Financial Planning Newsletter

Fall 2017

Financial Advisors, Inc.

Inside This Issue:

Equifax Data Breach

Although we sent an email to all of our clients describing steps to take immediately following the Equifax Data breach announcement, additional information about the breach and steps to take continue to evolve. We encourage you get in touch with us if you have any questions or concerns about how to protect your identity and credit after this breach.

Please understand this breach reportedly involved social security numbers, driver's license numbers, birthdates, addresses and information about existing credit. As such, this breach will require each of us to maintain vigilance for years to come. The cyber attackers who stole this data could wait for a year or two to let this breach settle before they start using the information they stole.

While initially we were concerned about the free credit monitoring Equifax offered, Equifax quickly removed the language preventing you from participating in future class action suits. As a result, we now believe you can accept their one-year free credit monitoring service. While credit monitoring for one year seems like a good start, it is likely to be insufficient and you should strongly consider extending a credit monitoring service. Equifax may extend their offer beyond one year though there are many other options available for this service. AAA members have access to credit monitoring with their membership. LifeLock is another example of an independent company offering credit monitoring. There are also many other services.

Continued on Page 2

Cybersecurity Project

In December 2016, Karla and Katie began a project to review the status of cybersecurity readiness at our firm and we committed to cover some of these important topics in each newsletter this year. In the last newsletter, we reviewed protecting your money and limiting what you share online. In this edition, we discuss the last two topics in our cybersecurity circle: safeguarding email accounts and keeping your technology up to date.

Safeguard Email Accounts

DO

- Exercise caution when reviewing unsolicited email.
- Obtain secure storage programs to archive sensitive, private data and documents instead of storing emails. Examples of secure storage are Box, Dropbox, Sharefile, iCloud, etc.

Continued on Page 4

Navigating a Homeowner's Insurance Claim

Suppose you're the victim of a huge natural disaster like Hurricane Harvey, or have experienced some more local damage, like a tree falling on your house. What are the best practices for filing a claim for the damages your home and property have suffered?

Recently, the Consumer Federation of America offered tips on how to get all you're entitled to from your insurance company.

The organization starts by noting a disturbing trend: families victimized by Harvey-related wind and flood damage will have to dig deeper into their pockets. Few of today's homeowners have federal flood insurance, and insurers have been steadily increasing hurricane wind coverage deductibles, as well as imposing other homeowner's insurance policy limitations.

Among the tips: Report your claim as promptly as possible, since insurance companies generally handle them on a first come, first serve basis. Be sure to write down your claim number, since insurance company claims departments can locate your file most promptly using your claim number.

Meanwhile, maintain receipts for any expenditures related to immediate repairs necessary to secure your home, and any living expenses incurred (hotel, meals) if you could not return to your home in the wake of the storm or as a result of your own home

Continued on Page 3

Equifax Data Breach(continued)

In addition to credit monitoring, we do believe you should also consider these additional steps to help protect your identity and credit information.

- Consider placing a freeze on your credit. A credit freeze blocks anyone from opening credit in your name. A freeze MUST BE PLACED AT EACH CREDIT AGENCY in order to be effective. The freeze will also block you from opening credit which can be a bit of a hassle, but know that you can "unfreeze" your credit to access new credit at any time, then put the freeze back on. Each of the three large credit agencies (Experian, TransUnion, and Equifax) currently charge a small fee to freeze your credit. To set up a freeze, please call each of the 3 credit agencies and request they freeze you credit. Their phone numbers are: ***Experian*** - 888-397-3742 ***TransUnion***—888-909-8872 ***Equifax*** - 800-349-9960.
- Be vigilant about reviewing your bank, credit card and brokerage statements. If you spot or suspect any unusual activity, alert the bank or brokerage immediately.
- Consider setting up an online account to view your Social Security statement. If you are currently receiving Social Security, you may have created this account previously. If you are not receiving benefits, you may need to establish an online account for the first time. To establish an account, go to www.socialsecurity.gov/myaccount. Select "Sign in or Create an Account" and follow the steps for creating a new account. Setting up an account serves two purposes: it prevents someone else from opening an account with your social security number and trying to claim benefits on your record, and it allows you to review the information on your Social Security statement for accuracy.
- Be aware of tax fraud. With your Social Security number, a fraudster can file a tax return in your name and request a refund. This crime had been escalating in recent years and is certainly feasible with the data obtained in this breach. If you have a problem with a fraudulent filing at the IRS, please call them at 1-800-908-4490.
- Be very careful with unsolicited emails. We have already seen a few instances where a person has received an email from someone claiming to be ready to help them with this data breach. The email sender provides a fraudulent link in the email as they try to steal more of your personal and private information. Always be extremely cautious of unsolicited emails that contain links.
- If you discover that someone has been using your information fraudulently, contact the police and the Federal Trade Commission (FTC). The FTC can be reached at identitytheft.gov. In addition to reporting the incident, they provide a number of resources to help you recover from your stolen identity. If you would prefer to call, the FTC phone number is 1-877-438-4338.

We understand that this data breach has been very upsetting. Please know that we will continue to help you however we can. We will also continue to work with Schwab and TD Ameritrade to help guard our clients' accounts against fraud now and in the future. If you would like any help or guidance, please call us.

