

AMERICA'S LEADING IDENTITY RESOLUTION AND EDUCATION SERVICE

THIS MONTH'S TOPIC...

The Holiday Give-and-Take

Avoid identity thieves' seasonal rush

For many, the holiday season is cause for excitement—an opportunity to spend time and share gifts with the ones you love. Unfortunately, law-abiders aren't the only ones who find this time of year attractive. In this month's newsletter article, "The Thieving Season," we outline the identity theft risks posed by the holiday season—from surges in travel and shopping—and offer tips on how to mitigate them.

The editorial, "A Holiday Season With No Red Flags," meanwhile, examines the delay in the enforcement of new anti-identity theft guidelines for credit issuers, and how it leaves consumers vulnerable through yet another season. Now is the time for everyone to do their part to combat identity-related fraud. We hope you find the information here to be useful and that you have a safe and happy holiday.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters
To learn about the latest scams on identity theft, visit: www.identitytheft911.org
Comments, questions? Contact us: newsletter@identitytheft911.com



THE THIEVING SEASON

Holidays Marked by Fraud for Many



At the height of the holiday shopping season last year, someone started opening credit card accounts in Michelle McCambridge's name. McCambridge didn't discover that her identity was stolen until January, when she received thousands of dollars' worth of bills for purchases she never made.

"I was kinda furious," McCambridge, a retail clerk at a J.C. Penney store in the Seattle area, later told the Seattle Times.

One week after McCambridge discovered she'd been victimized, a woman walked into the women's casual department where McCambridge works. The woman asked to open a J.C. Penney credit card. For identification, she gave a driver's license with McCambridge's name and address on it. ▶

Of all the cash registers in all the stores in all the world (much less Seattle), this bumbling identity thief picked the one where her victim happened to work. McCambridge excused herself and asked other managers to point security cameras at her sales counter, capturing the video that eventually was used to indict five people for allegedly stealing 39 identities.

“Yes, no violence was done to me, but that’s my identity,” McCambridge said. “It’s a violation of your space and who you are.”

Many people will experience this sense of violation as a result of this holiday and Christmas shopping season. More than 9 million identities are stolen every year, according to the Federal Trade Commission, and a disproportionate number of those crimes happen during the holiday shopping rush.

One reason for the seasonal surge is need – many people push their finances to the limit during the holidays and use fraud to bail themselves out. Another reason is opportunity. With so many people buying so much stuff in so many different ways, the holidays are a prime time to commit identity fraud. And finding the perpetrator can be difficult.

“Identity-theft crimes are some of the most difficult criminal cases to investigate,”

Social Security Administration
Special Agent Joseph Velling
told the *Seattle Times*.
“It is not that law

enforcement does not know what crime was committed. Rather, it is a simpler question — who did it?”

Unfortunately, a situation like McCambridge’s, where catching the thief is so easy, is all too rare.

‘Tis the season

For identity thieves, the holiday season is the season of taking: Taking purses and wallets, as more and more shoppers descend into retail stores. Taking credit card and debit card numbers swiped by keystroke-recording malware. Taking personal information obtained in phishing schemes and phone conversations in “vishing” schemes.

“We tend to be busiest during the fourth quarter of the year—October,

remember how to mitigate yours.

“The most common thing that goes up during the holiday-time is what’s considered account takeover fraud — the fraudulent use of existing open accounts,” Vargas explains.

“People are shopping more often, and credit cards are out of their possession more often,” Vargas says. In addition to the physical loss or theft of credit and debit card numbers, the season is ripe for card ‘skimming’— that is, the deployment of small devices that steal account information. “When you’re shopping, be careful about your cards — whom you are handing them to and what that person’s doing once you hand it to them. Make sure you get your cards and ID back if you hand them to someone.”

“Identity-theft crimes are some of the most difficult criminal cases to investigate. It is not that law enforcement does not know what crime was committed. Rather, it is a simpler question — who did it?”

Social Security Administration Special Agent Joseph Velling

November, December,” says Raul Vargas, certified fraud examiner with Identity Theft 911. “I know that traditionally financial institutions take their biggest losses in January or February because fraud occurs around the holidays, but consumers don’t find out until these months.”

One consumer’s risk is a seasoned fraudster’s opportunity. As the shopping season approaches, it’s important to

Indeed, one of the most important consumer tips of the holiday season is a familiar one worth repeating: Be mindful of your belongings — don’t leave wallets and purses unattended or within easy reach of a pickpocket. And only carry identification and credit cards you’ll need when you shop.

The Federal Reserve Board chairman Ben Bernanke’s wife, Anna, learned firsthand



what happens if you don't heed that advice. She was sitting in a Starbucks on Capitol Hill when someone stole her purse, *Newsweek* reported. Inside were her Social Security card, driver's license, four credit cards, and a checkbook with the Fed chief's bank account number, home address and telephone number printed across each check. Within days, the crooks raided the Bernanke's personal bank account.

