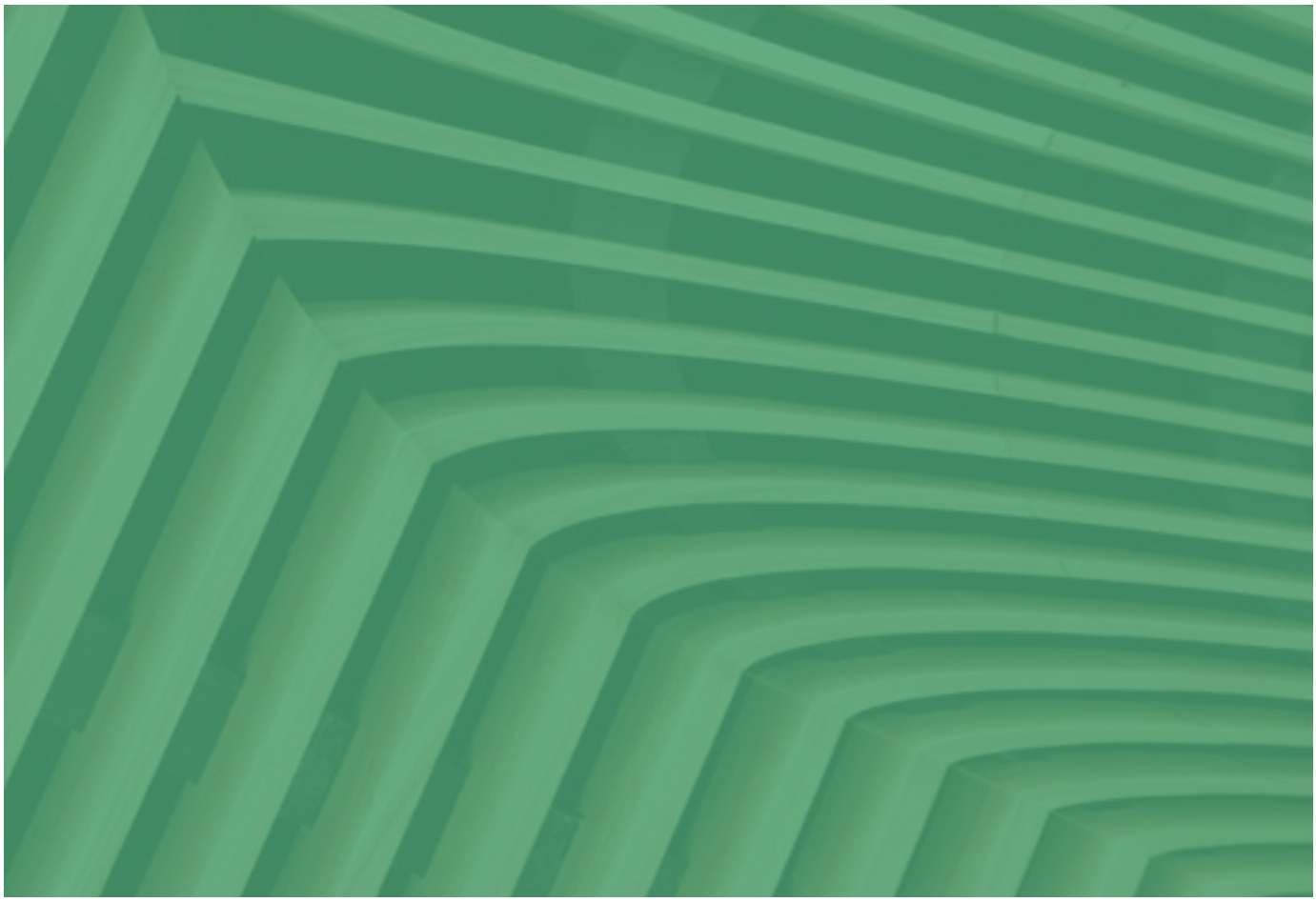
CEDAR HILL

WEALTH
MANAGEMENT

NOVEMBER 2017

CYBER SAFETY AND FRAUD AVOIDANCE: A PROACTIVE APPROACH IS KEY



AS OUR WORLD BECOMES INCREASINGLY INTERCONNECTED THROUGH TECHNOLOGY, WE RECOGNIZE THE IMPORTANCE OF PRIVACY AND VIGILANCE. IN RECENT MONTHS, WE HAVE SEEN AN INCREASE IN FRAUD AND CYBERSECURITY ATTACKS ON BOTH INDIVIDUALS AND BUSINESSES. WE WANT TO ASSURE OUR CLIENTS AND STRATEGIC PARTNERS THAT POLICIES AND PROCEDURES ARE IN PLACE TO DEFEND AGAINST FRAUD.

