FINANCE

Avoid Identity Theft and Outfox Scammers

by C.D. Moriarty

What do Target, Citizens Bank, and New York Life Insurance all have in common? They have all had corporate security breaches. If large, tech-savvy giants have these issues, it's no surprise that the average American is concerned. According to a survey by Citriz Security of 1,001 adults, 69 percent think that having their personal information stolen in their lifetime is inevitable.

Scams are rampant and identity theft is becoming commonplace. "Every two seconds someone's identity is stolen in this country," said Greg Marchildon, state director of AARP Vermont. "Con artists think they can bully people into forking over their hard-earned money."

When people think of money scams, phone calls targeting the elderly usually come to mind. But scammers are getting increasingly savvy. They now have caller ID systems and contacts through social media at their disposal, enabling them to make increasingly sophisticated phone and e-mail pitches, taking in even those who don't consider themselves gullible.

> **"Every two seconds someone's identity is stolen in this country."**
> *– Greg Marchildon, state director of AARP Vermont*

How can individuals adequately protect themselves when even big companies with deep pockets and high-end technology are having data breaches? You can arm yourself with information. Educating yourself about current scams is key to protecting yourself.

Know Thy Enemy

What follows is a list of common scams. For more information on scams, go to the Vermont attorney general's description of typical scams at *www.uvm.edu/consumer/?Page=scams.html*.

Debt: You have recently filed for bankruptcy. Someone claiming to be from your lawyer's office calls you, requesting you to immediately wire money to satisfy a debt. The caller ID correctly identifies your lawyer's office. However, the urgent call comes late at night—which seems suspicious, plus you have no way of confirming if the call is really from your lawyer. Or you've taken out a loan and then get a phone call or e-mail claiming that the loan is in default: you're in danger of criminal charges or some other dire consequences if you don't immediately pay a certain amount. Or the IRS e-mails you insisting that you owe money. Do not fall for any urgent requests for money.

Emergency: You get an e-mail from a friend or family member. In the message your friend says he has been traveling in a foreign country, but disaster has struck: someone stole his wallet and he's stranded. He asks you to please wire him money. Something seems odd, and yet the return e-mail address is correct. Or you get a call from an agency or person claiming to need money or help for a relative who is sick or injured. Confirm with others before sending money. Much like the debt scams, the scammer is trying to catch you off guard and in fear.

Investment: Someone calls you promising a terrific return on a time-sensitive deal. If anyone promises to double your money or let you in on a private investment, be wary. All investment vehicles are legally required to be registered as a security. First, check with the Securities and Exchange Commission *(www.sec.gov)* to confirm. Typically, outrageous promises have nothing to do with legitimate investment offers. Consider the old adage: "The best way to double your money is to fold it in half."

Romance: Sometimes our heart overrules our head, and we unwittingly empty our pocketbooks. There are several tales of women meeting men online and having a digital relationship for months. The man is sensitive and loving—almost too good to be true. And then he gets into financial trouble and begins to ask for money—and then more money. Ten of thousands of dollars later, the woman finally becomes suspicious and cuts off contact. Embarrassed, she does not want to admit she gave someone she never met thousands of her hard-earned money. Whether a dating service, online site, or social media, proceed with caution.

Construction and repair: If a contractor requests a large amount of money upfront before starting work, do not automatically provide it. Confirm with neighbors, friends, or the local better business bureau any repair folks before hiring them. Most companies get paid for the work they do as they do it, not ahead of time.

Protect Yourself

Just because in this day and age identity theft and scams are becoming commonplace does not mean you need to feel complacent. First, there are a few basics to be aware of so that you aren't drawn into a scam: Know that the IRS will not call or e-mail you, police and federal agents do not knock on your door looking for money, and tech companies do not call for access to your computer for updates.

There are regular sound steps you can take to protect yourself and be financially smart. Keep your receipts and monitor your spending. Many fraudsters first make small purchases with the credit information they obtain. Then, if these are never reported or caught, they make bigger purchases. So there is motivation to review your credit and debit card statements: if you see a purchase that was not yours, report it to the card company right away.

Check your credit reports annually *(www.AnnualCreditReport.com)*. You will be able to see if someone has used your personal information to apply for credit. Meantime, you should be doing a quality check on how these large credit-reporting agencies are inputting your information. Once you become comfortable with your credit report, you will know the steps to take to report fraud and freeze your credit with the agencies.

Practice cybersecurity. Credit card information, passwords, and personal data should not be shared. Be cautious about providing personal information online, even when a website offers a prize or makes some other promise. Know that the legitimate companies have "https" at the beginning of their URL to signal the site is secure.

Be aware that the information you input while using public Wi-Fi is a prime target for scammers. Choose wisely what you access on free Wi-Fi. This is not the time to do online banking, use credit cards, or access anything like e-mail that requires a private code.

Create security on your mobile devices with a password. Make all your passwords long and strong and change them regularly. Check for updates in your security software and run scans several times a week. And never click on links from unknown e-mails.

We may not be able to stay completely ahead of the scams, but we can surely stay on top of our digital presence. Taking care of your finances has many more layers in 2015 than 50 years ago. The one thing that has not changed is that your money is still your responsibility.

C.D. Moriarty writes from Bristol and is a financial speaker and coach dedicated to empowering others around their money. Her financial advice and information are at www.MoneyPeace.com. ❐

What to Do If You Are Scammed

If you are scammed, report it to the attorney general's Consumer Assistance Program (*www.uvm.edu/consumer/?Page=complaint.html*). Note that most large companies, after suffering a breach of secure information, offer a free credit monitoring service for three to six months to their customers. For example, after getting breached, Target offered three months of free monitoring. If you are offered a free service, take it. Otherwise, credit monitoring companies generally charge $10 to $15 per month, which may not be worth the cost, since your credit card company is liable for any fraudulent transactions, and you are only responsible for $50 of that credit card debt. Understand the implications and costs of a service before you sign up.

Reporting a Scam

Vermont Attorney General's Office
www.ago.vermont.gov; 802-828-3171

Consumer Assistance Program (UVM/VT Attorney General)
www.uvm.edu/consumer/?Page=complaint.html; 800-649-2424

Vermont Department for Financial Regulation
www.dfr.vermont.gov; 800-964-1784

Federal Securities and Exchange Commission: *www.Sec.gov*

Better Business Bureau: *www.bbb.org*

Social media sites: If a scam happens through or as a result of a site, let the company know. They typically shut down the offenders, preventing someone from ending up in the same situation.

Want More Information?

National Cyber Security Alliance: *www.staysafeonline.org*

Stop. Think. Connect.: *www.stopthinkconnect.org*

AARP's blog: *www.Aarp.org*

Free Annual Credit Report: *www.AnnualCreditReport.com*