CarrieKersky.mp3

*This transcript was generated automatically, please excuse any typos.

Brad Levin [00:00:00] Hi everyone and welcome to seeking the extraordinary. Michael Nathanson has been kind enough to share the host mic with me today. I'm Brad Levin, managing director and senior wealth advisor with The Colony Group in Calabasas, California. So October is National Cybersecurity Awareness Month. And in recognition of that, we thought it would be ideal to interview a renowned expert in the field and answer questions that I know are on minds of a lot of our clients today. My guest today is Carrie Kerskie, president of Kerskie Group, founded in 2001 in Naples, Florida. Although she originally started her business as a private investigator, a growing number of clients that she worked with as a P.I. experienced various forms of identity theft and had no one to turn to for help. With little or no resources available on how to recover from a cyber attack. Carrie worked towards discovering the best methods of identity theft, restoration and prevention. Now, for more than 15 years, Carrie and her team have helped thousands of victims. These cases have enabled the Kerskie Group team to view identity theft, fraud, and cyber threats from all angles. Unlike other identity theft restoration services that only focus on the issue at hand, Kerskie Group digs deeper to identify other areas of risk and implement solutions to minimize or eliminate the threat that hand and limiting any future attacks by providing risk management services, primarily focusing on affluent individuals and families. Carrie is also a highly sought after professional speaker, and she's an author of two books, Your Public Identity Because Nothing Is Private Anymore and Protect Your Identity. She's a media favorite, featured in numerous publications such as Consumer Reports, Wired.com, Huffington Post and MarketWatch. She's also appeared regularly on NBC, ABC and Fox. Carrie, welcome. It's great to have you here today.

Carrie Kersky [00:01:53] Well, thanks so much for having me. I appreciate you having me, especially for cybersecurity month.

Brad Levin [00:01:57] Yeah I don't think the timing could be even more perfect because this is such a hot issue today. And I've spoken to so many clients over the course of this year and also friends and people that I know in the local community that have shared with me their own experiences with identity theft and cyber attacks. And I personally, my wife and I have also been targeted this year multiple times. So it seems to me like more than any year before, in my 30 years of business in the financial advisory field, I've heard about cyberattacks more than any other year in the past. And so my first question for you, Carrie, is, is my perception a reflection of our reality that cases of cyber attacks are on the rise? Or is this just my own anecdotal experience? I'm really curious to hear what you have to say about that.

Carrie Kersky [00:02:50] Yeah. So what's your experience? And is the same that many other others are experiencing? This is definitely on the rise, really. We saw a big shift after the pandemic because the pandemic forced people who might have been a bit tech averse. They weren't ready to embrace the idea of online accounts or communicating with Zoom, which is what we're doing now. So the pandemic really forced people to embrace the technology and also businesses shift how they did business as opposed to everything being in-person. It's now done online. The more people you have online, the more the criminals are going to use that approach to get to accomplish what they want to accomplish. So, yes, cyber attacks have definitely increased. Also, there's advances in technology. We're looking at A.I., they're implementing A.I.. So in the past you used to get

these phishing emails and it was obvious that it was a phishing email. Now they are so well written that I'm sure companies would love to use the scammer emails in place of their home because they're so well-written. So it's getting harder and harder to determine what's real and what's not. But yes, everything that you're experiencing is absolutely true. Cyber threats have definitely increased.

Brad Levin [00:04:02] Yeah, it's really amazing. I think back to some of these phishing scams from years ago and getting that email that says some president from Zimbabwe is looking for assistance to help him get some money out of the country and he's calling upon you to help him with that. You know, those kinds of things are so obvious. But you're right. These bad guys are getting more and more sophisticated. And it's really interesting to hear that our willingness to embrace technology like we have since the pandemic has actually opened us up more to be possible victims of cyber attacks.

Carrie Kersky [00:04:38] Yeah, And I think what it is, we embrace this technology, but we don't fully understand it. And a big part of it is it changes so rapidly. So just as soon as we wrap our brains around how to use a certain app or how to use a certain piece of technology, it's changed and modified. I mean, just think about with your phones alone, how many updates and operating systems that come out with new features. So things are always changing. It makes it difficult for people to understand what is the norm, how does it work, how does it operate. And also people have their own I call it cyber beliefs. What they think and know about technology influences how they respond when they're faced with the cyber threat. So if they think, Oh, I don't do anything online, I'm perfectly protected, I don't have to worry about it. Well, they're more subject to becoming a victim than someone who's a little bit more paranoid. And I would say in this day and age, having a healthy dose of paranoia is completely normal. But one of the big things, again, people don't do anything online. Nobody has my information. You can go online and by anyone's name, address, date of birth and social for $0.25, and that's basically.

Brad Levin [00:05:47] $0.35. Why $0.05?

Carrie Kersky [00:05:49] $0.25? That's all you're worth. Mine is $0.25. And it's basically basic economics, supply and demand. Last year alone, over 1 billion records were exposed to data breaches. So when you have a surplus of supply, it drives the price down. And we're not even talking about having to go on the dark web or the deep web. It's right on the surface web, which is the part that Google and the typical search engines actually indexed. So it's not a matter of, well, I don't do anything online or I don't I don't use social media. I'm protected. Your affirmation is already out there and it's not going to disappear.

Brad Levin [00:06:23] Okay. So before we go further, we're. Talking about this broad umbrella category we call cyber attack and cyber security. But what I really want to be very clear about is what does your business's services really address in terms of what specific arenas within cybersecurity do you focus on?

Carrie Kersky [00:06:44] Yes. So what I like to say is we focus more on the human side because cybersecurity, you have the ones that businesses are using to protect their the business from data breaches and cyber attacks. And then on the personal side, you can use antivirus firewalls. Those are more the technology aspect. Ours is more of the human when it comes to the prevention side, because what we don't know is what can get us in trouble. The other thing that we do is obviously we've been working with identity theft victims for more than 15 years, and during that timeframe we've learned that if somebody comes to us and they're like, Hey, I have this issue, we've learned that you can't just fix out

