PNC Women in Business Webcast Series Transcript

Fighting Financial Fraud

September 16, 2020
2 p.m. ET

Moderator: Ladies and gentlemen, I'd like to welcome you to our 7th Webcast in PNC's 10th Annual Women in Business Week. Today's webcast is titled: Fighting Financial Fraud. Before we get started, I'd like to mention that today's webcast is being recorded and you are currently in a listen-only mode. Now, I'd like to acquaint you with some of the ways you can participate today. The ON24 room you are in allows you to individually adjust and resize all available panels on your screen. To resize any of the consol panes, simply click on the lower right corner of that panel to adjust. If you experience any technical difficulties today, first, try fleshing your browser to reset your connections and if that doesn't work, go ahead and enter a question into the Q&A panel stating your technical issue and I'll be more than happy to assist.

So now without further delay, let's begin today's webcast: Fighting Financial Fraud. It's my pleasure to introduce your first speaker today and that is Kate Rush, Senior Vice President and Security Director with PNC. Kate, you have the floor.

Kate Rush: Hello, I'm so pleased to be with you today. We have two wonderful speakers in this series. We've got Miranda Creel, who's an executive Vice President in Commercial Sales and Treasury Management and Debbie Guild who is an Executive Vice President and the Chief Security Officer at PNC. For the next 30 to 45 minutes we hope to have an engaging conversation on identity and fraud for individuals in business. So, without further -- let's start with deeper introductions.

Debbie, would you mind sharing with us a bit about your background, how long you've been at PNC and some of your responsibilities.

Debbie Guild: I'm happy to Kate. Thank you so much, real pleasure to be here today. As Kate mentioned, my name is Debbie Guild, I am currently the Chief Security Officer at PNC. That's a combination of cyber security fraud and physical security. I've been in that role for about four years. Prior to that I was the Chief Technology Officer here at PNC where I ran the datacenters, the mid-ranger servers, mainframes, networks and user computing devices and such. Prior to that was 21 years at Bank of America and then a little bit of time out on the West Coast with Intel. So, really pleased to be with you today to talk about ways and tips and techniques to help avoid fraud.

Kate Rush: Terrific. Miranda, why don't you share your wonderful background as well?

Miranda Creel: Thanks Kate, hello everybody. I lead a team of treasury professionals and we focus on managing clients working capital within the commercial segment across the U.S. I have a combined 35-years of experience with PNC and Legacy National (inaudible). I've had roles as branch manager with the retail, I was the employment manager in HR and then I spent pretty much the majority of my career, 25 years in treasury management. However my primary focus is on helping companies and clients protect themselves against financial fraud. So I'm just excited to be able to share with you today as well.

Kate Rush: That's great. So, the focus today, as we've said, is identity theft and fraud and this is a topic that's top-of-mind for everyone. Miranda, as you engage with clients, you must get lots of these questions and, you know, hearing clients concerns and unfortunately probably see some of these incidents. What are some of the most common things that you're seeing in fraud today?

Miranda Creel: Interesting. The speed of the business continues to accelerate and the efficiencies of faster payments allow our clients to not only keep pace but stay ahead. So think about 81% of our clients have experienced fraud. The two biggest areas that I've seen has been social engineering which is also known as business email compromise and what that is, that's where a client is manipulated to divulge information and allows them to be able to send information out and really is not the individual that had the intention of actually sending that information in the first place.

The other area I find is check fraud. As we know, checks continue to be prevalent within our industry and we know checks continue to decline over time but they are still very well and alive as far as the bad actors are and actually getting clients to be able to either grab their checks in the mail, they wash them, they change the pay names. They've had the ability to create checks. So, I see those two biggest areas of fraud as really alive and well as I say today within the fraud area of the institution and the industry.

Kate Rush: Yeah, really scary moments for individuals when they experience those. Debbie, from your seat, you've got to see a lot of the dark side. What are some of the other hot topics that you're seeing that you'd share with this audience?

Debbie Guild: Yeah, you know, Miranda mentioned social engineering and we're seeing some of the old school techniques be incredibly effective when it's placed on top of a society that's sort of grappling with the pandemic. And what's happening is people are -- they're -- it's certainly top of mind to want to be a victim of fraud or to not want to be an identify theft victim but when you're presented with an article on a COVID [map] or perhaps a website where you can look at the latest updates on vaccines or enter in your information to donate to a particular charity because the world's going through so much, and so you have this empathy so you're leaning in with this empathy and so you're sort of forgetting the fraud optic and the adversaries, the threat actors as we refer to them, are taking advantage of that and they are putting malicious links in front of you. They are creating by the thousands, websites that are full of malware and they are hoping that you're going to act with a sense of urgency and act with empathy and, quite frankly right now, they're incredibly successful at that.

So, we are seeing a massive update kick in and what we call phishing, which are those emails with links, phishing, old school, pick up the phone, call you, ask you for your credentials and try to take over your account and initiate a wire. We're also seeing what we call smishing which is -- what comes over your -- you get it on your cell phone, you get a text and it's like, oh, let me click on that link because I don't usually malware on my cell phone and the next thing you know you either have malware on your mobile device or you've entered your credentials into a bad site.

