



NEW YORK STATE SENATOR

William Larkin

Larkin Reminds Holiday Shoppers How To Further Protect Against Identity Theft

[WILLIAM J. LARKIN JR.](#) January 5, 2006

Senator Bill Larkin (R-C, Cornwall-on-Hudson) today reminded area residents to take as many precautions as possible to protect against identity theft during the busy holiday season.

"In the hustle and bustle of the holidays, it could be easy to become careless at times with spending, credit cards and record keeping," said Senator Larkin. "Identity thieves are just waiting to take advantage of unsuspecting shoppers who let their guard down. I strongly encourage area residents to be extra cautious right now and take the time to practice every measure of safety."

Below are tips to protect you and your family this holiday season:

DON'TS:

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." This is unwanted e-mail 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' maiden name, your birth date or the last four digits of your SSN.

DO:

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' " 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.

TIPS FOR SAFE ONLINE SHOPPING:

According to the U.S. Department of Commerce, online retail sales totaled \$36 billion last year. The Internet offers many benefits that are not available in a bank, store or mall. It is open 24 hours a day, seven days a week, and allows users to shop from the comfort of their homes. Below is some useful advice to help ensure that any transactions you make online are safe and secure.

WEB SITE SECURITY:

Use a secure web site and browser. Look for the "https" in the web site address or a closed lock or unbroken key icon on your status bar. Also, use the latest available version of the Internet browser to ensure that it complies with security standards such as Secure Sockets Layer (SSL). This technology scrambles your purchase and financial information.

Read the privacy policy of the web site.

This will help you to determine whether and how your personal information, such as your e-mail address and other identifying information, will be used or shared with others. Determine what security features are in place so that any personal information cannot be obtained and used fraudulently.

HOW TO PAY:

Credit cards offer additional protection in case of a dispute. Generally, you are liable for the first \$50 in charges, but some companies offer an online shopping guarantee that ensures you are not held liable for any unauthorized charges.

Electronic fund transfers

are transactions involving debit cards and other electronic banking transactions which result from direct withdrawal of cash from your bank account. Unlike with a credit card, this method of payment requires you to notify your bank of an error on your statement within 60 days. Also, if the card is stolen or lost, your liability can depend on when you report it. If you report within two business days of discovering the card lost or stolen, you will not be responsible for more than \$50 of unauthorized use.

C.O.D. – If paying by credit card or electronic fund transfers are not options, request that the merchandise be sent cash on delivery (C.O.D.). You can also make a payment with a personal check or money order. These methods are easier to trace than a cashier's check.

OTHER TIPS:

Always keep a record of your transactions online. Print a copy of your purchase order and confirmation from the web site. If the company sends you an e-mail confirmation, you should retain those until you have resolved any concerns regarding your purchase. Check shipping and handling fees, compare prices, and review warranties.

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. Consumers sometimes find out that they're victims of identity theft when they try to make a major purchase and discover unfavorable information in their credit reports. Legitimate loans can be denied or delayed while the credit mess is straightened out. Knowing what is in your credit report allows you to fix problems before they jeopardize a major financial transaction.

CREDIT BUREAUS:

Equifax (www.equifax.com) — 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.

Experian (www.experian.com) —

To order your report, call: 1-888-EXPERIAN (397-3742), or write: P.O. Box 2104, Allen, TX 75013.

To report fraud, call the same number.

TransUnion (www.transunion.com) —

To order your report, call: 1-800-916-8800, or write: P.O. Box 1000, Chester, PA 19022. To report fraud, call: 1-800-680-7289 and write:

Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834.

IF YOU BECOME A VICTIM OF ID THEFT:

If you become a victim, call 1-877-ID-THEFT to get a copy of the Federal Trade Commission's ID Theft Affidavit form. This affidavit will help you report information to many companies using just one standard form, simplifying the process.

It is also important to report the fraud to the following organizations:

1. Each of the three **national credit bureaus** (listed above). Ask each agency to place a "fraud alert" on your credit report, and send you a copy of your credit file.
2. The **fraud department** at each creditor, bank, or utility/service that provided the identity thief with unauthorized credit, goods or services.
3. Your **local police department**. Ask the officer to take a report and give you a copy of the report. Sending a copy of your police report to financial institutions can speed up the process of absolving you of wrongful debts or removing inaccurate information from your credit reports. If you can't get a copy, at least get the number of the report.

4. The **Federal Trade Commission**, which maintains the Identity Theft Data Clearinghouse and provides information to identity theft victims. You can visit www.consumer.gov/idtheft or call toll free 1-877-ID-THEFT.