one issue, which is unfortunately what a lot of the other companies out there do, they focus on that specific one. When we work with our clients, we like to look at everything. We'll review their credit reports, we'll look at a lot of other different areas because often times there are additional red flags of things that are in the pipeline that haven't presented themselves yet. So if you don't address those things right at the beginning, then you're just going to have this perpetual constant incidence. So when we work with our clients, they come to us with one. It's not unusual for us to find a couple other incidents that are pending out there, so we'll mitigate those. But the biggest thing is if you only fix those issues and you don't do anything to try to minimize the risk going forward, it's going to continue to happen because the once the bad guys have used your information and they've profited from it, they're going to continue to use your information. So we've seen often where somebody doesn't they have an issue, they get it fixed, nothing happens for 12 months. They watch their hands saying, great, I'm done. I don't have to worry about it. A year later is when the bad guys will come back because they know that you let your guard down. So we work with our clients to make their identities difficult to use so the bad guys move on to easier targets. You can't prevent yourself 100% or protect yourself 100% from identity theft. It's impossible because most identity theft cannot be monitored. There's no way to detect it until you get a notification after the fact, like a letter in the mail, for example, with the money laundering, identity theft. We saw a huge spike in that during the pandemic. And people would find out because they would get a letter from a bank saying we're suspending your account due to suspicious activity. Well, they don't have an account with that bank. So their first response is it's a scam letter. I'll throw it away, but it's not. That's a red flag that somebody used their identity, opened a bank account and is moving money in and out from money laundering. Now, it has no financial impact, direct impact on the victim, because it's not using their credit, not using their bank accounts, not stealing their money. Where it's going to have the impact. Is that SAR report or suspicious activity report that the bank has filed that gets reported to the IRS and the FBI? So identity theft is more than just somebody trying to get into your bank account or use your credit. We've seen it expand exponentially, especially during the pandemic. So that's why with our clients, we try to protect what we can block, what we can we monitor for the things that can be monitored for. And we do a lot of awareness and education. We help our clients keep aware of. Here's the latest thing so that when it's presented in front of them, they can recognize it and they know how to respond properly. And finally, when everything else goes wrong or slips through the cracks or other things that you can't prevent where they're playing in place. So when something happens, they call us, we jump into action and we fix it, because the sooner you detect and respond, the faster you're going to be able to recover.

Brad Levin [00:10:17] Okay. Really interesting. I want to go back to what you said a couple of minutes ago. That was really pretty shocking. And that was you said that our information is already being accessed by bad guys and it's being sold for a fraction of a dollar. So that makes me really concerned because the reality is I'm thinking about this and it's like it's so easy to attack us without us even doing anything to open ourselves up for attack.

Carrie Kersky [00:10:45] Absolutely.

Brad Levin [00:10:46] But a question I have related to that is what about the actions that we might be taking on our own that actually make us more vulnerable to a possible attack?

Carrie Kersky [00:10:55] Yeah, and that's that's a great question. And this is something that if you don't listen to anything else in this podcast, pay attention to this, because these

are the things that also people come to us, they made these mistakes and that's what made them become a victim. So the first thing is privacy versus convenience. Because of technology, everybody's thinking this convenience factor, Oh, if I use this, then it'll save me 10 minutes or it'll save me a few steps. We have become so used to convenience that the thought of having to do. Two steps to log into an account is is overwhelming. Oh, my gosh. I don't want to have to deal with that. That's too much work. I just want to do one because most financial organizations, they all now offer and a lot of online accounts, too, multi-factor authentication. When you log in, you have a username and password and then they'll send you a code UCB via text or email. Or you can use a passkey with an authenticator like the Google Authenticator or orthe or one of these other programs out there. These are all steps or barriers to protect your account. If it only takes you one step to log in, that's how many it's going to take the bad guy to log in. If it takes you two, three or four, that's how many hurdles the bad guys going to have to overcome to access your account. So when you're looking at these things, don't view it as negative. Oh my gosh, this is too much work. I don't want to have to deal with this. View it as Yeah, absolutely. I'm glad this takes me 10 minutes because it would take a bad guy even longer. So privacy and convenience, they don't live in the same space. The more you have of one, the less you have of the other. On that same note, when it comes to privacy, social media. Think about what you're posting. A lot of times people, we get caught up in the social media because our friends are on their families and there it is. They are a great way to keep in contact with other people. But sometimes people reveal a lot more than they really think they're putting out there. There are organizations out there that do nothing but scrape the information shared or liked, or if you check in somewhere like you're at a restaurant or whatever. Organizations harvest and sell that information, and sometimes the people that buy it are the bad guys. Or they'll do these online polls and quizzes like, Oh, what was your first? What was your first car? Well, that's a security question answer for logging into an online account. Right. And people don't put that in the same space. They view that as, oh, well, this is social media and this is my bank account. You need to think about what you're putting out there and how it can be used against you. Quick little tip for answering security question answers. Those are the ones where whatever answer you create becomes the main answer, right? Don't use real answers because again, you can buy it in a database. So here's a trick. We call it the one off method.

Brad Levin [00:13:37] Okay.

Carrie Kersky [00:13:38] Pick somebody well and use that person as your answer key. So, for example, if I choose my son as my answer key, when the question is, What's your favorite food? I'm going to answer with his favorite food. So this way you don't have yes, you don't have to remember fake answers. All you have to remember is who is your answer key? And it's enough of a variation. The bad guys won't be able to buy it in the database. So little things like that. It takes a little bit of extra work, but it makes the difference. One last thing. Passwords. Passwords need to be a minimum of 12 characters. These eight character ones supercomputer can crack them in mere seconds. So when you're thinking of creating a password, don't think of it as a word. Think of it as a passphrase so you can use a line from your favorite song, book or movie. For example, I live in Florida, so one I could use is it doesn't snow here. That could be a password. And then I swap out the number. If I have to do symbols, I swap out it with one of the characters or one of the letters. And same thing with numbers. So if you use things like that, it's easier to come up with those longer passwords. Now, if you're listening to this, you're thinking, Great, I have 100 online accounts. I know exactly what I'm going to go and do that for each one of them. Break it down into tiers. Tier one, Those are your crucial accounts. If somebody got into them, they would do a lot of damage. Your bank accounts,

your mobile phone accounts. Otherwise, they could do sim swapping and porting of your number. Anything that if they got into, they could do damage. Those need to be unique passwords and that doesn't mean changing one or two characters. That means unique, unique, unique passwords with a minimum of 12 characters. Change them once a year. Unless you think that password has been compromised for everything else like your Netflix and such. If they got in, they might be able to do something, but you'd be able to repair that. So it's not that big of an issue. So that was, yeah, it's good to have a good strong password and don't recycle them, but they don't have to be as strong and unique as your Tier one. So it's just a simple way to kind of break it down.

Brad Levin [00:15:45] So then could you potentially just create two passwords that you use, one that is long and complicated that you use for those critical sites and then another one that you use for the less critical stuff, or is that not being safe enough?

Carrie Kersky [00:16:00] Yeah, unfortunately, in this day and age, that's not safe enough because if there is a data breach, for example, the Facebook data breach that happened I think was the last year this year seems like they've had quite a few lately. But the biggest thing that was exposed was username and password. So if you use that same password anywhere else, the bad guys can get into that. Years ago, when LinkedIn had a data breach, usernames and passwords, all the criminals did is they took those harvested usernames and passwords. They created a computer program that pointed to all the major financial institution websites, all the major banks, and it just ran all the combinations that were exposed during the LinkedIn breach. And they got into, I think, more than half of the accounts.