So, we're seeing that in a -- you know, also sort of a, now, a very massively digital world, we're seeing the devastating effects of all the data breaches that have occurred over the past decade plus with things like Equifax where people's data, such as their social security number, their date of birth and where they work are now being used to do things like file for unemployment benefits on your behalf. And you know, and it's been a devastating effect, I think to our country when people from other countries

are out there filing for unemployment and leveraging real-time payments and money movement to actually get that money to other countries. And, you know, it's been I think devastating for a number of states here in the U.S. when that data has been used against them.

So, we're seeing a combination of definitely top-of-mind but when we're going through a seismic shift it's really having a really devastating effect on the fraud metrics and we're seeing a lot of activity out there right now.

Kate Rush: Yeah, Debbie, we're hitting on really hot topics, right, and it's -- when people are the most vulnerable that they --

Debbie Guild: That's right.

Kate Rush: -- can be preyed on, right? I shared with both you and Miranda that I started receiving checks to my house from unemployment on something I certainly didn't file for and was filed for on my behalf. So with these bad actors continuously evolving, with them preying on us when we're the most vulnerable and taking advantage of some of the political economic realities that are going on, awareness and education is so important. So, how do you stay current?

Debbie Guild: Well, I'll start. You go ahead, Miranda.

Miranda Creel: I was going to say, you know, what's so interesting is as we continue to educate our clients and have conversations and continuing to tell them about the things that they need to be aware of. I mean, it is still really critical for our clients to pay attention. And just real quick, just a couple of days ago, my head CEO, who had actually reached out to me because the CFO sent a wire and basically, as Debbie was talking about, the business email compromise on the social engineering side where the email came in to the CFO from the CEO saying, hey, you need to send this money. The CEO was out of town, the CFO did not reach out and try to connect with the CEO to make sure it was a valid wire and pretty much the money was gone.

And, you know, it's interesting because we continue to have those conversations and having people kind of think about when you get that email, stop. Because nine times out of ten if it's really something urgent, somebody's pushing you to do something, something has to be wrong and it's automatically a red flag. So, you kind of think about some things that you do from other -- educating yourself, having your conversations with your banker. Because the bankers are always willing to have those conversations and we do it all the time. But then also if you're reading, you're looking at what's going on in the news. The one thing that I always want to stress is to stop and nothing is that urgent that you can't really take five minutes or five seconds or whatever just to stop and reach out, pick up your phone, send a text, just whoever is asking you to do something, just confirm and make sure it's okay to do.

Debbie Guild: You're so spot on, Miranda. I mean, it's a very simple tactic and it was taught to me that this whole -- and it is a tactic because it's -- because you'll see it now that we talk about it, you'll see the act with a sense of urgency, circumvent controls, those type of things and when I was sort of younger in my career, I was taught this notion of defer to a higher power at some point, right? And if you say -- if you're on the phone and you say, you know what, I've got to make a phone call real quickly and you see it, we hear this actually on the recorded fraud calls. When somebody finally says, I have to

talk to my supervisor, my manager, the client, then they know they're owned. They just basically hang up because they know that they are -- out, right?

So, it's an important yet old school, non-tech -- you know, you think I'm a tech, right? This is all I've done my entire life, it's the most non-tech answer I give and yet it's the most effective in these situations. It's -- you know, place a phone call and I think the other thing that we have to do for our constituents is really make room for people to call us and ask us those questions and make sure that, you know, I think some people are like, well, if I call the CEO they might be mad at me, right? Well, guess how mad they're going to be when the money's gone too, right?

So, really making sure that people feel that sense of confidence in being able to make those phone calls and to question things and have a place to go to ask those questions. We have a dedicated 1-800 number that's 24x7, 365 where if somebody suspects that they're being, you know, vished or phished that they can call and actually get advice; literally like a counselor. Okay, so tell me what did they say and we'll help them figure out if they're being socially engineered. Like, literally, a helpdesk to find out, are you being socially engineered?

Kate Rush: Yeah, that's super helpful, Debbie. So, Miranda, I know that you've got an easy framework that people follow. You call them the five E's but it really helps to resonate and make sure that those items are top-of-mind. Do you want to share with this audience your five E's?

Miranda Creel: Absolutely and it's funny because I always think about the protection strategies and you kind of try to make it in the simplest way possible. So, I think about the first E as establish. Establish policies and procedures for the payment processes. Enforce. Enforce the standards that you've established. Educate. Educate your employees to recognize the warning sings. Empower. Empower your employees to question suspicious emails. Debbie had mentioned that before, it's okay. And I think sometimes you have to give your employees the right and actually the okay to ask questions at the CEO. Evolve and enhance. Evolve and enhance your risk to scale with your changing landscape because it continues to change everyday.

The fraud that we had five, ten years ago, other than check is totally different now and the fact that we're working virtually makes it that much harder because everybody's on their computer, looking at their emails, trying to respond quickly. Just again, go back to like stop and think before you move.

