How to reduce your risk

➤ Do not carry your Social Security Card or give your Social Security Number to anyone just because they ask for it. Keep birth certificates, account statements or other similar information in a secure area. Make a list of ALL you credit card account numbers and bank account numbers along with the customer service phone numbers and keep in a safe place.

➤ Do NOT give personal information over the telephone, through the mail or the Internet unless you know 100% who is asking for the information.

➤ Shred credit card offers or other papers containing your name, address or other identifying information.

➤Protect computers by using firewalls, anti-spam/virus software, update security patches and change all passwords

➤ If you post your profile on social networking sites, keep the information you reveal as general as possible.

➤ Check your credit report annually and check your bank and credit cards statements often.

Steps for victims of identity theft

➤ File a report with the local police.

➤ File a complaint with the Federal Trade Commission at www.identitytheft.gov or call 877-438-4338

➤ Contact credit bureaus to place a 'fraud alert' on your credit records:

www.Equifax.com 1-800-525-6285

www.Experian.com 1-888-397-3742

www.TransUnion.com 1-800-680-7289

➤ Complete IRS Form 14039, Identity Theft Affidavit and mail or fax to IRS according to instructions or contact the Identity Protection Specialized Unit at 1-800-908-4490.

Know Your Rights

➤ Create an Identity theft report by combining your Police report with the FTC Identity Theft Affidavit.

➤ Place a 90 day initial fraud alert on your credit report

➤ Obtain free copies of you credit re-port.

Visit the Federal Trade Commission at www.consumer.ftc.gov o r www.identitytheft.gov

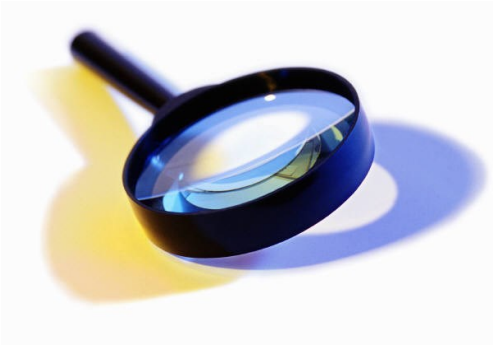
Daniel D. Gagnon CPA, P.C.
Certified Public Accountants

212 Fair Street
Kingston, NY 12401
Phone: 845-331-3600
Fax: 845-334-9465
www.gagnoncpa.com

Identity Theft

Tax related and non-tax related Tips and Information for all tax payers

Daniel D. Gagnon CPA, P.C.
Certified Public Accountants



Protecting your Identity

Identity theft is the fastest growing crime in America—Millions of Individuals have their identities stolen by criminals every year. Thieves use a victim's identifying information to commit financial fraud—filing income tax returns, applying for loans, establishing accounts, obtaining credit cards and even establishing account with utility companies. You should be aware of how identity thieves operate and exercise caution in your daily life.

What is identity theft:

Identity theft occurs when someone obtains your personal or financial information and uses it fraudulently without your permission. Identity theft may be:

Tax related—when someone learns your social security number and uses it to file a tax return.

Nontax related—when you have been identified as a victim in a data breach where your personal information has been compromised.

How to recognize possible identity theft

The best way to recognize tax-related identity theft is to read thoroughly any notices you receive from the Tax Department and the IRS.

You may be a victim if you receive a notice indicating:

➤you owe tax for a year you did not file a tax return;

➤more than one tax return was filed using your social security number;

➤you received wages from an employer you do not know or work for; or

➤your refund request was denied because the refund was already claimed.

You may get collection calls about accounts you never opened.

Your credit report contains accounts you did not open.

You are unexpectedly denied for a credit card or loan

Your credit card/utility bills suddenly stop coming in the mail or you receive bills for accounts you never opened.

How Does Identity Theft Occur

Identity thieves use virtually any method they can to trick you into revealing private information.

➤ Phone calls asking for information such as your Social Security number, your credit card number or the three-digit security code on the back of your credit card

➤ Standard mail such as pre-approved credit card offers containing your name and address

➤ Electronic mail with logos and names that appear realistic

➤ Fake Web sites that mimic real financial institutions' Web sites or social networking Web sites that contain identifying information about individuals

➤ Instant messages and text messages requiring you to call a toll-free number to "confirm," "verify," or "update" your information

➤ Impersonators - IRS, Bank or Retail customer service and even Police authorities—IRS will NOT call you with threats of jail or lawsuits, nor will they send you unsolicited emails suggesting to update your account information. Telephone impersonators are persistent—Don't fall for them! Report IRS-impersonation telephone calls at www.tigta.gov.

➤ Dumpster diving—sifting through your trash obtaining pieces of information from bills, financial statements and bank statements.