But even if she was alert, it might have been hard for Anna Bernanke to protect herself. That's because the crook who stole her purse was a member of a sophisticated crime ring that called itself "Cannon to the Wiz" ("cannon" being a term for expert pickpockets).

If you're traveling for the holidays, make sure that someone is picking up your mail for you. That way they can gather up all those unsolicited credit card offers, which offer open invitations for fraud.

A Secret Service investigation found that the crime ring stole \$2.1 million from various victims. Her case reminds us that we're vulnerable all year round; however, criminals thrive on shoppers' heightened state of distraction during the holidays.

So this leads to the next piece of advice: Before you pay attention to your wallet or purse, pay attention to what you put in it. Only carry the identification and credit cards you'll need when you shop. Likewise, NEVER carry your Social Security number with you. Criminals can use it to open up fraudulent credit accounts in your name (not to mention gain employment, obtain medical treatment, set up utility service and more).

If you're traveling for the holidays, make sure that someone is picking up your

mail for you. That way they can gather up all those unsolicited credit card offers, which offer open invitations for fraud.

And like always, be sure to shred your credit card and financial statements and other financial documents.

Online Shopping Safety

In this age of growing Internet commerce, fraud doesn't wait for you to go to a retail store, handle a Social Security card or write an actual check. Many more crimes are happening online, says Identity Theft 911 Information Security Officer Ondrej Krehel.

The first step is to protect your personal computer. That starts with choosing the right Web browser. The most popular ones are Internet Explorer, Firefox or Safari. Before you use them, be sure you have the latest, most-secure version. Newer versions include phishing filters, pop-up blockers and malware protection, among other improved security features. Make sure that your operating system and Internet browser have downloaded the latest security patches

Next comes the process of buying and installing antivirus, anti-malware and personal firewall protection. These programs have become the bare minimum steps required to protect yourself

online, Krehel says. Make sure that your security software is up-to-date and updated regularly. Because simply having security software on your computer without properly updating it is like becoming a member of a gym but never going.

Personal firewalls should stop unwanted applications by displaying a warning message, and then you can decide if that application should be allowed to open, Krehel says. "Tweaking" and managing your own firewall protection can be challenging for a basic user, but firewalls usually come pre-configured, and technical support is included. Tips and tricks for personal firewall improvement can be found on various vendor and technical Web sites.

There are many antivirus vendors, and some of them provide all of the above in one program. If you're unsure whether your computer is "clean," you can use free online scans from major antivirus vendors, such as Kaspersky, Eset, McAfee and Symantec.

If you use a laptop to shop, be aware of where you go for Internet access. Shared wireless access points, like those WiFi found at coffee shops and other public places, are not secure places to disclose your private financial data. Depending on an access point's security configuration, an attacker may be able to eavesdrop and record whatever is being transmitted over the network.

It's true, there are seemingly countless points of entry for criminals to exploit your identity, and the distractions of the holiday only give them an easier way in. And while there is no way to fully guarantee the protection of your identity, you can always increase your chances of staying safe, mitigate the risks, and – if you do become a victim – hopefully discover the crime before too much damage is done. ■

15 TIPS to keep in mind while shopping online this HOLIDAY SEASON



1. Make sure you have installed and updated antivirus, anti-malware and personal firewall software on your computer. Your operating system and Internet browser should be updated with the latest security patches.
2. Only shop on secure sites. To see if a Web site is secure, look for "https" in the address bar. Also, there's usually a small yellow padlock logo at the right of your Web browser address bar. If you double-click on the lock, a digital certificate of the Web site will appear. It's a good idea to review these certificates on the sites that you are not familiar with.
3. Make sure that you enter the correct URL. There are cases where hackers have purchased misspelled domains.
4. Shopping Web sites have no reason to ask for your Social Security number, or passwords to your e-mail or bank accounts as part of the buying process. Never provide them.
5. If you suspect a Web site is not what it claims, leave it immediately. Do not click any buttons on the site, run any content or download any software.
6. Use different "strong" passwords (those that are more secure) for online retailers and your personal e-mail accounts. A strong password is composed of numbers, upper- and lower-case letters and symbols. For example, a password like "3Dogz\$\$!" is a better option than "1006." The longer and more unique the password the better, but make sure it's also something you can remember.
7. Before purchasing anything on a Web site, read site reviews or blog comments by other people. Use sites such as Pricegrabber.com or Froogle.com (Google shopping) for comparing prices and to read users' reviews of the retail Web site.
8. Retailers may try to lure you into saving your personal information on their Web site in return for more convenience or better deals. Don't do it. So many Web sites have had their customer databases breached by identity thieves lately that it's just not worth the risk.
9. Read each Web site's return and privacy policy before making your purchase.
10. Be aware of phishing e-mail scams that include Web site links advertising incredible deals. Rather than clicking on them, type the link of known sites by hand into your browser.
11. Use credit cards for online purchases, not debit cards. That's because debit cards automatically deduct money from your bank account. Try to use cards with low credit limits to minimize the damage in case someone steals your information to take over the account. Or, use a "one-time" credit card number from payment processors such as PayPal.
12. Do not send your payment information via regular e-mail; these communications are not secure.
13. As a general rule, uncheck boxes advertising "additional offers." These services are sometimes offered for a low initial fee that later increases to a high, recurring charge on your credit card.
14. Save records of all your purchases either in an electronic document or on paper.
15. Don't forget to power off your computer completely when you are finished using it.

