



Consumer Credit Counseling Service
of Maryland and Delaware, Inc.

FOR IMMEDIATE RELEASE

December 20, 2011

Contact Information:

NANCY STARK
410.357.0614 (phone)
410.357.0613 (fax)
nstark@cccs-inc.org

Helping people help themselves through Education, Financial Counseling and Debt Repayment

PROTECT YOURSELF FROM IDENTITY THEFT THIS HOLIDAY SEASON

(BALTIMORE, MD) There are only a few more shopping days before Christmas. Afterwards, many of us will hit the mall or go online again to return gifts or take advantage of post-holiday sales. Identity thieves are drawn to these activities, because consumers are more vulnerable this time of year. "It really comes down to two factors," Steven Toporoff, who works as a staff attorney in the Division of Privacy and Identity Protection at the FTC, explains, "Around the holidays, we are inundated with offers and packages, with all kinds of information. We're also more rushed and distracted than usual. We need to recognize this fact and take precautions to protect ourselves from identity theft." Local nonprofit Consumer Credit Counseling Service of Maryland and Delaware (CCCS) offers these suggestions for a safe, secure holiday season:

For consumers who plan to shop at stores, identity theft precautions begin at home. "Take a look in your wallet," Toporoff suggests. "What types of identification are you carrying? Never take your Social Security card with you to the mall. Also narrow down the number of credit cards -- choose one or two -- and leave the rest at home. That way there will be fewer items to keep track of and they're less likely to get lost or stolen."

Once you're at the mall, be aware of your surroundings. Keep track of your purse, wallet, and other valuables. If you carry a purse, loop the strap over your shoulder and keep the clasp-side against the front of your body. Don't carry your wallet in your back pocket, where it's easily accessible to thieves.

"When you're standing in line waiting to pay for a purchase, keep track of what's going on around you," CCCS President and CEO Jim Godfrey recommends. "At the counter, be on your guard. Shield your credit or debit card from 'shoulder surfers' who may try to copy down your credit account or take a picture of it with their cell phone. Also pay attention to what the cashier does with your id. If you're asked to provide sensitive information during a purchase or in order to apply for a store card, write it down instead of sharing it verbally. You never know who may be listening."

Given the choice of using a credit or debit card, opt for the credit card. "Credit cards make it easier to dispute charges on items that don't work out," Godfrey concedes. "If someone steals your credit card, and you report it promptly, you're normally only responsible for the first \$50 of unauthorized charges, and many companies won't even charge that. If someone steals your debit card, they have direct access to the money in your bank account. Once you discover the fraud, you may have less protection under the law. The bank may not be required to cover your loss."

When you're out, only use ATMs with camera monitors such as those found in bank lobbies. Freestanding kiosk-style ATMS in less secure locations are more likely to be infected by skimmers (electronic devices that automatically record account and PIN numbers.) If you have to stand in line

to use an ATM, keep your debit card hidden, and be aware of anyone standing nearby. When you're at the machine, shield your transaction with your body to keep thieves from obtaining your PIN when you log in.

Once you're home, gather your sales receipts and put them in a safe place. When they're no longer needed for returns, shred and dispose of them. The holiday season is also a time when lots of packages arrive. Toporoff recommends keeping track of these. "When packages don't arrive on schedule, check to see what's going on. They may have been stolen for their contents or the information packing slips or bills of lading provide."

Consumers also need to be careful when shopping online at home. Toporoff cautions, "Only purchase from online vendors you know and trust. There are lots of sites out there that don't really sell a legitimate product. They're strictly interested in gathering your personal information. Never provide info, such as your bank or credit account number, to an online vendor you don't know. Also don't respond to unsolicited email or social media messages with links to offers or sales -- even if they look like they're from a company you know. These are often 'phishing' scams set up to steal your information. To find out if an offer is valid, log out and visit the company's website instead."

When it comes to purchasing items online, only use secure sites. Before you make a transaction, always check to see if the web address includes "https" or if the site has the traditional yellow padlock or key icon. Godfrey also cautions against making transactions using your laptop or Smartphone on a public WiFi network. "The free WiFi at the corner coffee shop probably isn't secure. This means that any personal information you provide can be easily stolen."

Before opening online accounts, choose difficult passwords that use a combination of letters, numbers, and other characters. Avoid using the same passwords over and over for several accounts. Keep a written password list in a secure place in case you forget, but don't share this information with family members, friends, or coworkers. Believe it or not, the identity thief is often someone that you know.

Despite all of these precautions, identity theft can still occur. Toporoff notes, "Given the increased risk from the holidays, it pays to start the New Year with a careful review. Check your bank statements and credit card statements for unexplained deductions or charges. Also request and review your credit report." Federal law allows consumers to receive one free credit report from each of the three major credit reporting companies (Equifax, Experian, and TransUnion) each year. Copies are available from each of these companies at: www.annualcreditreport.com.

Godfrey suggests that consumers stagger their free credit reports requests. "The information the credit reporting companies maintain is often the same. If you request one every so often, you can keep better track of where you stand throughout the year."

If you suspect that you may be a victim of post-holiday identity theft, take immediate action: Contact one of the three major credit reporting companies and request that it place a fraud alert on your credit report. The company you contact is required to contact the other two. Immediately close any accounts you believe have been compromised or fraudulently opened. Also visit the FTC website (www.ftc.gov) to file a complaint and fill out an affidavit. Take the affidavit to your local police department or the police where the identity theft took place and file a report. Godfrey says, "Finding out you've been the victim of identity theft is not an easy way to end the holidays. But the sooner you act, the better chance you have to minimize damage." To learn more about identity theft, please visit CCCS's website (www.cccs-inc.org) and take advantage of its free e-Learning course.

###

###

Consumer Credit Counseling Service of MD & DE, Inc. (CCCS) is an accredited 501(c)(3) nonprofit agency that has served the local community since 1966. CCCS creates hope and promotes economic self-sufficiency for individuals, families and communities through financial literacy education and counseling. To learn more about what we do, please visit www.cccs-inc.org. MD State License #14-01 / DE State License #07-01.