Brad Levin [00:16:42] So I know what some people do just dealing with this issue of the frustration of memorizing all these passwords is they write them down, right? So they write them down and their notes app of their phone or they write them down in a Word document or Excel spreadsheet, and it's saved on their computer. And that's what they go to look at to find that passwords so that they don't have to keep it in their memory. What do you think about that? Is that is that really an opportunity for them to be more exposed to somebody being able to access that information in a way that they might not be aware of?

Carrie Kersky [00:17:17] Yes, absolutely. It used to be that was a good way to do it. But now with all the viruses and we're seeing a lot with the remote access software, which I'll talk about a second here. So storing it on your device in a like a. A word document or a spreadsheet or notes. Bad guys know this. That's the first place they're going to go when they get into your device. So I do not recommend that. And password protecting it is not efficient because they can bypass passwords as well, especially for the documents in the spreadsheet. So I don't recommend that if you want to have it on penser pencil and paper written down on good old fashioned, that's fine. Just keep it in a locked file cabinet or hide it. If you have a book that's in your office or a bookcase, fold it up and put it in one. The between the pages of one of the books in the bookcase somewhere where somebody is not going to be able to find it, but don't put it underneath your keyboard. That's the first place I look, and that's where I find them rich. The other thing with the password storage is be very careful. Do not store them in your web browser. Again, it's that convenience factor for the autofill, right? What's happening with the remote access software? So you will get either an email or you'll get a text message or you'll get a phone call. So remember, the old phone scam would call and they would say it was Apple or Microsoft, and there was a problem with your computer and they were there to help.

Brad Levin [00:18:37] Yep.

Carrie Kersky [00:18:38] Yeah, well, that's evolved. And then it went to the Amazon phone call about a purchase you didn't make. Now you're getting these emails. It looks like it's a PayPal invoice showing something was already paid. And if you didn't pay this, click here or call this number. Well, in that instance, and typically it involves around some kind of been antivirus program or you'll have a pop up on your computer that looks like it's from my antivirus detected. You know, viruses call this number. There's different ways to do it. But the ultimate goal is to get you on the phone. Once they have you on the phone, then they'll go through this whole big story. If it's an invoice that was paid, they're going to tell you they're going to refund it. Then it's, oops, I screwed up, I forgot the decimal places. So instead of giving you 200 back, I give you 20,000. But now I need to get that money back or I'm going to get fired. But what they have you do is install remote access software. It is a legitimate software program used by the IT industry to remotely troubleshoot technical issues. Sure, it's not a virus, but once this is on your computer, they have you download it, install it, then they ask you to read the code. That code allows them to now take over your computer and they're going to do this dog and pony show making you put all these things in the command prompt or whatever, making it look like, Oh yeah, you got all these viruses. One of them is they'll have you type in. There's a command if you type into the command prompt on a Windows computer, it shows the IP address for that computer, but most people don't know what that is. So the bad guys tell you, Oh yeah, that IP address that connected to China, they're already in your computer. People don't know because they don't understand what that is. So they believe it. And then once everything is said and done, they have different versions. Either they'll have you do wire transfers or they'll have you buy cryptocurrency or whatever the case might be. But the biggest thing that people miss after the dust settles, that phone calls done and they called the bank, they called everybody. They think everything's resolved. That remote access software is still on that device, meaning that if you go and you panic and go, Oh my gosh, I'm going to change all my passwords, well, you save them back in your Web browser. When you go to bed, the bad guy fires up your computer and goes to your web browser and it fills it in and now they're in your bank account.

Brad Levin [00:20:49] So obviously don't use those password storage options like that Google offers you. Or maybe what about on your phone? Like iPhone will ask if you want to save your passwords so that it's convenient for you to be able to do that. When you go back to that website again, what do you think about that?

Carrie Kersky [00:21:07] So the ones in the Apple products you use keychain, which is a little bit better because you have to do the master password to be able to get to access the keychain to be able to do it. So it is an extra layer of security that the ones like on the normal web browsers, Chrome and whatnot, they don't have if you're if you're storing your passwords there. Definitely do not. And it'll always ask, do you want to store your password? Always say no. I recommend if you're going to use a password manager, there are plenty of third party ones out there that you can use and I'm the type of person I don't like putting all my eggs in one basket because of that gets compromised. Now you're out of everything, so there are many that you can use. The big thing is to look for encryption at rest, which means when your passwords are stored on their server, if their server gets hacked, your passwords are scrambled and they can't be unscrambled without that decryption key.

Brad Levin [00:21:56] She said it's called encryption at rest.

Carrie Kersky [00:22:00] Yes. So when your passwords are at rest on their server, they're encrypted.

Brad Levin [00:22:05] Right. Okay. So do you know what services out there provide that?

Carrie Kersky [00:22:10] Yeah. So the one there are many of them out there. Like you have you have dashlane. One password is another one. That's really good. There are some of them out there. But look for encryption and rescue and encryption and transit. And if anybody has any any question about so many by email, I'm more than happy to answer questions. Sometimes these things change a lot. So depending on somebody listening to this, if you still have a question, reach out and I'll be happy to answer it. But encryption arrests and encryption in transit because that's when you're retrieving or storing your passwords, that communication between you and their server. That's the weak link. So it encrypts that communication. So if somebody intercepts it, they're just going to have a bunch of gobbledy goo, a bunch of nonsensical characters that aren't going to mean anything. Because what encryption does, it takes the content and scrambles it and you have to have that decryption key to put it back into the original order so that it's actually usable. But if you use one of those, another great benefit and we get calls all the time from people after a loved one is either had a medical condition, an accident or they passed away and they were the one in the family who managed all the online accounts. Now, nobody can get into the accounts because they don't know where any of that.

Brad Levin [00:23:20] That's right.

Carrie Kersky [00:23:20] Yeah. So by using one of these password managers, you can create a family account and you can have separate vaults. So, for example, I use one of these and I have a vault that's for our family. So like the Netflix passwords. And so my cell phone, my children, my husband, and then I have another vault that's just for my husband and I. And that's where we keep things that just he and I need to know. So you can you can categorize these and then you can also point someone to B and I'm drawing a blank on the actual terminology, the use, but it's almost like the emergency contact. Okay. So if something happens to you, that person will be able to get in and get access to all the passwords.

Brad Levin [00:23:57] It's sort of like maybe on your phone or your social media sites, you can appoint somebody to be sort of be like your legacy. Contact, I think is what they call it.

Carrie Kersky [00:24:06] Yes. Yep. I think that yeah, I think that's the term I always blank on that one. But yeah, that's, that's what it is and it's good to have because again we get calls all the time that people are like, we can't manage any of the bank accounts, we can't pay for any of mom's stuff and she's in the hospital. And can you break into her her iPad? No. Right.

