MALLARD Money Matters

October 2017

NOTICES

Paul will be attending a financial planning conference in Orlando, October 18 - 20. He will attend a government conference in Las Vegas, December 13 - 15. He will be in legislative session in Dover Tuesday through Thursday afternoons, January 9 - 25, 2018.

Ed will be out of the office October 16 - 19. He will be on vacation in North Myrtle Beach, November 6 - 20.

Pam will be on vacation December 13-15.

Jacqie will be out of the office January 2-31, 2018 for class in Cambridge, MA.

Mallard will be closed November 23 and 24.

Mallard will also be closed December 25 2017 and January 1, 2018.

MALLARD
Financial Partners INC

750 Barksdale Road
Suite 3
Newark, DE 19711
302.737.4546

www.mallardfinancial.com

Protecting our digital selves after the Equifax Breach — Ed Mink

Like it or not, we live in a digital world, and it is rapidly becoming more digital, not less. As with other transitions, it comes with growing pains and exposures, such as the recent Equifax debacle. How could we, as mere victims of the system, have avoided the exposure of our data to those people who were intent on obtaining it? Apparently, we couldn't (at least not if we didn't go "off-the-grid" many years ago), but we can't change the past.

What can/should we do in the future? We must take all reasonable steps to guard our information and monitor our credit reports. Here are some concrete steps that we should consider taking:

Determine if you are affected. Go to www.equifaxsecurity2017.com and enter your last name and partial Social Security number to find out if Equifax believes you are one of the people affected by the hack.

Consider freezing your credit. After doing this, no one can make inquiries about your credit history or open a new credit card (or other account) in your name. *That includes you* -- unless you lift the freeze when you are applying for a new credit card, account or loan — or by using a PIN that should be provided to you when you initiate the freeze. *If you decide to freeze your credit, you need to do so with **each** of the three credit bureaus*, and can do so by going to:

https://www.experian.com/freeze/center.html

https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

https://www.transunion.com/credit-freeze/place-credit-freeze

Or, you can call Equifax (1-800-349-9960), Experian (1-888-397-3742) and TransUnion (1-888-909-8872). The credit bureaus may charge $5 or $10 to freeze your credit.

Sign up for credit monitoring (as an alternative to freezing your credit). Equifax is offering all those affected *one year of free credit monitoring*, which would let you know when activity occurs on your credit history, such as the opening of a new account or credit card. While there have been questions, Equifax is publicly representing that "enrolling in the free credit file monitoring and identity theft protection that we are offering as part of this cybersecurity incident does not waive any rights to take legal action." There are other credit monitoring services commercially available if you don't want to use the one offered by Equifax.

Monitor your credit history yourself. Anyone can check their own credit history at www.annualcreditreport.com, which is required to be offered by the federal government. You are able to get a **free check** with each of the three bureaus once a year. Some people choose to check on a rotating basis, checking with a different bureau every four months. Watch for accounts or loans or other activity that you did not initiate.

File your taxes early. One of the things identity thieves may do is use your information to file a false tax return in an attempt to obtain a refund. For people whose personal information may have been stolen, it is recommended to *file your tax return as soon as possible in the tax season* after receiving all the required tax information, to reduce the length of time that identity thieves might have to file using your information.

Regardless of whether or not you were affected by the recent Equifax breach, it is important to get in the habit of taking measures to protect your identity. It is not a matter of *if* your information will be compromised, but *when*. Here are some best practices to help keep the criminals at bay.

Guard your information:

- Refrain from providing businesses with your Social Security number just because they ask for it. (Medicare recipients should be careful, because Social Security numbers are printed on Medicare cards.)
- Don't provide personal information over the phone, through regular mail or via Internet *unless you have initiated the contact* or *you know with whom you are dealing*. This is especially important to communicate to older relatives or friends, who are prime targets of fraudsters.

  Beware of over-sharing on social media, where criminals are finding treasure troves of information. Because criminals are explicitly targeting children under the age of 18, parents need to talk to their kids and explain why it's so dangerous to share too much information.

Protect your Password: Change logins and passwords monthly, use password generators and sign up for two-factor authentication services.

Shop carefully: Don't send financial information on unsecured wireless networks and when making purchases, use a credit card, which has more fraud protections under federal law than debit cards or online payment services.

Review credit card statements: Before you pay, make sure that there are no fraudulent charges. While you're at it, enroll in a credit card notification program, where the credit card company alerts you about charges over a preset amount.

