Introduction: Welcome to the Paragon Financial Partners podcast where we discuss the markets, our strategies, and how to live better today while planning for tomorrow.

Elean Mendoza: Hello, and welcome to the Paragon podcast. I'm Elean Mendoza and I'm here with Evan Shorten, the firm's founder and principal.

Evan Shorten: Hello. I'm Evan Shorten and I want to thank you for turning in to another episode of the Paragon podcast. If you enjoy this episode or the information we provide, please subscribe to our podcasts via iTunes or Stitcher Radio.

Elean: In this episode we want to discuss some examples of financial fraud or abuse that we have personally encountered or have seen happen to our clients. We think it's important to discuss this topic and to provide you with some tips on how to better protect yourself. Additionally, we have included a Cyber Security checklist you can download using the link in the description below or by visiting our blog at paragonfinancialpartners.com/blog. With that, Evan do you want to start off this discussion by telling our listeners about an experience one of our clients had in their assisted senior living facility?

Evan: Yes, of course. In 2014, one of our clients felt her retirement community was pressuring her to make large donations to the facility. As it turns out, the community helps prepare its residents tax returns ultimately giving them access to the residents' intimate financial details. Now to be clear, we are not trying to cast a negative view of senior residences or retirement communities helping their residents by providing basic help with their finances, but it's okay to maintain a healthy level of skepticism when it comes to your personal finances.

Surely, after the retirement community helped prepare our client's tax return, she felt the community and its employees began pushing the idea of making large donations for facility improvements. While no single person outright asked her, she did feel a new amount of pressure being added. Fortunately, we maintain a close relationship with all our clients and she came to use discussing her feelings. From that point, we spoke to the retirement community directors through various methods of communications, ensuring our client's concern and ours were being addressed. After that the issue was put to rest and our client's concerns abated.

Elean: That goes to show you how important it is to have an advocate on your side you can trust.

Evan: Exactly. One of the best ways to reduce your chances of becoming a victim of financial abuse or fraud is to speak openly about your service providers, caretakers and living conditions with those you trust.

Elean: Now, recently Evan you and I both personally experienced phishing attempts regarding our personal information. For our listeners, phishing, which is actually spelled P-H-I-S-H-I-N-G, is the attempt to obtain your personal and sensitive information by posing as a legitimate company or entity.

Evan: Yes. A few weeks ago, I received a call supposedly from the IRS. I had supposedly won a business grant to help expand my practice through a new government program. When I began to press the caller about

the program specifics, why I had never heard about it before, the caller's name and identification, they began to get frustrated with me and insisting that I provide my business' information just to get the process started.

Ultimately, the caller got frustrated with my refusal to provide them my information, swore at me, and hung up. It's very important to understand that if you receive a call from the IRS, the Franchise Tax Board, or most government agencies, it's typically a follow-up call from something you have already submitted to them. These agencies, the IRS, the Franchise Tax Board, will not be calling you as a first contact. Something will always be coming in the mail. These supposed representatives will be providing you with some information and if it is a legitimate person from an agency, after there is some follow-up, they will provide you with their full name, where they're calling from, and some type of agent ID that is unique to them. If the person calling you is unwilling to provide this information, hang up and just don't waste your time. If they do provide you with their credentials, consider putting the conversation on hold and calling back from another phone line. This allows you to verify that an agent of the organization or institution is indeed calling you.

Elean: Speaking of verifying with the institution, I received a text message supposedly from Bank of America, who I personally don't have any kind of banking relationship with. That text said, "*Please update your Bank of America contact information by using the following link,"* and there was a link in the text message. Now, like I said, I don't have any personal relationship with Bank of America so it was easy for me to delete the message and move on.

What if I did have an account with them? It definitely would have gotten by attention and I am signed up for text alerts with my actual bank. It's important to never follow a random link sent to you whether it's an email or a text message. If you need to update any account information, do it in person at a branch with a customer service rep; by calling the service phone on your account statement or the back of your debit and credit card; or through your company's website. When logging into your bank, brokerage, or online accounts, ensure the web address on the login page starts with H-T-T-P-S. The S is very important as it denotes a certain level of encryption and protection embedded in the website. I can't stress how important the S is as some online phishing schemes goes far as building a nearly identical website, resembling those of financial institutions.

Evan: Finally, I really want to talk about cat phishing, where an individual establishes an online relationship, representing themselves as a romantic interest or even a person in need with the intent of causing financial and emotional harm. As online dating and its various platforms become more and more popular and commonly used, it's important to develop a few habits to minimize your susceptibility to being taken advantage of.

First, it's important to maintain open communication and dialogue regarding new relationships with your close family, friends, or whomever you trust. While it might be embarrassing to talk with your friends and family about online dating, at first that is, it's the best way to ensure you have someone watching out for your best interest. This becomes even more important as one ages and it becomes easier to be taken advantage of by a new friend or relationship.

Keep your initial communication and messaging limited to the dating app until you get to better know someone you've met. Do a Google search on them to establish some legitimacy and their identity. If your communication begins to increase with a new person, set up an online video chat. Finally, when you're comfortable, arrange to meet in person. If the other person refuses to meet in person or continually makes excuses to avoid meeting in person, just move on and definitely don't transition money to this person. Lastly, don't send any compromising pictures of yourself to someone who you've met online. It seems obvious of course but we've seen plenty of examples of social figures or political leaders finding themselves in this very situation.

Elean: Finally, one last tip. Check your credit report periodically. No matter how careful you are someone can steal your identity, or unfortunately as we recently found out, a large institution can even open accounts in your name without you knowing. By checking your credit report, at least annually, you can see if anyone has attempted to open new lines of credits using your name or social security. Additionally, many banks do a credit inquiry when opening a checking or savings account and those inquiries will appear on your credit report.

Keep in mind there are three major credit reporting agencies used by institutions to check your credit; Equifax, Experian, and TransUnion. Not all institutions pull your credit from the same credit reporting agency so it's best to check each one once a year. It's good practice to obtain your credit report annually from each reporting agency, rotating each one every four months.

Evan: We hoped you've enjoyed and took something away from this episode. If you have a topic you would like for us to discuss, you can definitely contact us via our Facebook page or via email at info@paragonfinancialpartners.com. To listen and subscribe to our podcast, visit us on iTunes or Stitcher Radio. Finally, don't forget to download your Cyber Security checklist using the link in the description or on our blog at paragonfinancialpartners.com/blog. Thank you again for tuning it.

Disclosures: Paragon Financial Partners Inc. is a registered SEC Investment Adviser. The podcast is for informational purposes only and should not be considered a solicitation or offer to purchase or sell securities. The financial strategies and guidelines discussed herein may not be appropriate for everyone as each individual's circumstance is unique. Please review all tax information with your tax professional. Please review all legal information with your legal professional. We hope you enjoyed the Paragon Financial Partners podcast and again thank you for listening.