Brad Levin [00:24:23] Right. So that's what that's one protection now is actually preventing us from doing what we need to do. So but I like these ideas. You're suggesting because it's it's methodical. That's something that anybody can do. And obviously it adds a serious layer of protection that we all need. But I want to ask you about a couple of different types of attacks that I'm aware of. So you get a call from somebody that says that they're from your bank. Now you have an account with that bank that they're talking about, and they say that they're notifying you that they see some suspicious activity going on in your bank, that there is somebody at a point of sale right now attempting to make a charge. And they ask you, is this legit or is this forger? Well, yeah, that's fraudulent. I'm not

there. Okay. So we need to first verify your identity. We're going to send you a code. Please write us back. The code so you do that. And now within minutes, they're actually changing your password to that banks website. Yes. They then get into your bank account and they're moving money around. How does that happen?

Carrie Kersky [00:25:24] Yeah. So the way that scam works is the bad guys know that the banks use the two factor authentication with the code that gets texted to the mobile phone. So what they'll do, it's almost like a two part process. So you have the one person who's initiating either the text message or the phone call or the email saying that they suspect fraud. So you have that one being watched. And then at the same time, when you get on the phone with the person, there was the email or the or the text message. When you get on the phone with them, they're going to go through this whole thing. And then at the same time, one of their partners is sitting there on a computer trying to do a getting ready to initiate a password reset.

Brad Levin [00:26:07] Right.

Carrie Kersky [00:26:07] And as soon as they say, okay, we're going to send you a code, when you get the code, let us know the initiate the password, reset, you get the code, you read it to them. They now entered the code in there in your account. They change everything.

Brad Levin [00:26:20] So what they're doing is they're using that two factor authentication protective service to actually get you to participate without your knowledge in changing your password. So when they send you that code, that's the forgot password code. So you read it back to and they then go in, they change your password, then they're in your bank account just like that.

Carrie Kersky [00:26:40] Yes. Yeah. And that's really what we see here. But a lot of these these scams is they're using they legitimate or anti hacking or security programs that were designed to protect people. They're using them against us. So anything that you get, whether it's a letter or phone call, email, text, message, validate or eliminate. It really is that simple. You don't need to remember all these rules and all these steps. Forget that because the step changes week to week. Validate or eliminate. So how do you validate? Well, if you have an account with that company, let's say it's a bank. Yeah. Log in to your bank account. If there's a suspicious activity, it's going to show there. Right. If you get a thing that says your password is reset on your online account, try logging in. Don't click any of the links in the emails or in the text messages. And do not call the phone numbers in the emails or the letters or anything like that. Always look up the phone number at the organization's website. That doesn't mean do a Google search for a phone number because what pops up in the search results is not actually the legitimate phone numbers. For example, if you try to do a Google search for a phone number for Google. Phone numbers are going to pop up. The Google doesn't have a phone number that you can call them. Those are the bad guys doing well. Wow. Yeah. And we've seen them register old phone numbers that when when companies decide to get rid of older numbers and they consolidation or whatever, the bad guys immediately register those numbers and answer them the same way we see a lot of that with Comcast because they recycle some phone numbers and there are still some of the old phone numbers circulating on the Internet and it's the bad guys who own it and they answer saying Comcast. And they've gotten into a lot of email accounts that way. So validate or eliminate no matter what comes across, you can't validated 100% to know that it's true. Get rid of it.

Brad Levin [00:28:30] Right so that old saying trust but verify, you're essentially saying don't trust but verify.

Carrie Kersky [00:28:36] I'm saying don't trust and verify about 25 times.

Brad Levin [00:28:40] Yeah. Yeah. So I want to go back to something you were talking about earlier, and that is social media. So this is where I was actually the target of an attack earlier this year where my wife was contacted by a friend of ours, said Brad, sending me some interesting messages through Instagram, kind of asking about my interest or involvement in investing in cryptocurrencies. Is is is he pitching that stuff through social media? And she was like, No, no, no. Of course, of course she's not doing that. And then her brother to contact her and said, I was having this conversation with Brad, direct messaging me through Instagram and he was talking about something that I know is part of your guy's life. But the question's then kind of diverted and they got a little bit strange. Well, I rarely post on my personal social media because I'm concerned about this stuff, but somehow somebody essentially took over my profile and was posing as me. I was communicating with people that I know and they were using information from my past, I guess, as sort of the the the the backup or the documentation to support the story that it was legitimately me. So what should people not be doing on their social media that makes them more likely to be the target of an attack, if at all? There's anything that we can do or what are some of the things that we might do that otherwise make us potentially more vulnerable that we should avoid doing?

Carrie Kersky [00:30:11] Sure. So there's two ways that that could have happened with your your your Instagram account. So either they took over your Instagram or the cloned your Instagram account, meaning they created a whole new profile, took your profile picture off your account, moved it over. So now there were two of you with Instagram accounts out there. We see that a lot on Facebook. There are tons of cloned accounts out there. And the minute that it's cloned, they now look at your profile. If you have your profile set as public, they can now see who all your friends are. So then they send, send, send friend requests to all those people. And those people, they don't stop and think, well, I thought we were already friends online. They just go ahead and accept it because they know you. And then that's how they start messaging. Or other times it could be sometimes you might get a direct message from someone in or have like a link or something in it. There was a big one going round on Facebook that was called This Looks Like You. So somebody would send you a link to a video and they're like, Hey, this looks like you in this video. Well, I had a curiosity that people were clicking the minute they did allow the bad guys to get into their accounts and then share that exact same thing out to all of their contacts. So the big things to remember with using social media is don't it's not your personal diary. It's not your personal chat room with you and your closest friends and family. It is a public domain. If you're not going to put it on a billboard on the side of the highway, don't put it on social media because in essence, you're doing the same thing right, with direct messaging. Be very cautious. I don't even use direct messaging. I don't even have the direct messaging app on my phone for Facebook or any of that stuff. I took it all off because they get into way too much information on the phone. Yeah, but yeah, but when I go in and I look at those messages, most of the time I don't even respond it. Sometimes I do that it looks like it's something legitimate, but the minute the questions start kind of going south, that's when I just say, okay, that's it, we're done responding. But yeah, you have to be very, very careful with what you post out there. And again, don't participate in these surveys, these polls, these. Quizzes. It's. Oh, learn. Find out what was your job if you lived back in during the wild Wild West, It's like, who cares? Stop doing these things because you don't realize when you're doing those you could be giving

someone access to your online account. The other thing is social media, though, should be a tier one password. They should be a strong password. And you can send out multi-factor authentication for logging in with social media. If it offers it, take advantage of it, or at the very least activate the of alerts. So when somebody logs in to your social media account, you'll get an email saying, Hey, someone just logged in. So those are extra things you can do to keep an eye on it. But even if you get an email that says, Hey, somebody logged in and you didn't do it. Don't mess with that email. Log in to your social media account and go in and look at the history. Or as a precaution, when in doubt, change the password. But yeah, this is where the bad guys are getting all the information because they can go back and see everything that's on there. That's another thing too. In your settings, you need to go in and adjust them because when you first sign up for these apps, the settings are in favor of the social media company, which means everything and anything is out there. Go in and adjust those and if they do an update, they tend to push out an update on the app. Check them again, because sometimes they'll revert back to the other way. But make your profile private. The only way people can view your photos or anything else that you're doing is if you are friends with them. So that's one way to block some of that information from getting out there.