CEDAR HILL TAKES A PROACTIVE APPROACH TO SAFEGUARD CLIENT DATA AND PERSONAL INFORMATION. THE FOLLOWING WHITE PAPER PROVIDES INFORMATION ON STEPS YOU CAN TAKE TO PROTECT YOURSELF FROM IDENTITY THEFT, AS WELL AS THINGS YOU CAN DO TO AVOID ONLINE, PHONE, CHARITY AND TAX SCAMS.

ASHA T. GOLDSTEIN, CFP®
MANAGING DIRECTOR

CYBER SAFETY

At Cedar Hill, our policies are in full force for safeguarding client data and identities. We are vigilant with regard to requests that are out of the ordinary, and we have “red flag” procedures in place to defend against fraud. Bottom line - we take data privacy and security very seriously, and protect client information as we would protect our own.

From a technology perspective, the Cedar Hill network is designed to contain the workspace in a single environment which is heavily protected with various layers of security. Our email system has its own safeguards keeping all confidential business correspondence secure. Our network is monitored 24/7, and the system is regularly updated to protect against security attacks.

Unfortunately, there are many different tactics and clever schemes crooks use to defraud millions of people every year. In addition to hackers, identity theft and fake IRS communication, the FCC (Federal Communications Commission) is also warning consumers about new phone scams.

The technique involves a robocall or an actual person who calls consumers and asks: “Can you hear me?” The consumer responds, “Yes” thus providing the scammers a recorded voice signature. Subsequently, the voice signature can be used by the scammers to authorize fraudulent charges via telephone. A one-word response is all it takes.

The following is a friendly reminder of things you can do to avoid fraud.

IDENTITY THEFT

Review your credit reports for free by visiting www.annualcreditreport.com. Federal law requires that each of the three major credit bureaus provide you a free credit report each year. You can spread out your requests by getting one free report every four months if you want to monitor your credit throughout the year.

While no service can protect you from having your personal information stolen, there are monitoring and recovery services to which you can subscribe. Often sold together, monitoring services watch for signs that someone may be using your personal information, while recovery services help you deal with the effects of identity theft after it happens.

Credit Karma (www.creditkarma.com) is a free online resource which provides your current credit score, as well as free credit monitoring through Equifax and TransUnion. With this service, if unusual activity is suspected, you will be alerted. Following the Equifax breach, CreditKarma announced they will launch a new free ID monitoring service that will keep track of data breaches and will let you know if you are potentially a victim.

There are several other subscription-based credit monitoring services that charge a monthly or annual fee - usually following a 30- or 60-day free trial. We encourage you to do your due diligence, as most of these services are essentially the same but repackaged by different companies. For additional information, a list of credit monitoring resources is provided at the end of this article.

Another option, and the most restrictive path, is to place a credit freeze with each of the bureaus. A credit freeze largely stops all access to your credit report and makes it difficult for anyone (including you) to open accounts using your personal information.

Depending on your state of residence, there is likely a nominal fee to place or lift a credit freeze. Additionally, each credit reporting company will send you a confirmation email or letter containing a PIN or password that you will need in order to lift the freeze.

Don’t forget your kids! A child’s social security number can be used by identity thieves to open bank and credit card accounts, to apply for government benefits, or even rent a place to live. A strong preventative measure would be to place a freeze on your child’s credit report until they are of age to establish credit. The credit bureaus will not allow you to place a freeze for a minor online, but there are manual steps you can take.

To see if your minor children have credit reports, TransUnion will do a search for free: https://www.transunion.com/credit-disputes/child-identity-theft-inquiry-form

If you think you’ve been a victim of identity theft, visit the Federal Trade Commission www.identitytheft.gov for advice and resources.

To place a freeze on your account, contact one of the nationwide credit bureaus listed under *Additional Resources and Information* at the end of this article.

CYBER SAFETY

PHONE SCAMS

If you answer the phone and hear a recorded sales pitch, please hang up! The products are often phony and these calls are illegal. Do NOT press 1 to speak to a person or to be taken off the list as it could lead to more calls. Hang up on robocalls, and report your experience to the Federal Trade Commission (FTC) online at https://www.ftccomplaintassistant.gov or by calling *1-888-382-1222*.