Additional sources:

<http://www.staysafeonline.info/content/online-shopping>
<http://www.microsoft.com/security/pypc.aspx>
<http://www.onguardonline.gov/topics/online-shopping.aspx>
<http://www.us-cert.gov/cas/tips/>

A HOLIDAY SEASON with No Red Flags

Editorial by Adam Levin



Michelle McCambridge had a rare opportunity, and she used it brilliantly. After her identity was stolen during the peak of last year's holiday shopping season, McCambridge assumed she would never get the chance to confront the person who violated her.

But just a month later, the thief unwittingly walked right up to the victim and tried to commit another fraud. Even though she was caught off guard, McCambridge did exactly the right thing. Instead of confronting the thief in a rage (as many probably would have done), she had the presence of mind to ask her coworkers to train security cameras on the woman, gathering the first piece of evidence that eventually busted a sophisticated crime ring. ▶

Unfortunately, most identity theft victims never catch such a break. Like McCambridge, they usually have no idea how thieves managed to steal their account numbers, address, Social Security number and other personally identifiable information. Like McCambridge, most people don't discover they've become victims until months after the crime, when they start to receive bills for purchases they never made. Without any information about the suspect or how the crime was committed, most victims find that police can do little to help.

And like McCambridge, victims are left feeling angry, violated, powerless.

Who's to blame?

It's no coincidence that reports of identity-related fraud spike after the holiday season. We visit so many stores, in person and online, and everywhere we go we hand out the keys to our financial lives: Our credit cards, our checks, our driver's licenses, phone numbers and addresses, not to mention all the ephemera we carry around in our wallets and purses, like insurance and library cards. Each of those bits of information is one more piece of the puzzle that thieves use to construct a new identity that can be used for fraud.

It doesn't help that giant retailers offer instant credit to anyone who presents a driver's license without verifying that the license is legitimate. Every level of government maintains databases containing citizens' personal information, and most of them post those databases online for identity thieves to view from the comfort of their bedrooms.

A season of change, delayed again

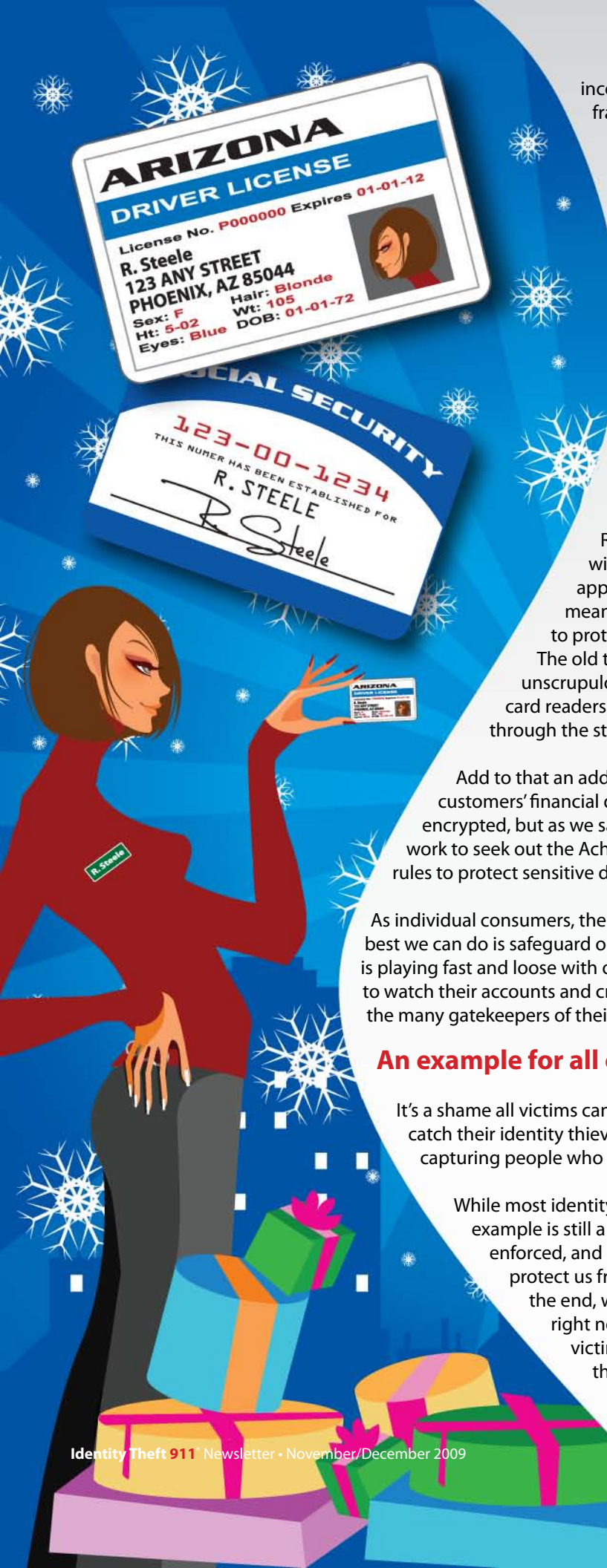
In this bleak economic environment, however, we thought that this year we might finally be able to celebrate some measure of progress. This was supposed to be the first holiday season in which the Federal Trade Commission required all credit-issuers to comply with the Red Flags Rule, which calls for the monitoring of credit applications for warning signs of identity theft. In theory, if creditors abided by these guidelines, we would expect to see fewer reports of new account fraud in the months post-holiday.