Brad Levin [00:33:43] So one of the things that I see people doing probably most commonly on their personal social media, especially Instagram, is they're posting photos of themselves on their family vacation. And so do you have any suggestions regarding that? And does that expose people to risks that they might not be thinking about?

Carrie Kersky [00:34:00] Most definitely does appear posting a picture and you're like, Hey, the family were on a two way cruise. Well, great. Now they know they go rob your house because nobody's there. And you might say, Well, they don't know where I live. It's really easy. They go by your name, address, date of birth and social for $0.25. Don't forget that. So if you do want to share those things, wait till you get back home and just say, Hey, we had a great vacation. Here are some photos. You don't have to tell people where you are every minute of your life. I just it is mind blowing to me how in the past, before social media, if you ask somebody some of the questions based on like what they're showing now, they'd be like, Well, I'm not telling you magical. I'm going, Hey, what did you eat for breakfast today? So there's. But now everybody take a pictures of their food, taking pictures of their their friends, their family, where they are checking in. The other thing, parents, be very careful what you're posting of your children. You might think it's great to take a picture of Suzy and her little cheerleading outfit. But on the front of that is the name of the school, or at least the mascot. People could figure out where your kids go to school now, and from there they can figure out basically what city you live in and proximity goes to that school and eventually, where do where do you live? So we need to start reining it in a bit. We don't need to share everything in anything. As a matter of fact, I don't really use social media anymore. I have the apps. I log into a maybe once a month and it's still the same old stuff, so I'm not missing anything. And as far as posting, I just mainly like safety tips. I'm not really big on posting anything anymore because I've seen the aftermath of what can happen.

Brad Levin [00:35:37] I agree. And I and I know people that really are documenting everything that's going on in their lives. And I always say to my friends, I'm not posting on social media. That's because I'm out living my life.

Carrie Kersky [00:35:49] Right.

Brad Levin [00:35:50] So the other thing I wanted to ask you about is I often talk to clients of ours about things that they are concerned about in terms of their possible exposure to identity theft and financial fraud, and especially elderly clients will say things like, I don't want to receive electronic statements, I only want to receive paper statements in the mail. I don't want to do any transactions online. I want to do it all by check, for example, and send the checks in the mail. So what I wanted to ask you about, Kyra, is what about misperceptions about our activities that may actually not be exposing asterisks and the actions that we think are safe that do expose us to risks that we might not even be aware of.

Carrie Kersky [00:36:39] Yeah. So real easy. Everything has risk. Nothing is safe anymore. You'll never hear me say anything is safe. Okay. So if you're paying by, check the risks you're going to have. Is that from your mailbox to the receiver's mailbox? That check can be intercepted. If it's intercepted, somebody can open it up, Take a picture of it. Now they have the routing and account number. They go to an office supply place. They get the print on demand checks, and now they start printing checks for your account. Or they can do check cashing. But if they if they do the check watching, then the receiver never gets the check. But if they do the middleman, it's. Where they just take a photograph of it, they seal it back up and mail it on its way, and you never even knew that it even happened because the person you send it to actually gets that check. So that's the risk there. If you're doing it online, yeah, there's a risk that something could be hacked or be intercepted. But from my opinion, when you're paying things online, you have instant confirmation that the other side has received it. So let's say I'm paying my American Express bill. I'll log into my American Express, I'll initiate the payment through from my bank or whatever. And then after it says it's done, obviously they use my app or log into my bank account and I can confirm. Oh, yep, that's it. In process, it's pending. It's on its way out. So now I know the transaction is done. The other thing is there are laws in place to protect you from fraudulent activity in bank accounts and credit cards. So the most important thing to remember is monitor your activity. Reconciling your statements is the best thing that you can do. But don't wait 30 days to look at it. That's the only problem with the paper statements is if you're only seeing what's happening in your account every 30 days, it could be wiped out and you won't know it until 30 days after the fact. And then it just takes even longer to try to recover those funds. So I recommend, first of all, if you don't want to use the online law, online banking for transactions, that's fine. But at least set up the online account because the individual institutions all offer online accounts. Heck, everybody has online accounts. Now, if you're not so-called, you can tell your dogs that you're not marking your territory. You go, then you're leaving it open for someone else to do. And we used to see a lot of this before the pandemic is people are refusing to do online banking. We had one gentleman. He lost a quarter of $1,000,000 in 30 days because he refused to do online banking. So the bad guys called. He was a private wealth management client of a large national firm. They just called the 800 number. They had his name, address, date of birth and social, which is what was required for ID verification. And the imposter said, Yeah, I'd like to set up online banking. And they're like, okay, great. We'll call Mr. Smith Gray, Mr. Smith, we'll send you an email. They send an email that the bad guy, the bad guy set up username and password. Now he was in the online account and he linked it to an American Express gift card. So when they looked at the statement, it just said Gift card or is it American Express?

Brad Levin [00:39:40] Yeah.

Carrie Kersky [00:39:40] And that would not be picked up by credit monitoring because there were no credit transactions.

Brad Levin [00:39:45] Wow. That's fascinating.

Carrie Kersky [00:39:47] Yeah. So, again, at least set up the online accounts. At the very least, if you're not comfortable doing the transactions, that's okay if you want to slowly get into it. But it doesn't matter if you're going to the website or if you have the app on your phone. For me, every morning I get up and I look at the all my financial accounts and I do it again before I go to bed, because I only have to look at what happened during the day as opposed to waiting 30 days and having to look at tons of transactions. But again, the thing with mail, we're seeing a lot of mail theft, a lot of mail. I mean, it was so bad that I think it was Seattle. They actually announced that they're are shutting down mail service for a period of time because that that was so bad. Oh, my gosh. With the mail forwarding and everything. So here's a tip. Set up an online account with the post office USPS scheme. Once you have the account set up, activate informed delivery every day you'll get an email with the snapshot of all the first class mail arriving in your mailbox that day. So it's a way to yeah, it's free and it's a way to monitor for theft, but it also helps monitor if somebody tries to initiate a mail forwarding or change of address because you'll get an email from the post office. If you don't have informed delivery, you might get that letter from the post office 4 to 8 weeks after the changes already been made. So every account.

