By Adam Levin, chairman and co-founder of credit.com and IDT911

12/14/15

The holiday season is a busy time of the year for identity thieves and other kinds of identity-related fraudsters. Scams abound, but if you follow a few simple rules, you can sidestep some avoidable holiday blues.

There is so much personally identifiable information floating around — readily available on the dark web where information black markets thrive — that it truly is a wonder more people are not becoming victims. That said, Javelin Strategy and Research reported that $16 billion was stolen last year from 12.7 million identity fraud victims. It is a stunning figure — a new victim of identity fraud every two seconds.

While there is no way to avoid getting "got" entirely, there's plenty you can do to reduce your attackable surface. In my new book Swiped: How to Protect Yourself in a World Full of Scammers, Phishers, and Identity Thieves, I lay out a plan called the Three Ms: Minimize your exposure to fraud, monitor your accounts and manage the damage.

I urge you to put the above three habits in daily rotation, but during the holidays you should be on an even higher than usual alert. Before you go do something rash like seal your chimney, there are things that you can do to make yourself a little more secure this holiday season.

Phone Calls & Email: Never Trust, Always Verify

You might be surprised who "has your number," and I don't just mean that figuratively.

As a result of major data breaches at Heartland Payment Systems, eBay, Target, Home Depot, the Office of Personnel Management, Anthem, Premera and countless others, there are more than a billion records containing sensitive personal information “out there.”

The information compromised takes many forms, ranging from personal email addresses, phone numbers and a person’s name and street address, to more granular information such as place and date of birth. And yes, it often includes the skeleton key to all things financial, a Social Security number (SSN).

As if that weren’t already enough to keep you up at night, there are ways for a savvy thief to know even more about you, making it hard for you to discern whether that phone call or email you receive from a trusted source is actually legit.

Earlier this year, the *New York Times* reported that an MIT graduate student, Yves-Alexandre de Montjoye, had successfully re-identified anonymized personal information from mega data sets that are routinely made available for research purposes. What he found was astonishing: “knowing just four random pieces of information was enough to reidentify 90 percent of the shoppers as unique individuals and to uncover their records.”

If a graduate student can do it, so can a clever thief. This is one of the many reasons you should consider thinking twice when you are contacted by a trusted source or favorite retailer. Put simply, it might be a fraudster.

There is a relatively easy way to protect yourself: hang up that phone and don’t click through on emailed links, no matter how good the proffered sale or incentive is. Instead, go online and check to see what’s what. And remember to look for the lock. In the URL address area, usually to the left, you will find an icon of a lock on secure sites. If you don’t see it on a major retailer or bank site, close the window and do another search for the correct address.

An Added Bonus: Staying Safe Can Rein In Holiday Spending

The second M in my book is monitor. The easiest way to avoid trouble from identity-related

fraud is to discover it as quickly as possible.

This can be a challenge with some kinds of fraud, such as child identity theft where parents don't think to check their kids' credit (identity thieves do, and the knowledge of a child's SSN can mean years of spending to them) or open those explanations of benefits that your healthcare provider sends out, which are often the only way to know if a third party has been Goldilocks-ing your health coverage.

You need to check your accounts every day. That's right. Every day. The benefits are not only knowing if you have been scammed, it can also curb your spending and be a reminder if you've missed a payment if you're monitoring your balance every single day.

You can also monitor your credit for other signs of fraud and identity theft like new-account fraud – when someone uses your information to apply for credit, for example.

What You Should Add to Your Holiday Checklist

Log into each of your credit card accounts and make sure you recognize all the charges. This is precisely the time of year fraudsters will try a small charge on your account, knowing that thousands of successful charges for $7.84 will go unnoticed. You should also check your accounts on auto-pay, such as cellphone carriers, and review your bank accounts daily.

The good news: most organizations that accept payment can also provide real-time transaction notices, so if you set up transaction alerts (and more importantly, look at them), you will have incorporated a great deal of what needs to happen to stay on top of your identity portfolio, which is every bit as valuable as any stock portfolio.

In addition to checking your accounts, here's a list of things that may help you stay safe from scams — not all of them identity-related.

- If you go online while away from home, always use a secured wireless server.

- Never ask for a number to call nor accept their proffered number when you receive an unsolicited phone offer. Either check the back of your credit or debit card, or go to the official site (which you verify), to get the right number.
- Keep all receipts and check them against credit card statements.
- Take screenshots of your confirmation screen for online purchases, and save confirmation emails.
- Spyware, phishing and social ads are very tricky these days. Instead of clicking through from an emailed offer or tweet, better to search for your destination and click the link.
- Overseas orders are not all suspect, but do your homework to make sure there are no complaints against the company.
- Gift cards are increasingly a target for fraud, whereby fraudsters record physical card numbers at retail locations using a magnetic strip reader (not all cards require a scratch-off PIN code) and then try to use them in the hope that the card has been purchased and activated, but not yet used. If they do find a balance, they can move the money by issuing themselves an e-gift card.

As this is the time of the year when we are the most distracted – our heads are into the joy of the holidays and most of us have day jobs – identity thieves and scammers look at us at the gift that keep on giving. Stay alert, spend wisely and never forget that the ultimate guardian of the consumer is the consumer.