The commission already postponed the deadline for enforcement three times. Incredibly, they've done it again. Under heavy lobbying pressure from retailers, lawyers and physicians (the latter two who are counted as creditors under the rule because they accept deferred compensation for services), the FTC postponed enforcement of the Red Flags rule for the fourth consecutive time, pushing the deadline back to June 1, 2010.

This is an outrage. Millions of consumers will pay the price for the commission's cave-in with stolen identities and fraudulent credit charges. According to its statement, the FTC made its decision under intense pressure from members of Congress, who were being lobbied hard by retailers and other creditors. These companies appear willing to put consumers at risk indefinitely.

Unfortunately by doing this, the companies are in many respects hurting themselves the most. That's because the Red Flags Rule is not some onerous new regulation from Washington. It's a series of common-sense steps that any smart business should have





incorporated years ago to protect itself and its shareholders from fraud. Too bad they don't see it that way.

Since the Federal Trade Commission and members of Congress refuse to stand up for consumers' rights, we must do it ourselves. As part of your holiday to-do list, I urge you to write a letter to your senator and congressman expressing outrage that the Red Flags Rule was postponed again, and urging them to take steps now to ensure that next year's June 1 deadline is not just another empty promise. The rule is important because it places responsibility for identity theft squarely where it belongs: The credit-granting organizations that enable thieves to convert stolen identities into services and cash. We cannot afford, nor should we be expected, to go another holiday season without its protection.

The true test will come

It will take time to see how well creditors comply with the Red Flags Rule when it does go into full effect. Many creditors will likely take all the steps required to safeguard their credit application process, but others will undoubtedly fall short. That means the responsibility remains with us, the consumers and citizens, to protect ourselves. And that job grows more complicated every year. The old threats were bad enough – purse snatchers, check forgers, and unscrupulous sales clerks who surreptitiously swipe credit cards on hidden card readers to steal the account information before running the charges through the store's machine.

Add to that an additional layer of risk. Companies still gather and transmit their customers' financial data, at brick-and-mortar stores and online. It's supposed to be encrypted, but as we saw with TJX and Heartland, not only do hackers make it their life's work to seek out the Achilles' heel in a system, but sometimes companies don't follow the rules to protect sensitive data, period.

As individual consumers, there's little we can do about retailers' data security practices. The best we can do is safeguard our own information, and vote with our feet if it seems a company is playing fast and loose with our financial information. In the meantime, consumers are left to watch their accounts and credit reports for signs of fraud that might have occurred because the many gatekeepers of their information were not following the rules.

An example for all of us

It's a shame all victims can't have Michelle McCambridge's luck, tenacity and resources to catch their identity thieves and that few ever get the opportunity to play a lead role in capturing people who try to defraud them.

While most identity theft victims never meet their doppelgangers, McCambridge's example is still a good one to follow – while we wait for better protections to be enforced, and even after they are. We all want police, banks and retail stores to protect us from identity theft, especially during the holiday season. But in the end, we're still left to be our own best protectors. We have the power, right now, to safeguard our identities and reduce our risk of becoming victims. It isn't a mirthful thought, but it is a realistic one. It is not a threat to fear, rather it is an opportunity to be seized. ■