Brad Levin [00:41:08] I was actually talking to a client of ours just last week that was saying that they were the victim of bank fraud twice in the same month. And what happened was they had checks sent to them that they ordered from the bank and they did not receive the checks. The checks were intercepted twice. So either it was intercepted at the bank or at the post office. But ultimately, the bad guys got their hands on the checks both times and wrote checks out to whoever they wanted to write them to. And our clients were the subject of that attack. But fortunately, as you said, there are protections that these financial firms, whether it's banks or investment firms, offer in the event that something like that happens, but you need to be able to identify it right away. So I like the idea that you suggested of just checking everything on a daily basis, because if something bad happens, at least you know that it just happened. Right. What I wanted to ask you about something else as far as online bill payment. So you were describing a scenario where you go to American Express, you make the payment, you get confirmation right away. But the other side. Or are you is you go to your banks website and you're doing online bill pay through them, but you're not going to get a confirmation that those bills have been paid because actually what they do in most cases, if my understanding is correct, is that they're going to send out a check from the bank or maybe in some cases they do electronic payments. But a lot of times those are going to be checks that they send out. So you don't get confirmation right away that payment has been received. What are your feelings about using that kind of service?

Carrie Kersky [00:42:40] Yeah, so for me, I prefer the 1 to 1 method because when you're doing the bill, paying through the financial institution, through the bank, often that's outsourced to a third party. And how that was discovered was years ago one of these third parties had a data breach and they had an issue where somebody hijacked their website and people were got into accounts. So I always try to have as many people involved as or at least amount of people involved as possible. So when I pay American Express, American Express pulled it from my bank, I go to my bank, I confirm that they send it over to American Express. And like you said, you don't know if they're going to be sending it by check or they're going to be doing it through electronic. And if they do it by check, if you had something typed wrong, then might go somewhere else. And then you have to wait at least 7 to 10 days before they get the check and the payment gets processed. So if you're

going to be doing the online, the benefit of having that instant confirmation. So I personally I don't do the online bill paying through the bank. I prefer to just do it direct.

Brad Levin [00:43:41] Okay. Thanks, Carrie. So I want to get to talking about remediation and restoration services and how you can help people. But one more question I've got for you about exposures to risk before we do that. And that is. We're talking about technology and all the technology that we utilize these days that make our lives theoretically simpler. And they do in a lot of cases. But what about devices that we have in our home? I've heard that the devices that we might have, like Alexa power devices, that they're listening to us, that they could be actually picking up information from us that then could be used against us. Is that real or is that just, I don't know, hocus pocus?

Carrie Kersky [00:44:21] So, yeah, there's been a lot of cases that have come out showing that even though the company might say, No, we don't, it actually is recording. There was one woman before where she went to Amazon. You can have you have an account with them. You go in, log in and you can request all the data. And she got this ginormous file and she has the what is it, the echo or the dot or one of those smart speaker things. And when she accessed that file and opened it up, there were snippets of her conversation. She heard she listened to them. Wow. But think about the way these things are designed. Now I'm having to reverse engineer any of these. Take no part or anything. As a matter of fact, I don't have them in my home. I always buy the dumb appliances. I don't want anything smart except for now. Some things you can't even buy a dumb car anymore. Everything is smart technology, so it's getting harder and harder. But the way that they're designed is if you say a phrase, whether it's, Hey, Siri, hey, Google, hey, whatever. Yeah, it's supposed to turn on. How does it know when you say that?

Brad Levin [00:45:23] I was listening all the time, right?

Carrie Kersky [00:45:25] Right. That that's my point. Because if it says, oh, no, we don't listen to anything, well, then how does it know when you've said that? That's the question that I asked. So, yeah, my my family, I'm the party pooper. I won't allow any of that. So, Mike. No, I'm sorry not having it even on my phone. My iPad. Siri, all that's turned off. Yes, it probably still is listening to some extent, but yeah, I turn all that off again. That's just me. Only because of what I do. I see a lot of what could happen. So I'm probably a little bit more paranoid than the average person out there.

Brad Levin [00:45:56] I bet it's scary, though. I mean, what we're talking about is really scary. It's like you can't really do much these days and feel like you are being safe enough. Right. I think that's really concerning. So let's now address the situation where you have been the victim of an attack, financial fraud, identity theft or anything along those lines. What can be done? What are the services that your firm offers to help people in that situation?

Carrie Kersky [00:46:22] Sure. So the first thing we do when talking with a victim, I don't like the word victim, but it's just an easy way to to explain it. We like when we assess the situation, what happened that led up to the event and then what was done afterwards. So so what happened and what is the person done since then? The what happened is crucial because like we were talking before about the remote access software being used on these phone scams, if I know that what happened to them initiated through a phone call and based on some things that they're telling me that that happened during that phone call, I know that there is a 99% chance that remote access software is still on all their devices. So in that case, we, depending on the location where they are, will bring in either

one of our tech partners or if they have a tech person or an IP person that they work with, we will tell them explicitly what to say to how they get their devices checked first, because no matter what we do, if their remote access software is still there, the bad guys are can continue to do damage. So that's why the beginning we assess the situation to make sure there are no outliers out there that are going to interfere with what we're doing. If that's not the situation and it's just, you know, remote access after anything, then we find out what happened to them, what steps they've already taken and any responses they might have received. So if they've already contacted the bank or the credit card company, what did they do? What was the response? So that way we know where they are in the process. Then we schedule a a call with them. Usually we do an intake session, takes about 2 hours, and during this call we're going to go look at everything that they have, any incidents, whether it's an email or correspondence or a letter that got in the mail. We're reviewing everything because we like to read it, because if we see it ourselves, we can see things that that other people won't pick up on. We're going to look at the credit reports. We're going to make sure that they have good the minimal protection in place, which the best way to protect yourself from new account fraud is with a credit freeze. Mm hmm. And you do that by going to each credit bureau, You can have a free online account that you can set up with Experian, Equifax, TransUnion. There's also and Nobis, which is the fourth credit bureau and NCT. We National Consumer Telecom Utilities Exchange, that's utility industry, meaning mobile phone accounts. So we look at all five.

Brad Levin [00:48:41] What was the fourth one?

Carrie Kersky [00:48:41] You said Nobis and Nobis. So I kn the or invests in a business that's another. And we're starting to see a lot of activity on those now.

Brad Levin [00:48:53] And of course, really to effectively freeze your credit, you have to do it across the board, because if you just sign up for a service, let's say through Experian, you've just covered one opportunity for attack, but not all the others, right?

