



ISSUE #34 – 4th Quarter 2010

Holiday Shopping: Avoid Becoming a Victim of Identity Theft

As the holiday season quickly approaches, so do the identity thieves who thrive on the vulnerabilities of holiday shoppers. Popular shopping days like Black Friday and Cyber Monday are breeding grounds for fraudsters. Taking into account the chaos of retail stores, and the anonymity of the internet, it is increasingly important to put our guards up and approach our holiday shopping with safety and vigilance.

CNBC recently reported that online shopping increased by about \$831 million from 2008 to 2009, and is projected to jump another \$1.2 billion in 2010. This is completely understandable if you consider the convenience and ease with which one can purchase and ship items via the internet, as compared to the time, hassle and energy expended by visiting the shopping malls. However, the increased activity in the e-commerce world is partnered with that of identity thieves who prefer the internet approach.



So, if you decide to be cyber-Santa this year, consider adding these online shopping tips to your checklist!

- ✓ Beware of phony websites offering popular products for a deal. If it seems “too good to be true” and you are not familiar with the website, research its credentials and proceed with caution. Before proceeding with payment, check to make sure the website is secured. A secured website will read **https://** and then the web address in the URL. That little, inconspicuous “s” after the “*http*” indicates transmissions on the website are secured by encryption. Many websites will also have a website security verification logo, usually near the bottom of the page, which indicates secured payment processing. But be cautious, as phony websites can spoof this logo.
- ✓ Observe which payment methods are being offered. If check, cash and money order are accepted but not credit cards, you may want to reconsider. Credit Cards are the safest way to online shop because they do not provide a direct link to your actual funds or your personal identity, and they can easily be cancelled if lost or stolen.
- ✓ Be sure to read your order/shipping confirmation e-mails closely. One popular form of scam based phishing during the holiday season is to send out spoof confirmation e-mails that ask customers to verify their account information or other personal information in order to confirm the purchase. Refrain from exposing yourself to this identity fraud tactic. You can also check the veracity of these e-mails by looking closely at the sender’s e-mail

address and the links you are asked to click on. If they are incoherent or misleading, be sure not to click any links, reply to the e-mail, or provide any information.

- ✓ Beware of E-cards. You've seen them. The cute, animated cards with music and a special note? E-cards are popular during the holiday season. But, if yours is a scam, the malware you inadvertently download when attempting to view the card will not be so popular. Avoid following any links to download software that the e-mail claims is required in order to view the greeting, as this link may deceive you into downloading a Trojan horse virus instead.
- ✓ Always use strong online passwords that include letters, numbers and symbols if possible. When creating passwords or pin numbers, avoid using any part of your social security number, mother's maiden name, birth date, middle name, pet's name, consecutive numbers or anything else that a hacker could guess. Also consider changing your passwords periodically to further prevent chances of a breach into your account access.
- ✓ Exercise caution with classified ads and auction websites. On the internet, it is easy for criminals to post items for sale that are stolen or that they cannot deliver. When shopping these ads, review the seller's contact and rating information, product description, purchase policies, and any fine print very closely. Also avoid providing your financial information directly to the seller through unsecured means, as they can easily use it to commit fraud. Make sure that the website used to process your payment is legitimate and secured.
- ✓ Monitor your financial accounts and credit reports for suspicious activity. This is one of the best ways to identify and prevent fraud and identity theft from meeting their damage

potential. Monitoring your financial accounts and credit files on a regular basis will allow you to quickly detect and thwart unauthorized transactions, thus reducing risk and lessening the amount of damage to recover from. Many identity fraud victims remain unaware that their identities are being used because they fail to check their financial and credit records for changes. The longer these crimes go undetected, the more difficult it is to fully recover from them.

If you do decide to go the "old fashioned" route to your local retail establishments, you are not off the hook. Identity thieves are no strangers to shopping malls, and they are increasingly getting more clever and inconspicuous. As you stand in line and pay for your purchases, be wary of the people in close proximity. With today's camera and video phones, your credit card information is at greater risk for being captured and abused by a sneaky fraudster. Therefore, guard your credit card and pin number at the register. Also be sure to monitor your possessions closely as you weave your way through the holiday crowds. Pick-pocketing is still a popular and easy way for criminals to steal.

If you think you are a victim of identity theft, please contact:

**Identity Fraud, Inc.
1-866-4-IDFRAUD
(1-866-443-3728)**

