7 ways to avoid identity theft this holiday season

Consumers will face a slew of hidden threats as they pour into stores and scour retailers' Web sites for holiday deals over the next couple of days.

Retailers are moving to use more secure technology that is expected to cut down on credit card fraud, but credit experts say identity thieves will still be attempting to steal data that they can use to commit fraud in stores and online.

Nothing shoppers do can protect them fully from having their credit card information hacked or their identities stolen, said Nick Clements, co-founder of credit comparison Web site MagnifyMoney.com. (The Target hack in 2013, he recalls, was an attack on a large retailer that consumers could not have prevented.) But shoppers can take small steps to make it more difficult for identity thieves to go on a shopping spree under their name.

Use a stricter log-in

Use a different password for each of your online shopping accounts so that if someone grabs your username and password for one Web site, they won't be able to go on a shopping spree for other accounts. Some merchants such as Amazon have also introduced multi-factor authentication, which requires users to enter a code that is sent to their e-mail or phone number when they try to log on. The added step can make it harder for thieves with stolen user names and passwords to take over people's accounts. Shoppers can ask retailers to remember certain devices, such as their phones and home computers, but require the codes whenever someone tries to log on from a new device.

Choose credit over debit

While debit card users are also protected from fraud, identity thieves who go on a shopping spree with your debit card would be tapping into the cash you need to pay your everyday bills. In contrast, fraudulent charges on a credit card would only take up part of your credit limit. "It's

not fun when all of a sudden that cash you need to get through the month is gone," Clements said.

Use a chip card

This will be the first holiday shopping season where most retailers are required to have credit card terminals that read the more secure chip cards. The chips, which generate a new code every time they are used, are supposed to be safer than the magnetic stripes on cards, which send the same information for every transaction and are easier to copy. About 7 in 10 Americans have at least one chip card, according to Visa. People who don't have a chip card yet can call their banks to request one.

Consider mobile pay

New mobile payment options such as Apple Pay and Android Pay let consumers shop with their cellphones at retailers and through certain apps. Instead of swiping or dipping their credit cards, shoppers tap their phones, which transmit a unique code to the retailer for each purchase that is useless to fraudsters, said Mike Cetera, a credit analyst with Bankrate.com. In the case of Apple Pay, shoppers have an added protection by requiring that their finger prints be used to complete the transaction.

Monitor transactions

Most banks will refund consumers for fraudulent charges made with their debit or credit cards as long as they report it in a timely matter. Consumers should check their transactions every day or every other day to scan for unauthorized purchases, especially when they are using their credit cards frequently. If you don't have time to monitor transactions every day, then you can set up alerts to have a message sent to your phone or e-mail every time your card is used.

Stick to one card

Using one card for most of your holiday purchases can limit the number of cards you need to track closely. It also cuts down the chances that more than one card will be compromised. (Though you should still check transactions on all of your cards periodically.) Try to use a card that is different from the one you use to pay your monthly bills. That way you can avoid having to reset all of your payment settings if your card is stolen.

Watch for phishing scams

Fraudsters often send e-mails that promise consumers a phony promotion if they enter their personal information or click a link. The messages can include logos that closely resemble those of the legitimate retailers. And the links may download malware on your computer that gives thieves access to your personal information. Shoppers should check the Web address included in the messages and avoid clicking on links. Visit the retailer's Web site directly before making a purchase.

Visit **www.countrywideppls.com** for more information!