YANKE FINANCIAL

3737 Glenwood Ave, Ste 100 | Raleigh, NC 27612
919-573-1816 | Toll-Free: 800-513-2812 | Fax: 919-573-1817
patrick.yanke@yankefinancial.com
www.yankefinancial.com

Patrick H. Yanke, CFP®
Branch Manager

September 19, 2017

This is a Very Big Deal

The Equifax Hack and What it Means to You

On September 7, 2017, Equifax (one of the three largest American credit agencies) announced a cybersecurity incident involving consumer information. The information includes Social Security number, birth dates, addresses, and a whole lot more you may have forgotten they know about you. In addition, credit card numbers for approximately 209,000 US consumers and certain dispute documents with personally identifiable information (PII) for approximately 182,000 US consumers were accessed. The potential for fraud and identity theft is significant.

Determine if You Were Impacted

Equifax has created a site to assist us in determining if our PII was compromised in the breach. If your information has been compromised, you will have the ability to sign up for credit-monitoring and identity theft protection free of charge through this site. You have to provide your full legal name and the last six digits of your Social Security number. Even in this situation, they still have to identify you first.

Go to https://www.equifaxsecurity2017.com, click on the "Potential Impact" link and enter your information. You will receive a message indicating whether your personal information may have been impacted by this incident. Equifax is offering its free identity theft protection and credit file monitoring to all US consumers through Tuesday, November 21, 2017.

I recommend freezing your credit file. This creates some additional hoops when you want to apply for financing but it also puts roadblocks in the way of thieves. The credit agencies tend to be resistant to credit freezes but you can make this happen. Why are they resistant, especially in the face of this monstrous data breach? The reason they don't like credit freezes is fairly simple... follow the money. We are not their customers. We are their product. Their customers are those who buy our information from them. Credit freezes work against their profitability model.

Monitor Your Finances

If you or a loved one's PII has been compromised, you might not see an immediate reaction. Be sure to monitor all financial accounts for unauthorized transactions or activity. If activity is identified, time is key if returns, recalls or reimbursements are warranted. The sooner activity is identified, the better. This will require long-term vigilance.

Here's where the real risk lies. When you set up an account through the credit agencies, you are asked questions like "what is your mother's maiden name?", "where did you live in 1985?", or "which one of the following is an old address?" That is the type of information they use to verify your identity--so that type of information is at risk. When you call to set up online financial services, you will encounter the same types of questions. This information is also used to identify you when you forget passwords. The potentials from this data breach are far-reaching and go beyond only financial considerations.

Who Can You Trust?

In an age of automation, we are all at considerable risk in these situations. Anyone can call an 800 number or go to a website and either set up accounts in our names or take over existing accounts. A faceless, voicemail world has no other way to identify us than the very information compromised in this data breach. Get around the machines and talk to people.

There are many reasons my clients enjoy a personal relationship with me. In getting to know my clients, I get to know how to serve them best. In situations involving ID theft or fraud, that personal relationship makes me their first line of defense. Anyone can call the home office about their account at any time. The home office will do their best to identify the caller and take instructions. Then, the home office notifies me. My next action is to call my client to confirm the instruction. If the action is fraudulent, it stops right there. Has this happened before? Yes.

A personal relationship can solve a lot of problems before they start. Make sure you know who is watching out for you and make sure they know you. **Set up fraud alerts at all financial institutions.** Like the credit freeze, this will require the institution to go through additional steps to protect you.

Fraud Prevention

While financial firms like Raymond James employ the most up-to-date safeguards to protect client account numbers and other important personal information, clients also have a very important role to play. Now, and always, here are some ways to minimize the exposure to fraud and ID theft:

- Protect passwords, PINs, and answers to security questions by not sharing them with anyone you don't want to have access to your accounts. Avoid easily guessed

MY BUSINESS PHILOSOPHY

Do unto others as I'd have them do unto me. I don't like to pay people just to have a conversation with them. Let me do a confidential financial review for you. There is no obligation.

ONLINE RESOURCES

My webpage has a wealth of resources and calculators for the online investor. Go to www.yankefinancial.com. Clients can also access their accounts for statements and tax forms.

Continued from the front:

passwords (e.g. family members' names, birthdates, Social Security numbers, etc).

- Keep firewalls and security software up to date and use encryption software, where able.
- Use your personal computer for financial transactions and avoid using public-use computers, if at all possible.
- Do not give our vital information over the phone, by email, or through in-person requests. Type in the URL of a website you want rather than clicking on a link in an email.
- Check financial accounts regularly to ensure no unauthorized activity is taking place. Contact credit card companies or financial institutions immediately if suspicious activity is suspected.
- Monitor email, social media, and online financial accounts for unauthorized changes. If an email comes into the inbox claiming a change has been made to an account that you did not authorize, do not click on the links provided in the email. Contact your service provider directly to confirm the change and follow their instructions to protect accounts.
- Only click on links or open attachments you expect and are from trusted and known sources. Even if an email is from a known party, if it looks suspicious, play it safe and confirm with the sender before opening.

What to do When ID Theft is Feared

As the radio commercial says, "no one can prevent all ID theft." It's true. Even if you never go online or sign up for account access, your information is still available from government sources, credit agencies, medical authorities, financial institutions, and others. A data breach of one of these sources (like the current one) puts you at risk through no fault of your own. So what should you do?

I recommend having some form of ID Theft insurance. The most well-known is Lifelock but there are others--like the program offered at Zander Insurance. Lifelock's main program is to minimize exposure through credit alerts in the credit agencies. However, since ID theft is still a threat despite the alerts, the real benefit of any ID Theft insurance is the promise to help rebuild after ID theft has occurred. This is an expensive and time-consuming process that is best shared with competent agencies.

I do not sell ID Theft insurance, nor do I or Raymond James have any affiliation with anyone selling this type of insurance coverage. I simply believe it is a necessity in the modern age. Personally, we have had ID Theft insurance for many years and that gives me a certain amount of peace when I hear of major data breaches beyond my control.

Be Proactive

The one thing we should not due in this situation is nothing. We know the data breach occurred and we know it is far-reaching. Change passwords everywhere, set up fraud alerts on accounts, update firewalls and security software, be vigilant with your personal information, and consider ID Theft insurance to help recover after problems occur. Seek a personal relationship with those providing services to you.

For more information on ID Theft, please read my special report on my website. ID Theft is not just a financial problem. Our identities are important in nearly all aspects of modern life and valuable to those who would exploit us. Arm yourself with knowledge as your first defense. I am ready to answer questions at any time.