Homeowner's Claim (continued)

damage experience. (If your claim is limited to flood insurance, additional living expenses are not covered.)

When an adjuster arrives to survey your damage, ask if he/she is an employee of the insurance company or an independent adjuster (I.A.) hired by that firm. If this person is an independent adjuster, ask if he or she is authorized to make claim decisions and payments on behalf of your insurance company, and ask for the name of the in-house company adjuster to whom the I.A. is sending your information.

Many insurance companies will send out one of their approved contractors to estimate your property damage. You are not under any obligation to use them, and you should realize that these approved contractors have likely agreed to limit repair costs based on average cost estimates in the area. You might benefit from getting an estimate from other local contractors, since your damage situation will be unique.

Before you file a claim, know that it helps to have pictures of your possessions, which you can file as evidence of what you're claiming. Make as thorough a list of your possessions as you can. When the claim is made, start a notebook documenting contacts with your insurance company, writing down the date, time and a brief description of every exchange.

Suppose the claim is denied, or you feel the offer is too low. At that point, you should ask the company to identify the language in your homeowners' policy that served as the basis for denying your claim or offering so little. Once the company pinpoints the appropriate language in the policy, you should be able to determine the fairness of the offer. If you feel that the company has slipped new limitations into the policy and not adequately informed you, it might be a good idea to consult an attorney.

For those not living through Harvey, this might be a good time to look hard at your current policy. The Consumer Federation of America has noticed that new provisions are showing up which limit replacement cost payments, and many insurers no longer cover the additional costs to bring a damaged home up to new building codes (wiring, elevation for flood risk, etc.).

Once the insurance company tells you the reasons for its action, it cannot produce new reasons for denying payment or making a low offer at a later time. You have locked them in an important protection for the consumer.

If you feel that the offer is too low or the claim denial is wrong, complain to an executive in the firm's consumer relations (who is paid to keep consumers happy) rather than an executive in the claims department (who is paid to keep claims costs low). In the conversation, use the records you've kept since the claim process began. The more serious the insurance company sees that you are in documenting how you were treated, the more likely they will make a more reasonable offer.

If that doesn't get you anywhere, complain to your state insurance department. All states will at least seek a response to your complaint from your company, which will give you more information as you consider your next steps.

Your last option is to consult a lawyer. If you're sitting in the attorney's office, the notes you took take on additional importance. If your treatment was particularly bad, the courts in many states will allow additional compensation when the insurance company acted in "bad faith." Since insurance companies take your money in exchange for their promise to make you whole when disaster strikes, they must act in utmost good faith in performing that obligation.

Article by Bob Veres

Source: http://consumerfed.org/press_release/consumers-get-fair-claims-payments-wake-hurricane-harvey/

FINANCIAL ADVISORS, INC.

3685 Mt. Diablo Blvd.
Suite 200
Lafayette, CA 94549

Phone
925-299-1800

Fax
925-299-1812

E-mail
info@hcfinancial.com

Helping You Successfully Navigate Your Unique Financial Life

If you no longer wish to receive our newsletter, please send us an email at info@hcfinancial.com

About HC Financial Advisors, Inc.

HC Financial Advisors, Inc. is a fee-only registered investment advisory firm offering full financial management services to individuals and their families. We offer ongoing investment management and financial planning services for an annual fee based on assets managed.

Our current minimum annual fee is $10,000 ($1,000,000 under management). This fee includes the investment management of all assets as well as our comprehensive financial planning services.

We welcome your referrals to our firm. There is no charge for a preliminary, one hour informational meeting to learn more about our services, investment philosophy, and backgrounds. You can also find us at our website www.hcfinancial.com.

Cybersecurity (continued)

DO (continued from page 1)

- Create separate email accounts specifically for financial transactions.
- Delete all emails that include financial information.
- Do not provide or send financial information via unsecured email.
- Be very selective about the information you choose to share on social media.

DO NOT

- Click on the links or pop-up ads in unsolicited emails as these links may pass on a virus.

Keep Technology Up to Date

DO

- Install the most up-to-date antivirus and anti-spyware software on all devices that connect to the Internet (e.g. PCs, laptops, tablets and smartphones). Top anti-virus/spyware products would include McAfee Anti-virus, Symantec/Norton, Avast and many others.
- Set each device to run regular scans to update software.
- Ensure you've installed the latest version of your software and your patches are up to date.
- Make sure your networking equipment and computers are all still supported by the manufacturer.
- Recycle, exchange or dispose of your old mobile device safely by:
  - ⇒ Backing up your data
  - ⇒ Performing a secure erase (factory reset) or have the device vendor wipe your device
  - ⇒ Shred your old computer's hard drive. There's a service provided by Automatic Response Systems in Berkeley (berkeleyshreds.com), that will physically shred each hard drive for $12.
  - ⇒ Remove SIM and SD cards from your cell phone and destroy or transfer to new phone.

DO NOT

- Purchase any networking devices secondhand.
- Forget to set up a passcode or PIN and auto-lock on your mobile devices.
- Use free or found USB devices as they are often infected with malware.

If you ever suspect suspicious activity with any of your financial accounts, we encourage you to call us immediately. We put a high priority on keeping your accounts safe and free from cyberattacks.