Fred Dunbar
CLU®, ChFC®, RFC®, AIF®

We bring quality services to the shore, providing a "common sense" approach to pursuing our clients' financial goals for thirty years.

Financial Planning* Asset Management* Investment Planning* Retirement Planning

COMMON ¢ENTS PLANNING

1-800-647-0762

239 Baltimore Pike Glen Mills, PA • 6606 Central Ave. N. Sea Isle City, NJ

fdunbar@commoncentsplanning.com • www.commoncentsplanning.com

*Securities offered through Commonwealth Financial Network, Member FINRA/SIPC. *Advisory services offered through Planning Directions Inc., a Registered Investment Adviser, are separate and unrelated to Commonwealth.*

DEALING WITH AN IDENTITY CRISIS

Normally I love to wish everyone the holiday cheer you so richly deserve. My wish this year is that you give yourself the gift of protecting your identity.

You might have heard that on Sept. 7 the credit-rating agency Equifax disclosed a massive data breach that affected approximately 45 percent of the U.S. population. The original number released by Equifax was that 143 million people were affected. They later adjusted that to slightly more than 145 million. Hot on the heels of this major breach, PC Magazine reported that the user database in Equifax's Argentina office had "admin" as both the username and password. That is unbelievable.

Last year, Yahoo! revealed that it had a massive breach involving practically 1 billion accounts. The Yahoo! breach exposed users' phone numbers and passwords.

The Equifax breach was more egregious. Equifax said its breach included names, Social Security numbers, birthdates, addresses and, even in some instances, driver license numbers. With this type of information, any bad actor could open a credit-card account or apply for a loan because he or she would have all of the pertinent information.

This article is not to frighten you, but to make you highly aware.

In addition to these breaches, there also is fraud using ATM "skimming" devices. Back in June, I received a call from my bank questioning withdrawals from ATMs in North Philadelphia. The withdrawals started early Friday evening from various bank ATMs through the weekend. By 7am Monday, the total amount withdrawn from our checking account was more than $1,416. This was a total of five ATM withdrawals. I went to the bank and swore an affidavit that these withdrawals were not mine. About three days later, the bank refunded the fraudulent withdrawals and placed the money back in my account.

Also, there are stories in which credit-card information has been stolen while people are making purchases at a store or paying for their meal at a restaurant. Your credit card is out of sight for just a short time, but that is all it takes. About a year ago, I received our statement that listed a purchase at a sporting-goods store online site and that it was being sent to an address I did not recognize. I immediately called my bank to cancel my credit card and alerted it about the fraudulent charge.

One thing you can do is set up online alerts from your credit-card companies and banks triggered by a parameter such as the balance or size of the transaction. I have our credit-card companies send me an alert on any purchases. Monitor your own accounts for fraudulent activity indefinitely. Check your online bank statements and your credit-card statements on a regular basis, at least weekly.

Unfortunately, data theft happens all the time, so you must be vigilant.

Maybe we hear about identity theft on a regular basis and we have become callous to it and don't pay attention.

I recently returned from the national conference for my broker-dealer, Commonwealth Financial Network, where I attended a compliance workshop on this very subject.

How can you protect yourself?

First, Google “Equifax” and see if your information has been impacted.

Look for the box showing “Equifax cyber security incident.” Click the box to enter the www.equifaxsecurity2017.com box. Then start by clicking on “Am I Impacted?”

Next, enroll in Equifax’s credit monitoring and identity theft program. Equifax is offering a one free year of its Trusted ID Premier (its credit-monitoring and identity-theft protection products) to all U.S. consumers, even if you are not affected by the breach ...

Once you enter your information in Equifax’s self-service portal, you will then be given an option to enroll in the Trusted ID Premier. Click “enroll” and you will then be provided with an enrollment date. Be sure to write down this date and return to the site on or after that date.

Be wary of emails that come from Equifax. Because of the high volume of victims, Equifax has notified only 209,000 consumers whose credit-card information may have been affected via US postal mail. Do not trust emails that appear to come from Equifax regarding the breach. Attackers are likely to take advantage of this situation and craft sophisticated phishing e-mails.

Monitor your accounts at the credit agencies for suspicious activity.

For additional information, visit the Equifax FAQs page regarding the incident.

Place a security freeze on your credit files. This will help keep fraudsters from opening new accounts in your name. Block your credit history by applying a credit-file freeze at all three credit-rating agencies, Equifax, Experian and TransUnion.

Two things about security freeze you should be aware of:

Security freeze may not protect you from every identity fraud. If you’re looking to buy a home or a car, you must then remove the freeze to allow your bank or lender to access your credit information.

Please note there might be a fee to apply and, in some cases, to remove the credit-freeze service from your credit file. Also note that Equifax stated it would not charge for credit freezes for those affected by the breach.

Protect yourself and your money.

Another way of protecting yourself is with your passwords. Change your passwords on a regular basis THIS IS CRITICAL. One of the biggest complaints I hear from clients is that they hate passwords. They have trouble remembering them. Amazingly, many use the same password for all of their accounts. So basically, if someone hacked one of your accounts, then they would be able to get into all of your accounts.

Never start your password with a capital letter or end your password with !. The bad guys have programs designed to break your passwords. PC Magazine states that a password like “123456” or “monkey,” although easy to remember, is also easy to crack. At a conference last year, financial advisers were asked for passwords when they entered a meeting room. A computer program was able to quickly crack the passwords. Do not reuse a password. You might have a password that was compromised and when you use it later, the hackers already have that information.

Some of you may be able to remember all of your passwords, but most cannot.

Consider using a password manager. This is a service that stores all of your passwords. With the help of a password manager, you can have a unique and strong password for every secure website you use. To get information about password managers, Google “the best password managers of 2017” and look for PC Mag.com. Evaluate which password manager best suits your needs.

The best gift you can give yourself this year and every year is to protect your identity and your money.

I don’t know about you, but I could certainly use a little eggnog after thinking about this topic. Once you’ve done all the things necessary to protect your information, sit back, relax and enjoy the holidays.

I hope each of you has a Merry Christmas or a Happy Hanukkah.

May 2018 be a year of health, happiness and prosperity.

Fred Dunbar, CLU, ChFC, RFC, AIF,® is President of Planning Directions, Inc., a registered investment adviser, and Common Cents Planning, Inc. He is also a registered representative of and offers securities through Commonwealth Financial Network, member FINRA/SIPC. Advisory services offered through Planning Directions, and fixed insurance products and services offered by Common Cents Planning, are separate and unrelated to Commonwealth. Fred may be contacted at 800-647-0762, by e-mail at fdunbar@commoncentsplanning.com or by mail at 239 Baltimore Pike, Glen Mills, PA, 19342.