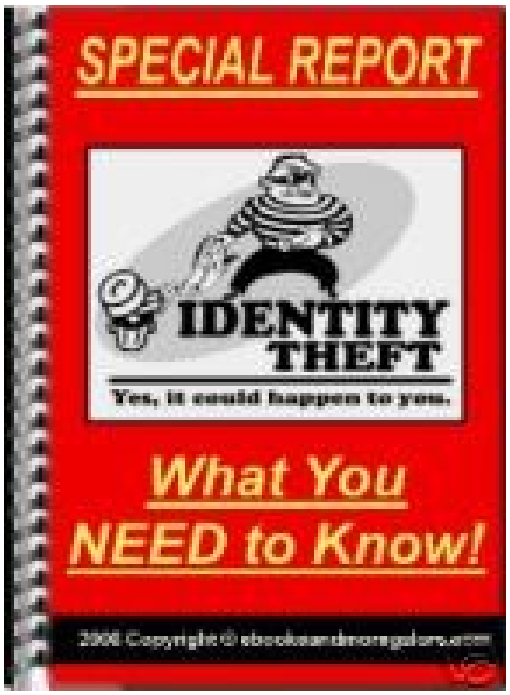

Visit **Ebooks and More Galore** for great deals on eBooks covering a variety of subjects

See My Current Ebay Auctions

SUPERCHARGE Your eBay Sales

IMPORTANT Identity Theft Prevention and Recovery Tips

Special Note: It is recommended that you print this Report for quick reference and keep it visible as a reminder to protect yourself and your family from identity theft.

PREVENTION TIPS:

1. **Never sign the back of your credit cards**. Simply write, “SEE IDENTIFICATION” or "PHOTO ID REQUIRED" (best to use something like a Sharpie Permanent Marker). Sure, it means you have to show your ID every time you use the card, but it is for your protection. If your card has a pin number, DO NOT write the pin number down. Get your picture on your credit card, if this is an option. Keep track of your credit card statements and bank statements as soon as they come. Keeping track of them online is even better.

2. If you have requested a **new credit card, ask when you will be receiving it**. If it hasn’t arrived by the expected time, call the credit card company immediately. Also, keep track of your credit card expiration date. If a new card has not arrived before the expiration date, call the credit card company right away.

3. If you pay your credit card accounts using a check, **DO NOT put the complete account number on the "Memo" line**. You only need to put the last four numbers. The credit card company knows the rest of the number. This way, anyone who might be handling your check, as it passes through all the processing channels, will not have access to your account number. Also, if you mail your check, make sure it is not readable through the envelope. You may want to fold it in half or cover it with a blank sheet of paper.

4. **Never put your complete name on your checks**. Use your first initial (and middle initial, if you want) with your last name. **Do not put your home number on your checks**. It is better to put your work phone number on your checks. If you work from home, then consider signing up for a private phone number (disposable phone number) at http://www.privatephone.com. This service does not cost anything at the time of this writing. Then you can use this private phone number on your checks. **Do not put your home address on your checks**. If you have a PO Box, use that rather than your home address. If you do not have a PO Box, use your work address. **Never have your Social Security number or Driver’s License number printed on your checks**. You can write them in, if necessary, and even then, they shouldn’t need your Social Security Number.

5. **Do NOT carry your Social Security Card in your wallet.** Do not carry any ID with you that has your Social Security Number on it. If a thief gets your name and date of birth, but does not have your Social Security Number, they will be limited as to what they can do.

6. **Get a secure, locking mailbox,** if possible. If not, consider getting a Post Office Box and have all your mail sent there. Deposit all of your out-going mail directly at the Post Office. DO NOT leave it in your mailbox at home for anyone that wants it to pick it up.

