What you should know about ***IDENTITY THEFT***

Monitor your credit report. It contains your SSN, present and past employers, a listing of all account numbers, including those that have been closed, and your overall credit score. After applying for a loan, credit card, rental or anything else that requires a credit report, request that your SSN on the application be truncated or completely obliterated and your original credit report be shredded in front of you or returned to you once a decision has been made. A lender or rental manager needs to obtain only your name and credit score to justify a decision.

Order a copy of your free annual report. You are entitled to receive one free credit report every 12 months from each of the three credit reporting agencies. You can choose to order all three at the same time, or space them out over the 12 month period. Order your free report by phone, 877-322-8228 or online, www.annualcreditreport.com. You can order them by mail, send your request to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Put a Security Freeze on your credit reports. All third parties, such as credit lenders or other companies will not be able to access your credit report without your consent. Be aware this may interfere with the timely approval of any subsequent request or application you make that involves access to your credit report. This may include new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, etc. While your credit reports are frozen, companies that provide consumer data to the credit bureaus will not be allowed to update name and address information on your credit report. If your name or address needs to be changed, you must contact the credit bureaus directly with this updated information.

Truncate your social security number on your credit reports. This eliminates your entire social security number from being shown on your credit reports. Only the last four digits appear on your reports to minimize fraudulent activity.

To report fraudulent activity, contact Equifax 800-525-6285, Experian 888-397-3742 and TransUnion 800-680-7289, so these agencies can place an "Alert" on your credit reports. Also, contact the police and file a report, as well as the creditor with any incorrect information.

Credit Reporting Agencies:	www.Equifax.com	www.Experian.com	www.TransUnion.com
	(800) 685-1111	(888) 397-3742	(800) 888-4213
	P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022

Add your name to the name deletion lists of the Direct Marketing Association's Mail Preference Service and Telephone Preference Service used by banks and other marketers. You may contact the DMA at the following web address: http://www.dmaconsumers.org/consumerassistance.html or send them your request by mail:

Direct Marketing Association	Direct Marketing Association
Mail Preference Service	Telephone Preference Service
P.O. Box 9008	P.O. Box 9014
Farmingdale, N.Y. 11735-9008	Farmingdale, N.Y. 11735-9014

Presented by: Debt Management Credit Counseling Corp.
3310 North Federal Highway, Lighthouse Point, FL 33064
Office: 866-619-3328 www.dmcccorp.org
For a FREE Budget Analysis call 866-618-DEBT

To stop receiving someone else's mail, contact the company who sent you the mail and tell them that the person is not at your address. You can review the United States Postal Services' policy on refusing mail that is sent your address by visiting http://pe.usps.gov/text/dmm300/508.htm#wp1045146.

Remove your name from the marketing lists of the three credit reporting bureaus by calling the following toll-free number 1-888-567-8688. Ask to be removed from mailing lists for unsolicited credit cards or so called pre-approved loan offers. Learn more on how to stop solicitation telephone calls by visiting the Federal Trade Commission's website at www.fcc.gov/cgb/consumerfacts/tcpa.html.

Add your name to the National Do Not Call List. Make it easier and more efficient for you to stop telemarketing calls you do not want. Call, 888-382-1222 from the number you wish to register. It is free to register. For additional information, visit www.donotcall.gov.

Guard your social security number. It is the key to your credit report and banking accounts and it is the prime target of criminals.

Order your Social Security earnings and Benefits Statement once a year to check for fraud. Read the section "What to do if you are a victim" of this handout for additional information.

Cancel any credit cards you do not need or use. If you are thinking about purchasing a car or a home, consider waiting until after the purchase. Lenders look at the amount of debt you have versus the amount of credit available to you. Once you decide to close your credit card, be sure to tell the lender to note the card as "cancelled at the cardholder's request."

Actually look at your credit card and bank account statements, instead of just glancing over them quickly or passing them along to your spouse to pay off. This is usually the first place unauthorized activity will show up.

Call your credit card company or bank if an account statement is late. A missing bill may mean someone called the company using your name, and changed the billing address to prevent you from catching their shopping spree.

Do not give out personal information on the phone, through the mail, or online unless you initiate the contact or know the caller. Thieves will pose as bank representatives, Internet service providers and government agents, to get you to reveal personal information. They can also use caller ID spoofing to convince you that they are legitimate callers. Caller ID spoofing is when a caller can pretend to be someone else by falsifying the number or name that appears on the recipient's caller ID display. It enables telephone callers to insert any name or phone number that he or she wishes to show up on the caller ID display of the person being called. In some cases, it even allows the caller to change his or her voice (from male to female or vise versa). Be extremely cautious when someone calls you and starts asking for personal information.

Shred all bank, credit card statements, including "junk mail" credit card offers, insurance forms and physician statements before discarding these into the garbage. Use a crosscut shredder. Crosscut shredders cost more than regular shredders but are superior.

Do not carry extra credit cards or other important identity documents except when needed.

Place the contents of your wallet on a photocopy machine. Copy both sides of your license and credit cards so you have all the account numbers, expiration dates and phone numbers if your wallet or purse is stolen.

Do not mail bill payments and checks from home. They can be stolen from your mailbox and washed clean in chemicals. Deposit these items into post office boxes. A shocking number of thieves troll mailboxes for your personal information. If you are going on vacation, place a hold on your mail at the post office.

