NEW YORK STATE SENATOR
George D. Maziarz

Identity Theft - Don''t Be A Victim!

GEORGE D. MAZIARZ

The same technology that makes our lives easier and provides information at the click of a mouse, has also made it easier for thieves and scam artists. America's fastest growing white-collar crime is identity theft. The U.S. Justice Department estimates that more than a half million Americans will be victimized by identity theft this year alone, resulting in over $4 billion in losses.

How Does It Work?
Identity thieves obtain some piece of personal information, such as a social security number, credit card number or bank account number. They then use that to steal from you. The following examples are ways that identity thieves operate:

* They open a new credit card account, using your name, date of birth, and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.

* They call your credit card issuer and, pretending to be you, change the mailing address on your credit card account. Then, your impostor runs up charges on your account. Because your bills are being sent to the new address, you may not immediately realize there's a problem.

* They establish cellular phone service in your name and you are left with bills for calls all over the world.

* They open a bank account in your name and write bad checks on that account.

Be On the Lookout for E-Scams

The latest tactics being used by identity thieves involve Internet Service Providers (ISP), such as AOL and Yahoo. Scammers masquerading as your ISP send you an e-mail stating that your account information needs to be updated or that the credit card you signed up with is invalid or expired. They ask that you e-mail back to them your social security number, credit card number, expiration date, password and other sensitive information.

If you receive an e-mail like this, it is most likely a scam. Contact your Internet Service Provider via a separate e-mail or by telephone (do not reply directly to original e-mail) and ask if they are indeed requiring this information.

More importantly, remember you should never provide private information, such as your social security number, your credit card numbers, PIN numbers or passwords to anyone who calls, mails or e-mails you without double checking the validity of the request.

Phony Tax Form Alert

Another scam that is currently circulating involves phony IRS forms. You may receive a letter from a "bank" along with a fake "IRS" form, stating that you need to complete and return the form or you will be subject to additional taxes.

One of the phony forms is W-9095, "Application Form for Certificate Status/Ownership for Withholding Tax." It is similar to the real IRS Form W-9, Request for Identification Number

and Certification. The fake form asks for your name, address, Social Security Number and detailed financial information, including bank account numbers and investment accounts. The letter indicates that unless the form is faxed back within 7 days, 31 percent of your bank account's interest will be withheld for taxes.

Other phony forms that are circulating include W-8888 targeting foreigners with bank accounts in the United States with a similar scam.

Do not complete and return any form that is sent to you without first checking to ensure that it is on the "up and up."

What to Do If You Are Victimized:
If you suspect you are the victim of identity theft, call 877-ID-THEFT to get a copy of the Federal Trade Commission's Identity Theft notification form. You can also log on to www.consumer.gov/idtheft for helpful tips on how to avoid becoming a victim and printable forms to download.

#####