7. **Buy a shredder** and shred all documents/papers that contain your personal information. This would include, but not limited to, old credit cards, store receipts, pre-approved credit card offers, deposit slips, even the address portion on junk mail you receive. A shredder is worth every penny you pay for it for the protection it provides. A cross-cut one will provide more security than a straight cut one. It is also important to protect the documents and files on your computer. This is usually done with encryption. Now you can take it a step further and make your very important data invisible. You may even want to destroy your computer files and folders beyond recovery to protect your identity. The solution below offers an integrated Shredder for this added level of protection when needed.

8. Unless you know to whom you are speaking or dealing with, **Do NOT give out your personal information over the phone and/or internet.** This is especially if you did not initiate the telephone call or contact. Definitely **DO NOT** give your credit card number or Social Security Number to someone over the telephone or on the internet because you supposedly won an award or prize.

9. **Do NOT be scammed by "phishing" email.** This is when identity thieves try to lure you to their bogus websites made to look like those of a reputable company, such as eBay or PayPal. They can be very clever and seem very legitimate, but are usually easy to spot, if you know what to look for in these emails. Usually they contain several spelling mistakes and have capital letters where they don't normally belong. They often make threats and ask you to click on their link to enter your personal information. These are all signs that they are "phishing" for your private information. JUST DELETE THE MESSAGE. If you are not sure, many times you can forward the message (with full headers) to spoof@ebay.com or spoof@paypal.com or etc, and they will confirm if the email is for real or not.

10. **Check your credit report annually.** It won't cost you anything and will help you to spot any unusual activity. You can do this at http://annualcreditreport.com. A good recommendation is to request a credit report once every four months, each time requesting it

from a different one of the three national credit reporting companies. This way you can keep track of any unusual activity throughout the year and it will not cost you anything to do this.

11. **Protect your Medical Identity.** **If you don't, it could cost you your life.** If someone has stolen your medical identity and their information is now in your chart, just imagine what the result could be? Here are some important steps to take. A lot of people do not realize it, but your medical insurance card should be treated like a credit card. If it is lost, report it right away to your insurance company. Do not let it out of your sight or show it to anyone, except a trusted healthcare provider. Call your healthcare insurance company, at least yearly, and ask for them to send you a list of claims paid in your behalf. This way you can discern if there have been any fraudulent charges. Make sure they have all of your correct contact information as well. Under the new HIPAA law, you can now request an accounting of disclosures, or a history of disclosures, from every healthcare provider you have seen. You should request this also at least annually. This way you will know what personal information was released, to whom it went and why. If you have any unexplainable medical bills showing up on your credit report, start checking for medical identity theft. It is good to be familiar with the explanation of benefits received from your insurance provider. Take the time to call about any claims for services or medications that you do not understand. If you have had treatment recently and have not received an explanation of benefits from your health care company, perhaps a thief has already had your mailing address changed. Check on it. Finally, be cautious about offers for free medical care. Anyone that is trying to entice you to use their service may be just looking to get their hands on your private medical information.

12. Here are some **helpful websites** to visit (especially the first one listed):

- http://ftc.gov/idtheft (includes a 10 minute video worth watching)
- http://www.usdoj.gov/criminal/fraud/idtheft.html
- http://www.fdic.gov/consumers
- http://www.popcenter.org/problems/problem-identity_theft.htm
- www.usps.com/postalinspectors/idthft_ncpw.htm
- http://worldprivacyforum.org/

JUST IN CASE TIP:

13. **Make a photocopy (of both sides) of all the contents of your wallet**. This way you will have a record of what you had in your wallet and all of the account numbers and phone numbers to call and cancel these accounts, if needed. Keep this record in a safe place so you can find it when you need it. You may also want to keep all the toll-free numbers for your credit card companies and your health insurance company in your cell phone's contact list for quick reference.

RECOVERY TIPS:

Here is what to do if your wallet, purse or personal information has been lost or stolen.

(In general, be sure to keep track of the names, businesses, organizations, and phone numbers of people with whom you talk to about your case. Also, keep track of all reports and supporting documents, as this will be a big help in resolving your issue.)