Carrie Kersky [00:49:04] Exactly. When it comes to a freeze, you have to do it with each bureau directly. Now, a fraud alerts is different. So I'll explain real quick. So a fraud alert is just a disclaimer, a warning or statement that goes on your credit report to warn a potential creditor that there's an increased risk of identity theft. And they're supposed to call you and confirm before the account gets open. That's not 100% effective. We've seen accounts get open even though people have a fraud alert, a credit freeze. Both a fraud alert and a freeze are mandated by federal law. So you have federal protection with a freeze. It states that when you have a freeze, the credit bureau is not allowed to release your credit report for any new credit applications or increases in credit limit. So if somebody is trying to apply for American Express using your identity and I'm just using them because they're an easy one, remember when they get the application, American Express is going to pull the credit report. Well, if somebody has a freeze, the only thing they're going to see is file frozen for consumers request. They're never going to see the report. American Express can't make a financial decision. The account doesn't get opened. So it's the best defense against new credit account fraud. Now, with the freeze, if you need to lift it, meaning let's say you have all the bureaus frozen and you need to refinance or you're getting a car lease and it's up for a new your new lease on it. And they have to look at your credit report. All you do is log in to the accounts, do a temporary lift. You put the start date and the end date, and then you go to the car dealership and do what you're going to do. It's because we have clients where some of them will manage that for them. And obviously that's on a limited power of attorney and everything for us to be able to do that. But I've had them call me from a car dealership and they're like, Hey, if my hand doing my lease and I forgot it, can you help

me? So we're able to help them with it. So don't buy into the marketing about a credit freeze. It's going to be complicated, it's difficult, and it's going to add more time. That's all marketing garbage. Now, the other thing to watch out for, and I know we're getting a little off or I'll get us back to it, but this is important. I want people to know there is a freeze and there's a lock.

Brad Levin [00:51:19] On the credit. Ask you about that.

Carrie Kersky [00:51:20] Yeah. So the credit bureaus are going to promote a lock. The difference with a log is that it is not protected under federal law. Like he freezes a lock is just a contractual agreement between you and the credit bureau. So if you do a lock and not a freeze, you could be giving up the rights afforded to you by federal law. Now, recently, we have acquired where they have a personal assistant who manages all the freeze accounts for them. And we we did the monitoring and we got an alert about an acquiring, meaning a credit application. So I reached out to the personal assistant and I said, Hey, did you guys do this? And he's like, Well, no, no. How did this happen? We have everything locked down. I said, Well, I can't see the accounts. Log in and make sure you still have the freeze. And he said, All the bureaus? Yes. Then he calls back in the one with Experian. And he's like, Well, we have the freeze and the lock. I said, Why didn't the lock? She said, Well, we figured it was double protection. So I said, Well, you're going to have to call Experian and find out what happened. Experian told him that they had a contractual agreement with that particular creditor that allows them to release the report because they have a lock.

Brad Levin [00:52:32] Wow. So the lock really actually is not a lock. It's a way out. It actually exposes you to potential risk.

Carrie Kersky [00:52:40] So the way I view it.

Brad Levin [00:52:42] Okay. So having the lock on top of the freeze actually sort of undoes the freeze.

Carrie Kersky [00:52:47] It very likely could. I don't know if that was an anomaly or if that's the regular, but again, a freeze. Your rights are protected by federal law and the requirements of what the bureaus are required to do or what their bureaus are required to do is mandated by federal law with the lock, all that's gone. So stick to the freeze, only forget the lock.

Brad Levin [00:53:10] Yeah, I'm really familiar with the credit freeze because we deal with a lot of high profile clients, like celebrities and athletes who are very concerned about those potential for risk. When you're talking about the freeze. I just want to make sure that everybody understands in order to be effective with that, you have to freeze it across the board. You have to freeze it, which with each one of those credit reporting agencies. So does take a little bit of work because you can't unfreeze it in one simple step. You have to go to each of those websites to reverse the freeze temporarily.

Carrie Kersky [00:53:41] Right. Yeah. But it definitely is worth it because, again, that privacy, convenience you have, it takes this many steps to do it. And again, it's the five bureaus. There are actually there are more than 50 consumer reporting agencies out there. So when we see cases involving money laundering, identity theft, then we will. There are other consumer reporting agency reports for requests. So sometimes we'll have to do a check systems report or then there is second chance lending programs because

the bad guys know that people are starting to do a freeze. So they're going to predators that are for people who have lower credit scores or no credit, and they're getting things, their payday advance loans, those sorts of things. So even though you might have someone who is ultrahigh net worth and they're like, my credit score is the best of the best, the bad guys don't care. They're going to these subprime lending companies because they know that those credit reports are not frozen.

Brad Levin [00:54:33] Wow. Yeah. And what you're talking about here in terms of increasing our level of protection, this is not expensive. It doesn't cost anything to do this. Right.

Carrie Kersky [00:54:43] For some of these things. Correct. So like to put the credit freeze again, that's your best defense against new account fraud. It's free. Anyone can do it. Just make sure that you don't use the username and password. Some of them will still assign a pin and then you might have a security question answer so long as you keep those credentials. And we're working with clients good. The way we do our service for the restoration. We don't just fix though, like I said, we don't just fix the one or two problems. Ours is a 12 month program because we've found that somebody comes through it with one issue. Like I said, there might be other things in the pipeline that just haven't presented themselves yet. So that's why the rate that we charge covers everything that might occur within that 12 month window. So if we start January and then three months later, something else popped up that wasn't visible during that time. We fixed that too. And again, after 15 years of doing this, we know that it's not just very rarely is it a one time incident. So that's why we've made the model to be that way, where we cover everything during the 12 months, the monitoring that we help with, the prevention and that and with also the awareness, because that's another part of it. If you don't know about these things, when you get the letter about the account being closed due to suspicious activity and you throw it away, that's why we do a lot of education with our clients to make them aware. So when something happens, they call us, we jump in, we fix it. Problem solved.

Brad Levin [00:56:01] Okay, well, really good. So let me ask you about identity theft protection services. The big one out there that most people are going to be familiar with is LifeLock. So companies like that, what do they do and is it really worth it to pay for something like that?

