Be Mindful of the Fraud Grinch This Holiday Shopping Season
Friday, November 21, 2014 04:45:00 PM (GMT)

Capital One Offers Tips to Help Protect Shoppers' Personal Information

MCLEAN, Va., Nov. 21, 2014 /PRNewswire/ -- Holiday shopping is underway for many Americans and according to a recent survey from Capital One, they'll once again be doing much of their buying online. The survey found that while more than half (55 percent) of shoppers plan to go to a mall or local stores to buy their gifts, a large number (36 percent) will be searching and buying online. However they plan to shop, consumers are keeping fraud top-of-mind as they make their holiday purchases due to the data breaches experienced at various retailers this year. While neither mode of shopping is immune to fraud, there are steps consumers can take to protect themselves as they hustle and bustle.

In addition to where they shop, consumers are considering how they plan to pay. When asked about their holiday shopping payment method(s) of choice, credit cards topped the list with more than half of survey respondents (55 percent) saying they plan to use a credit card for their holiday purchases. Paying with cash was the second choice with 52 percent, and 24 percent will use either checks, debit cards, mobile payments or other means of payment this holiday season (survey participants were asked to select all that apply).

"Unfortunately, the threat of fraud is a reality, but it doesn't mean you're helpless. There are precautions people can and should take to help protect themselves and their information," said Phil Hatfield, Capital One Vice President, Fraud. "Ensuring that you're monitoring your accounts and getting alerts to make you aware of unauthorized activity are simple steps and things you should do year-round and especially during the hectic holiday shopping season."

Capital One offers the following tips for holiday shoppers to keep in mind when they're at the stores and shopping in the comfort of their homes.

When out and about shopping

- **Streamline your wallet** – Before shopping, clean out your wallet and take only the credit cards, checks and cash that you need for the day. Never carry your social security card in your wallet.
- **Watch out for skimming** - Inspect the ATM or credit card reader before using it. Do not use if any pieces are damaged, crooked or look out of place.
- **Protect your PIN** - Cover your hand and key pad when entering your ATM personal identification number (PIN). Thieves have been known to place hidden cameras even directly in front of the key pad.
- **Close out your session** - Press the 'Cancel' button once your ATM transaction is complete, and ensure you have your receipt and card in hand.
- **Be aware of your surroundings** – Be conscious of other shoppers standing nearby when you're making purchases. Identity thieves have been known to copy credit card information or snap photos of cards from their smartphones. Be especially aware if you're opening a credit card in the store, where you'll be sharing your social security number and other personal information on the application.
- **Hold on to your receipts** – Keep receipts with you – and get gift receipts that can be used for returns or exchanges. Shred receipts after you're certain the charges match to those on monthly bank and credit card statements.

When shopping online

- **Protect your computer –** Make your wireless connection password protected and make sure you have up-to-date anti-virus and anti-Spyware software. Run a scan of your computer at least once a month.
- **Use secure online shopping sites -** When you're asked to provide payment information, the Web site's URL address should change from *http* to *shttp* or *https*, indicating that the purchase is encrypted or secured.
- **Check out the seller** – In addition to third-party online customer reviews, look for online merchants who are members of a seal-of-approval program that sets voluntary guidelines for privacy-related

practices, such as TRUSTe (www.truste.org), Verisign (www.verisign.com), or the Better Business Bureau (www.bbb.org). Typically, merchants will list their affiliations at the bottom of their websites.

- **Ensure the website is legitimate** – Do some online searches using the business name and the word "scam" or "fraud" to see if others have posted about the merchant. Call the seller's phone number, so you know you can reach them if you need to. If you can't find a working phone number, take your business elsewhere.
- **Don't click hyperlinks from emails –** Be particularly suspicious of messages or promotions you didn't sign up to receive. Instead of following links, go directly to the store's website and navigate to find the special sale item. Familiar looking links in an e-mail can redirect you to a fraudulent Web site and spoof websites can be difficult to detect. The address bar and padlock can be faked.
- **Never give out your account information** – Never respond to emails or instant messages that ask you to provide account information for "verification." Don't follow links to websites in such emails either. These are known as "phishing" scams and are used to collect account information that can then be used for fraudulent purchases.
- **Consider how you'll pay –** Credit cards generally are a safe option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Don't send cash or use a money-wiring service because you'll have no recourse if something goes wrong.
- **Keep a paper trail –** Print and save records of your online transactions, including the product description and price, the online receipt and copies of any email you exchange with the seller. Read your credit card statements as soon as you get them to make sure there aren't any unauthorized charges.

Ways to protect your accounts

- **Sign up for security alerts** – Most banks and credit cards have free security alerts that can be activated by customers online and received via email or text message. Many can be customized and they help ensure one can quickly identify unusual activity or changes to an account.
- **Don't get stuck with fraudulent purchases** – Check for unauthorized charges on your bank and credit card statements as soon as you receive them. Contact your bank or credit card company immediately if you see any transactions you don't recognize. Capital One guarantees $0 fraud liability if a credit or debit card is ever lost or stolen and used without a customer's authorization.
- **Monitor your credit activity** – Keep tabs on activity that impacts your credit report and ensure it's accurate. Capital One credit card customers can sign up for Credit Tracker, which provides free bureau alerts that flag changes that could indicate fraud, such as opening a new account or a change of address.
- **Compile creditor information** – Keep a list of all creditor information including contact information, account numbers, expiration dates and any other relevant information.
- **Shred it** – Don't dispose of personal information in a public trash can—tear it up or shred it.

Survey Methodology

The Capital One Holiday Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 1,000 nationally representative U.S. adults ages 18+, between November 7th and November 14th, 2014, using an email invitation and an online survey. Quotas have been set to ensure reliable and accurate representation of the U.S. adult population 18 and older. The margin of error for the survey is +/- 3.1%.

About Capital One

Capital One Financial Corporation (www.capitalone.com) is a financial holding company whose subsidiaries, which include Capital One, N.A., and Capital One Bank (USA), N. A., had $204.3 billion in deposits and $300.2 billion in total assets as of September 30, 2014. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has approximately 900 branch locations primarily in New York, New Jersey, Texas, Louisiana, Maryland, Virginia and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

Logo - http://photos.prnewswire.com/prnh/20141030/155590LOGO

SOURCE Capital One

Contacts: Amanda Landers, 703-720-2478, amanda.landers@capitalone.com
Countries: United States
Industries: Retail, Banking & Financial Services, Household & Consumer Products
Languages: English
Primary Identifiers: COF-US
Related Identifiers: COF-US
Subjects: Public Safety