Place your cell phone and home phone on the Do Not Call Registry. There is only one Do Not Call Registry operated by the FTC; there is not a separate registry for cell phones. You can register online at www.donotcall.gov. Note that you will have to respond to a confirmation email in order to activate your registration.

To register by telephone, call *1-888-382-1222 (TTY: 1-866-290-4236)*. You must call from the phone number that you want to register.

ONLINE SECURITY

The single best thing you can do to protect yourself online is use complex passwords and change them often. Use a phrase of at least 10-12 characters and do not use names, dates, or common words. Add numbers, symbols, and capital letters into the middle of your password rather than at the beginning or end.

Security experts highly recommended using a password manager. A password manager is software that, among other things, generates and stores all your password information, including PINs, and security question answers.

Several password managers offer a free subscription. A list of these service providers can be found in the Password Management section under *Additional Resources and Information* found at the end of this article.

Many online services offer “two-factor authentication” where getting into your account requires a password plus an additional piece of information. The second piece could be a code sent to your phone by text, or a random number generated by an app or separate token. This authentication process protects your account even if your password is compromised. We recommend instituting two-factor authentication whenever possible.

Another popular scam involves bait emails coming from illegitimate senders. These types of emails often include some kind of sad story or promise of compensation. If you get an email asking you to send money to aid a stranger or for any reason - delete it!

Phishing occurs when scammers use copycat websites or false emails or texts in the hopes of getting you to share valuable personal information. Rather than clicking from links within an email, look up websites and phone numbers yourself through a search engine. Forward misleading or deceptive messages to *spam@uce.gov* to report it to the Federal Trade Commission.

CHARITY SCAMS

From hurricanes and natural disasters to terrorism and crime victims, fraudsters inevitably swarm to take advantage of highly publicized tragedies. If you’re thinking about giving money to support those in need, do your research.

A list of websites can be found under the *Additional Resources and Information* section at the end of this white paper. These organizations have vetted charities and can provide a list of ones that are raising funds for a specific cause.

TAX SCAMS

Tax scams have been a mounting issue over the last few years. File your taxes early to keep scammers from claiming your refund. The IRS will not initiate contact with you via email or text message. If you receive emails claiming to be from the IRS, do not reply or click on any links. Instead, forward them to *phishing@irs.gov*. Contact the IRS immediately if you think someone filed for a tax refund using your social security number or if the IRS sends you a notice indicating a problem. Specialists will work with you to get your tax situation resolved.

Internal Revenue Service:
Call *1-800-908-4490*

IRS Identity Protection Specialized Unit:
https://www.irs.gov/identity-theft-fraud-scams/identity-protection

CYBER SAFETY

CONCLUSION

We've merely skimmed the surface here. Technology gives you access to the world, but unfortunately, it also gives the world access to you. While putting preventative measures in place will cost you time, effort and in some cases money, choosing to do nothing can ultimately cost a lot more.

At Cedar Hill, we take pride in our personal approach to each client's unique circumstances. If you have questions or concerns, please feel free to reach out to a member of the Cedar Hill team and let us know how we can help.

ADDITIONAL RESOURCES AND INFORMATION

IDENTITY THEFT

Identity Guard
https://www.identityguard.com

FreeScoresAndMore
https://www.freescoresandmore.com

Privacy Guard
https://www.privacyguard.com

LifeLock
https://www.lifelock.com

CREDIT MONITORING

Equifax
1-800-349-9960 or
https://www.freeze.equifax.com

Experian
1-888-397-3742 or
https://www.experian.com/freeze/center.html

TransUnion
1-888-909-8872 or
https://www.transunion.com/freeze

PASSWORD MANAGEMENT

LastPass
https://www.lastpass.com/

Password Boss
https://www.passwordboss.com/

LogMeOnce
https://www.logmeonce.com/

Dashlane
https://www.dashlane.com/

CHARITY VERIFICATION

Better Business Bureau's (BBB)
Wise Giving Alliance
http://www.bbb.org/charity

Charity Navigator
http://www.charitynavigator.org/

Charity Watch
https://www.charitywatch.org/

GuideStar
http://www.guidestar.org/

CEDAR HILL
WEALTH
MANAGEMENT

Cedar Hill Associates, LLC
120 N. LaSalle, 33rd Flr.
Chicago, IL 60602
www.cedhill.com

An affiliate of MB Financial Bank, N.A.

WPCYB_111017