Carrie Kersky [00:56:17] So they do serve a purpose depending on budgets and whatnot. But I will say that the clients that come to us that are victims, most of them have one of those services, yet they end up hiring us to actually get the work done. What we've found is with those services and they only will fix certain types of identity theft, credit related, financial related. If you get into the criminal identity theft, the medical identity theft, the business identity theft, the money laundering, that the synthetic I mean, there's so many other types out there, they don't cover those. So that could be an issue because all time they've come to us and we're like, well, you're paying for that. Why are you calling us? They told me that wasn't covered in my plan. So if you are going to get one of these services, make sure you know what you're paying for. Don't fall for the marketing gimmicks of the million dollar guarantees and all this other kind of stuff. All that is that is a master insurance policy that because you are their member, you can get access to. Again, all the clients that we've had, none of them were able to get anything. And so it's insurance policy. It's not to say it's not possible, but just from our clients, from what they've told us, they have it. If you're looking for mainly the credit monitoring now, in my opinion, with the credit monitoring, if you have a freeze, you've walked everything down. So you really is monitoring worth it? Maybe not as much. You can get that now through your credit card. I

mean, credit cards will now offer it or they'll offer you can get your credit score or you can get your credit reports. There are free sources out there that you can do that. If you're going to pay for one of these services, you're paying for it, because if something happens, you want them. Who's going to fix it? Even though they're called identity protection or prevention, there's no protection or prevention whatsoever. They didn't warn you. Send you an alert through monitoring after. Something has already happened. So there's no proactive. It's all reactive. Most of them won't even tell you about setting up a credit freeze, because if you have a freeze, you really don't need to monitor. Yeah. Right, Exactly. So, like I said, they do serve their purpose there. There are some people out there where that's the only option they have and they are good for a lot of the basic stuff. So I'm not saying they're a complete waste of money, just depending on your needs and the level of service of you want. Obviously, they're a call center. With our clients, we have a dedicated person. We know we're no call centers here. We just work one on one with people. So that's really the big thing to consider when you're looking at one of these options. Ask these questions. And if you can't get a person on the phone to ask these questions, that's something to think about, too.

Brad Levin [00:58:54] Excellent. So just to clarify my understanding of best practices, we were talking about things that we should not be doing in terms of our behavior that exposes us to be more susceptible to risk. And we were also talking about steps that we can take to protect ourselves in terms of credit freezes. Is there anything else I'm missing? Is there anything else that we can tell our listeners that they should be doing or should consider doing that could increase the love, the layer of protection around ourselves?

Carrie Kersky [00:59:24] Yeah. So the two big things to remember, and I always like to make things simple and easy. Privacy versus convenience. Yep. When you're looking at something or when you're going to do something, your instinct might be, Oh, that's quick, that's easy, that's convenient. There are apps out there that you tie in to all of your financial accounts and it'll tell you what subscriptions you're paying for. Well, now that's somebody else who has access to all your bank accounts. So what happens? So again, it's that privacy versus convenience. I'm not saying it's a bad thing to do. You just have to identify what the risks are and determine if those risks are worth the reward when it comes to giving up your privacy. The other big thing. Validate or eliminate. That is really the biggest thing. That would save a lot of people. And when I say validate and eliminate, if you got a letter from the bank saying the account was suspended due to suspicious activity, you would validate that by looking at the phone number for the bank, calling them saying, I got this letter, What's this about? And you were determined that there actually was an account open. So that's a way to validate if you did it and you just threw that away, you could end up having some consequences down the road. So every letter, phone call, email, text message, if you're not comfortable with doing the validation, get a trusted partner who you can be an advisor. Like, for example, with our clients, they all know anything they get, they send it to us and we'll help them vetted and determine if it's legitimate or if it's a scam. Or they could just throw it away. If you have a trusted advisor, whether it's a family member, an attorney, a financial person, whenever, whatever, have just say, Hey, I just got this. Can you take a look at it? Tell me what you think. So when in doubt, it doesn't hurt to get a second opinion on these type of things. I do the same thing. I've been doing this for years. I do it day in and day out. And every once in a while I get a couple and I'm like, okay, I know there's an angle here, but I can't see it. So I have someone that I send it over to my. Kate take a look at this. Tell me what I'm missing. So don't be afraid to ask for help. Don't be afraid if if something does go wrong and you were manipulated by phone scam, email scam, whatever. Don't be so embarrassed that you don't tell anyone about it, because that could lead to a heck of a lot of problems down the

road. If you think something has gone wrong, you clicked on something or you gave somebody information on the phone or whatever the case might be. Take action right away. Please don't be embarrassed. Everybody makes mistakes. These people who do what they do, they are very good at it. They go to school to learn how to get you to do what they want to do. They know what to say and how to say it to convince you and manipulate you. This is their full time job. That's what we are up against. So don't be embarrassed or afraid to ask for help. Don't be afraid or embarrassed to reach out and say, I think I made a mistake. Can you help me figure out if I did the right thing or not? Those are the really the biggest things. Because once we get rid of all this stigma of, oh my gosh, I can't believe they fell for that. And we open these lines of communication and ask for help. We're going to be better to defend against the bad guys because the biggest advantage they have, we don't want to talk about this stuff. We don't want to tell anybody about it. And if we're not telling others about it, they can just do whatever they want.

Brad Levin [01:02:40] Oftentimes people are embarrassed. They're barest admit that maybe they did something that was a mistake and now they feel dumb about that. Well, fortunately, I can tell you, because of our role with our clients, we've been contacted numerous times about suspicious activity by clients and been able to help them identify that and thwart that potential attack before it's happened. Or in the event that they're notifying us after the fact, we've been able to get them in touch. With great people like your firm to be able to help them remediate the situation and get back on the right track. So this is all really very helpful and really important information. Carrie, I really appreciate what you've shared with us today. I think it's so valuable. We're living in an environment that I said it's scary, but it's it's comforting to know that there are things that we can be doing to increase our level of protection and that you guys are out there as the good guys that we can turn to for guidance and help in the event that we need that.

Carrie Kersky [01:03:41] Yes. Well, thanks so much for having me here, because like you said, the more people are aware of this, the better protected they're going to be. So I appreciate you invite me to come on and all that you do as well to help your clients. And it's great having that that trust and that relationship with them because everybody needs somebody they can turn to because the stuff changes all the time and you never know what's going to happen tomorrow. Yeah.

Brad Levin [01:04:01] You bet. Well, again, thank you, Carrie. And that is the extraordinary Carrie Kersee And you can learn more about Carrie and her company services at her website, which is Carrie k sorry c.a.r.e. I e kbr s-k i.e. dot com. And you can also follow Carrie on LinkedIn. Thanks again for joining us today.

Carrie Kersky [01:04:25] Carrie Thank you for writing for Janet.

Brad Levin [01:04:27] And thank you to our sponsor, The Colony Group. The Colony Group is a national wealth and business management company with offices across the country that itself seeks to extraordinary as it pursues its unrelenting mission of providing clients with peace of mind and empowering their visions of tomorrow. To learn more about The Colony Group and how it manages beyond money, visit us at The Colony Group dot com. You can also follow The Colony Group on LinkedIn and Twitter at The Colony Group for seeking extraordinary. I'm love it. You can follow me on LinkedIn and Twitter at RAD 11.