Review your (and your children's) credit report every 12 months at www.annualcreditreport.com. If you find an error, report it immediately and stay on top of the process.

You may also want to consider subscribing to an identity theft protection service. Generally, for about $10/month to about $30/month, at least 18 different Identity Theft Protection companies (such as *Lifelock* and *Identity Guard)* will monitor your tri-bureau credit reports, alert you if they detect a threat to your identity, and provide Identity Theft insurance (with coverage of up to $1 million). Each company typically offers several packages/options that provide varying levels of service, along with varying prices for those services. One service, civic.com, offers a basic level of protection for free.

Here are some signs that your identity may have been stolen:

- Credit card is declined.
- Drop in your credit score.
- Sudden increase in account balance.
- Unauthorized credit report inquiries.
- Reports of a new account that you did not open.
- Call from a debt collector.

Protecting our digital selves after the Equifax Breach — Ed Mink

Should you be worried?

Unfortunately, we have very little control over the actions of others. I think that the Dalai Lama was channeling that sentiment when he said, "Don't Let Behavior of Others Destroy Your Inner Peace."

Hopefully, we have been relatively cautious in the past, and will continue to be so. This is not a time to fret over what has happened, but rather a time to ask ourselves what, if anything, we should do differently going forward.

Like avoiding crime in general, protecting yourself against identity theft involves a series of precautions, none of which are completely foolproof but together give you a better chance of not being a victim. You need layers of protection. Be sure to visit only trusted, secure websites, especially for transactions involving your credit or bank account numbers. Make sure your passwords are strong and changed often. Shred your personal financial documents before throwing them away.

What is "Smishing"? — Ed Mink

On a related relatively recent identity theft issue, here's what Kate Murphy wrote for Yahoo News about the recent trend of "smishing."

Most people are probably aware of the fraud term phishing. It refers to emails that are meant to lure users to surrender personal information by purporting to be from the government, a bank, or a reputable company. The end game is to steal someone's identity. Scammers are targeting people via text messages. It's called smishing, a combination of the terms *SMS text messaging* and *phishing*. According to a study by Cloudmark, the number of spam text messages designed to defraud people is seven times that of email spam. Research also suggests that cellphone users are three times more likely than computer users to respond to spam.

Here are some smishing examples to watch out for:

- "IRS Notice: Tax Return File Overdue! Click here to enter your information to prevent being prosecuted."
- "We have identified some unusual activity on your online banking. Please log in via [URL] to secure your account."
- "Your entry last month has WON. Congratulations! Go to [URL] and enter your winning code to claim your $1,000 Best Buy gift card!"

Here are some tips to help with your smishing self-defense:

- Don't call the number or reply to texts asking for personal or financial information.
- Be aware that banks and legitimate companies don't send unsolicited texts, and government agencies don't contact people through text messages.
- Ignore instructions to text "STOP" or "NO," because this will let scammers know your phone number is active.

You can forward smishing texts to 7726, which spells out the word SPAM, on most keypads. This will alert your cellphone carrier to block future texts. And when in doubt, just delete the text message.

MALLARD
Financial Partners INC

750 Barksdale Road, Suite 3
Newark, DE 19711-3245

Working together, building your financial security

Compliance Corner

Pam Baumbach

All firms and individuals selling securities or offering investment advice, by law, must be registered with the SEC. FINRA maintains a tool for these firms and individuals to be researched called BrokerCheck (https://brokercheck.finra.org/). This tool allows the consumer to do due diligence on a firm or advisor, or it can be used to 'vet' an advisor for services sought by the consumer. BrokerCheck makes it possible for the consumer to find advisors and brokers with clean regulatory records.

On BrokerCheck, you can determine whether a firm or individual is properly registered, and also see their employment history, licensing information, regulatory actions, arbitration, rulings, and complaints.

Mallard has the BrokerCheck link on its website, www.mallardfinancial.com.

Mallard is pleased to announce that Joe Daigle and Kenny Beach, of our investment team, have recently completed the requirements of an Investment Advisor Representative and are now registered with the SEC.

Paul Baumbach, Susan Lehnerd, and Ed Mink have been registered Investment Adviser Representatives with Mallard Financial Partners since 2014. This is the year Mallard Financial Partners transitioned from Mallard Advisors. They each had been previously registered with Mallard Advisors.

News and Events

Mallard will be closed:

Thursday, November 23

Friday, November 24

Monday, December 25

Monday, January 1, 2018