NEW YORK STATE SENATOR

Owen H. Johnson

Protect Yourself From Identity Theft: Obtain A Free Copy Of Your Credit Report

OWEN H. JOHNSON

GET YOUR FREE CREDIT REPORT!

Thanks to a change in the federal law,you will now be able to obtain a free copy of your credit report once every twelve months. The report will be issued by the three nationwide credit bureaus (Equifax, Experian, and TransUnion).

A credit report is an important record of an individual's finances, and is used by creditors, insurers, and other businesses when determining applications for things like credit, insurance, loans, and mortgages. It is so vitally important foryou to review this information to make sure there are no inaccuracies.

Reviewing your credit history is one of the best ways to protect yourself from identity theft, so please make sure you take advantage of this new opportunity.

HOW DO I ORDER MY FREE REPORT?

*By phone: call 1-877-322-8228

*By mail: please CLICK HERE to access the request form. Once you have completed filling out the form, mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta GA 30348-5281

*On the Web: order online by CLICKING HERE.

REVIEW YOUR CREDIT REPORT

By checking your credit report on a regular basis you can catch mistakes and fraud before they ruin your credit rating. One of the most common ways that consumers find out that they're victims of identity theft is when they try to make a major purchase (such as a car or house) and discover unfavorable contents and mistakes in their credit reports. Legitimate loans can be denied or delayed while the credit mess is straightened out. Knowing what's in your credit report allows you to fix problems before they jeopardize a major financial transaction.

FTC Consumer Alert:

How Not to Get Hooked by a 'Phishing' Scam

"We suspect an unauthorized transaction on your account.
To ensure that your account is not compromised,
please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information.
Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing" — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond. The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

• If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.

• Use anti-virus software and a firewall, and keep them up to date. Some phishing emails

contain software that can harm your computer or track your activities on the Internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

• Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

• Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

• Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that

can weaken your computer's security.

• Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

• If you believe you've been scammed, file your complaint at ftc.gov, and then visit the FTC's Identity Theft website at www.consumer.gov/idtheft. Victims of phishing can become victims of identity theft. While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk.

If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus.
The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Report suspicious activity to the FTC. Send the actual spam to uce@ftc.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.

Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

ADDITIONAL INFORMATION REGARDING IDENTITY THEFT -
The best way to prevent the theft of personal information is to be aware of how these crimes are committed. The followingthe identity theftlaws and gives tips on how to minimize your risk, as well as what steps to take if your identity is stolen.

MINIMIZE YOUR RISK OF ID THEFT

It's not just pick-pockets who steal your credit cards and money anymore. Advances in computer technology have made it possible for ID thieves to ruin your credit and tarnish your good name with a couple of clicks of a mouse. Below are tips to protect yourself and your family:

DOs and DON'TS

DO guard your computer password and use only secure lines to transmit financial information via the Internet. Look for an unbroken key or lock in the corner of your computer screen to signify a secure connection.

DO ask why a merchant needs private information, how it will be used and secured, and whether it will be shared with others. Ask if you can choose to have it kept confidential.

DO know the privacy policies of businesses with which you deal and websites that you visit.

DO register for NYS's "Do Not Call" Registry to reduce the possibility of telemarketing fraud.

DO talk about privacy concerns with your children. Everyone should understand the importance of protecting personal information.

DO ask about information security procedures in your workplace. Find out who has access to your personal information and verify that records are kept in a secure location. Ask about the disposal

procedures for those records as well.

DO guard your mail and trash from theft. Promptly remove mail from your mailbox and deposit outgoing mail in official post office boxes. Tear or shred documents that contain personal information before depositing in the trash.

DON'T give credit card, debit card or bank account information over the Internet or phone, unless you've initiated the contact and/or you are dealing with an established business that you know.

DON'T give your Social Security number (SSN) to anyone, except your employer, government agencies, lenders and credit bureaus. It's all a privacy pirate needs to steal your identity; also, don't carry your SSN card.

DON'T provide personal information to merchants or sales clerks that isn't required.

DON'T reply to "spam", which is unwanted email messages that clutter up your computer in-box and slow your connection to the Internet. That tells a spammer that your e-mail address is active. Instead, notify your Internet provider of the offender.

DON'T use obvious, easy-to-guess passwords on your credit card, bank and phone accounts. Avoid using your mother's maiden name, your birth date or the last four digits of your SSN.

LAW CRACKS DOWN ON IDENTITY THIEVES

FRIDAY, DECEMBER 9, 2005:INFORMATION SECURITY BREACH AND NOTIFICATION ACT NOW STATE LAW.

Identity thieves obtain a piece of personal information — your Social Security number, credit card number, date of birth, address — and use it to run up credit card balances, write bad checks, take out loans, and ultimately, ruin your credit rating. The Senate Majority is committed to prosecuting thieves, hackers and scam artists who violate our right to privacy and security. The ID Theft law, which became effective November 1, 2002, includes the following provisions:

* establishes three new crimes of identity theft, from misdemeanors to felonies, and increases the maximum sentence to seven years in prison;

* establishes new crimes directed at leaders of ID theft rings who collect and sell personal information to other potential criminals; and

* recognizing that many identity theft crimes are closely related to terrorism crimes, the law allows for certain offenses to be prosecuted as terrorism crimes.

The law also provides important protections for consumers, such as:

* court-ordered restitution to victims who have suffered out-of pocket losses, as well as losses incurred when their credit rating is damaged by an identity theft crime; and

* allows victims to sue in civil court to recover damages done to their credit ratings.

CREDIT BUREAUS

* Equifax To order your report, call: 1-800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241. To report fraud, call: 1-800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241.

* Experian To order your report, call 1-888-EXPERIAN (397-3742). To report fraud, call 1-888-EXPERIAN (397-3742).

* TransUnion To order your report, call 1-800-916-8800. To report fraud, call 1-800-680-7289.