of the screen.
- Do not use passwords like your nickname, pet's name, or mother's maiden name. These are easy for a hacker to figure out.

There is no foolproof way of keeping Hackers off your PC but taking these precautions will help to protect your vital information.