14. **FIRST** - **VERY IMPORTANT – DO THIS FIRST** - Call the 3 national credit reporting organizations **IMMEDIATELY** to **place a fraud alert on your name and** also call the **Social Security Number** fraud line number. The alert means any company that checks your credit knows your information was stolen, and they have to contact you by phone to authorize new credit. This will usually stop the thief/thieves dead in their tracks. ***If you don't do this, then, even though you cancel all your credit card accounts, a thief can call and have them reopened and even open new credit card accounts with your information.***

Following are the numbers you will need to contact to report a fraud alert:

1.) Equifax: 1-800-525-6285 or 1-888-766-0008

2.) Experian: 1-888-397-3742

3.) Trans Union: 1-800-680-7289

4.) Social Security Administration (Fraud Line): 1-800-269-0271

15. **SECOND – IMPORTANT RECOVERY TIP** – Call and **cancel all your credit card accounts and close bank account(s),** if affected. Then, follow up this request in writing with each company/institution (supply any documentation such as police report, FTC forms, etc.)

16. **THIRD – IMPORTANT RECOVERY TIP** – **File a police report IMMEDIATELY** in the jurisdiction where the theft took place. This proves to credit providers and banking institutions that you are serious and diligently taking action. Also, this is the first step towards an investigation, if required.

17. **FOURTH – VERY IMPORTANT RECOVERY TIP** - **Contact Federal Trade Commission** online at http://ftc.gov/idtheft or call them toll-free 1-877-ID-THEFT (which is 1-877-438-4338) or 1-877-987-3728 or TDD at 1-202-326-2502 or by mail at: Consumer Response Center, FTC, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

18. **FIFTH – IMPORTANT RECOVERY TIP** – If the Identity Theft involved the U.S. Mail, report it to the nearest U.S. Postal Inspection Service Office, which you can locate here: http://www.usps.com/ncsc/locators/find-is.html.

19. **SIXTH – IMPORTANT RECOVERY TIP** – If you suspect Identity Theft in connection with tax violations, you should contact the IRS online at http://www.irs.treas.gov or call them toll-free at 1-800-829-0433

20. **Bonus Tip:** Beware of the Evil Twin Scam. Have you ever used your wireless laptop computer or PDA at a coffee shop, airport, hotel lobby, etc.? Be careful about entering any of your personal information, even passwords, while connected to one of these networks. Why? While you think you are connecting to the hot spot provided by the facility you are visiting, you may really be connecting to the network of the person next to you and not even realize it. Then this evil thief can watch and record your keystrokes as you enter personal and/or company information. He/She can even access your e-mails, attachments and instant messages. One way to protect yourself is to temporarily disable your wireless card's ad-hoc or peer-to-peer mode. Do this by going to your Control Panel and clicking on Network Connections. Under your adapter's utilities find where you can click to disable this feature. Find out more information about this danger and how to protect yourself at http://www.pcmag.com/article2/0,4149,1277504,00.asp.

21. **Second Bonus Tip:** Did you know that the 3 major credit reporting agencies can sell your personal information to companies that sell insurance, home mortgages or other credit offers? How can that be you ask? It is because of a loophole in the law that allows them make a lot of money selling your personal information to all of the lenders. But don't despair! You can STOP THIS FROM HAPPENING by going to http://optoutprescreen.com and follow the instructions to put an end to the credit agencies from giving out your personal information. Yet another way to PROTECT YOUR IDENTITY!

Note: It is recommended that you store all the above referenced toll-free numbers, credit card company numbers and web addresses in your cell phone for quick reference.

Disclaimer: I am no expert, nor do I claim to be one. This report is not to be considered legal advice. It is simply a guideline intended to help prevent and/or deal with identity theft. The information provided is accurate to the best of my knowledge. However, it may become obsolete, out-dated or change without any control on my part. If you have any questions or suggestions to improve this report you may contact me at admin@ebooksandmoregalore.com.

Visit **Ebooks and More Galore** for great deals on eBooks covering a variety of subjects

See My Current Ebay Auctions

SUPERCHARGE Your eBay Sales