Identity Theft and the Deceased

Steps to take when a loved one passes away to decrease identity theft risk:

1. Obtain at least 12 copies of the official death certificate when it becomes available (some business will request an original).
2. Immediately notify credit card companies, banks, stock brokers, loan/lien holders, and mortgage companies of the death.
3. Immediately contact the credit reporting agencies and request a "deceased" alert be placed on the reports.
4. Contact the three credit reporting agencies.
5. Also notify: Social Security Administration, any memberships (video rental, public library, fitness clubs, etc.), insurance companies, Veteran's Administration (if the person was a former member of the military), Immigration Services (if the person was not a U.S. citizen), Department of Motor Vehicles (if the person had a driver's license or state ID card) and agencies that may be involved due to professional licenses (bar association, medical licenses, cosmetician, etc.).

Identity Theft and Phishing

Phishing is a term used to describe a type of identity theft by which scammers use fake Web sites and e-mails to fish for personal information from consumers. Typically, this scam involves receiving an e-mail supposedly from a company or financial institution you may do business with or from a government agency. The context of the e-mail may request to "verify" information or "resubmit" confidential information. If you comply, the thieves hiding behind the seemingly legitimate Web site or e-mail can use the information to make unauthorized withdrawals from your bank account, pay for online purchases or even sell your personal information to other thieves. To prevent this from happening to you:

1. Never provide your personal information in response to an unsolicited call, fax, letter, e-mail or Internet advertisement.
2. If you decide to initiate a transaction with a bank or other entity on the Web, take some simple precautions. Type in the URL (Web address) from scratch and be careful, type it in correctly. Do not respond to the email or advertisement by clicking on the promotion or link offered. If it is a business that you are familiar with, contact this business by using a phone number on a receipt, statement or other literature from the institution itself.
3. Quickly report anything suspicious to the proper authorities. Contact your bank and let them know you received an e-mail that appears to be from them but it is not.

If you are certain the e-mail or Web site is fraudulent, contact the Internet Crime Complaint Center, www.ifccfbi.gov, a partnership between the FBI and the National White Collar Crime Center.

Presented by: Debt Management Credit Counseling Corp.
3310 North Federal Highway, Lighthouse Point, FL 33064
Office: 866-619-3328 www.dmcccorp.org
For a FREE Budget Analysis call 866-618-DEBT

What to do if you are a victim

If you are a victim of identity theft, follow these step-by-step instructions to protect and repair your credit:

1. **Contact the three major credit bureaus.** You will need to place a "fraud alert" on your credit reports. Once you notify one credit bureau, that bureau will contact the other two bureaus and all three of the reports will be alerted. Make sure this happens. A fraud alert not only tells creditors that the information on your credit report may not be accurate, but also, that your permission needs to be granted before any more credit is attainable in your name. A number will be issued to each of your reports. Make sure to notate this number as it will be useful when you begin communication with creditors.
2. **Contact the creditors.** Once a fraud alert is placed on your reports, each of the bureaus will send you a free copy of your credit file. The last pages of your credit reports contain the contact information of all your creditors. Contact those creditors that have reported inaccurate information. All of your complaints should be done in writing and you will need to keep copies of these for future reference. Request your creditors provide you with documentation showing fraudulent activity. Present this data to law-enforcement officials.
3. **Contact the FTC**. The Federal Trade Commission is constantly working on developing identity theft patterns to help minimize fraudulent activity. Visit their website, www.ftc.gov or call 877-438-4338 and complete the complaint form in order to have additional records to present to law-enforcement and your creditors.
4. **Contact the police.** Once you have the complete list of accounts that were fraudulently created, present these to your local police station. Speak to an investigator and keep his/her name and phone number readily accessible. Make sure they make an official report of this crime. Request a copy of the police report and provide the creditors and credit bureaus with their own copy.
5. **Change your passwords.** The most common passwords are your mother's maiden name and the last four digits of your Social Security number. If the identity thief has managed to get a hold of these, you will need to change them quickly. Think of where a password is requested, an email account, online banking, utility accounts, insurance companies and any other business that may require verification when speaking to them. Contact these businesses and request to change the way they confirm your identity when they are contacted regarding your account(s).
6. **Order your Social Security statement.** This information will disclose your up-to-date earnings. This statement will provide contact information incase you notice your earnings do not match your records. To receive a copy of your Social Security statement visit www.ssa.gov. Your request can be made online by following the steps on this website, or you may download a request form and follow the instructions to receive your statement via mail. To use their telephone services, contact 1-800-772-1213.
7. **Change your driver's license number.** This may be useful if someone has stolen your wallet or if you have misplaced your license. The Department of Motor vehicles can assist you with this process.

Finally, be organized; document all of the phone calls you have made to your creditors. Write down the name and extension of the person you talked to while making detailed notes with the results of your conversation. Place all of these documents and correspondence in a secured file, you will need to access them in the future.

Other reports you should monitor:

- Medical Information Bureau (MIB), is an organization set up by insurance companies so they can share information about you. You are entitled to one free report annually. Call 1-866-692-6901 and provide the necessary information to obtain your file, if one exists. You can also visit www.mib.com for additional information. Or write to them at MIB, Inc., P.O. Box 105, Essex Station, Boston, MA 02112.
- You can also obtain a copy of your driving record. You can do this by contacting your state's Motor Vehicle Department.

Presented by: Debt Management Credit Counseling Corp.
3310 North Federal Highway, Lighthouse Point, FL 33064
Office: 866-619-3328 www.dmcccorp.org
For a FREE Budget Analysis call 866-618-DEBT