Kate Rush: Makes a lot of sense. So, Debbie, you probably have a lot of business owners that are watching today and probably curious how PNC has educated their staff and maybe some ideas that you would recommend to business owners as they think about educating their employees.

Debbie Guild: Absolutely. I mean, we have sort of the old school, what I would call the required training. So as you come onboard, you know, you're sort of trained on, as Miranda mentioned, some of the red flags. But the most effective training though and education is sort of meeting people in line with what's going on. So as an example, we do phish tests. We have a recorder, we send out a phishing email that is, indeed a text, and if you click on it, you do the wrong thing, we put up this splash page that goes, no, no, no, no! You got that wrong. You are about to enter your credentials into a watering hole so to speak. If you fail that test twice in a row, there's a

consequence model. You actually have to take a required training course at that point, which, again, makes sure that you're aware of what those phishing emails look like and then if you have what we call privileged access, if you have the ability to do things that can have a more devastating effect either on our systems or our money movement, we actually remove that privileged access until you demonstrate that you actually are able to cognitively decipher, you know, sort of good from bad.

The other thing that we did is we recognize that in the vishing example, people weren't able to understand when it was sort of that social engineering on the phone. So we very recently deployed a video where we played an actual vish in the video for people to hear. And it sort of had gone viral internally in a good way where people are like, okay, now I get it. Now I get those red flags. When you actually hear them, you know, in an immersive learning environment that is going to help make everybody much more aware of when that's happening and then at the end of it we said, call the -- if you're in doubt, call this number and phone a friend, right? And ask somebody to help you figure out what just -- what might have happened or just happened.

And then we try to make -- we do try to make security fun. We just partnered with the American Bankers Association on creating a whole bunch of social media videos and trying to help educate people on what this looks like. And then every October it's Cyber Security Awareness Month so we have a lot of fun with that. It's not just a bunch of cyber professionals sort of preaching at you for why you are a bad person for all the things you don't know. I get that this is very, very hard so we try to strike it with making security fun and approaching it with a phrase I like to call equal parts empathy and tough love. So, we get that it's hard to detect but you've got to detect it. It's important.

So, lots of things that mostly are trying to meet people where they are and, you know, give messaging and feedback in the moment and trying to make security fun which I get is not the easiest thing to do but we try hard to do it.

Kate Rush: I certainly think it's fun and I agree with you, hearing the vishing call live was so powerful. Being able to really understand how would I answer those questions and really put yourself in the shoes of the agent who, by the way, did a really good job, but it would be very easy to fall prey to.

So Miranda, you seem to have a horror story for everything. You recently had an experience with a client that had a ransomware attack. Did you want to tell the audience a little bit about that?

Miranda Creel: Sure. You know, what's interesting about that is, and, again, we always have the conversations and we're always telling clients, even sharing like what Debbie has, our organization doing that they can actually do the same with their teams as well. But, again, it was an employee. Pretty much actually this was just a couple of days ago. So an employee that was on their laptop, kind of in the system an email came in. They really didn't pay attention to it, they just clicked on it and literally the malware just pretty much consumed their system. Locked it up totally. And sometimes you kind of hear about -- I know years ago I used to hear about ransomeware and data being locked up and clients can't get to their data and it's really real. Because this one client literally the bad actors, the threat actor, had said, hey, I want $250,000 in bitcoin to release your data. And the CEO was like, what are you talking about? And then literally they could not have access to their data. What's interesting about it is there was a negotiation between the client and the threat

actor and actually got the threat actor to accept $10,000 in bitcoin. So, think about it, $250,000 in bitcoin down to $10,000 but still they could not get their data until they paid the $10,000. It's usually in bitcoin to release the monies before they release the data back to the client. And think about that though. So now the clients had that exposure, I can't imagine there's not other threat actors that are going to come at them in different ways because they know they've actually been able to hit them once, they'll try and hit them again.

Kate Rush: Yeah, that's exactly right and you're right. It seemed far fetched a couple of years ago. We did a simulation internal to PNC and now all of the sudden it's becoming more and more common in headlines and we're seeing that our third parties are vulnerable to that and so it adds the need for extra protection. So, Debbie, maybe talk a little bit about the trends that you're seeing but also what are some of the protections that companies can put in place?

Debbie Guild: You know, the things that I talk about are multilayered protection. So, when my kids ask me what I do, I say at a very basic level, I keep the -- which is customer data and, of course, financial money movement type of activities so try to make sure that that only goes out to the intended recipient and then I try to keep the bad stuff out. So, I describe my job in any given day as a very large filter. And you know, you have to have openings in your defenses because if you're not you wouldn't be in business, right?

But you have to have multiple layers of defense. Everything from your firewalls at the parameter to email filtering systems to making sure that you've got a good data loss prevention which is -- when your data is leaving your firm and, you know, so don't just depend on any one thing, it should be multiple layers and view the humans as a huge part of your defensive ecosystem. That's what I -- human education, that's why having these conversations is so important.

There's a cartoon that shows boxing ring and it has all the technology which is the firewalls, the demilitarized zones, the servers, the -- all of the massive amounts of dollars that we spent on technology to help in this sort of fight and then on the other corner it's -- and then there's Dave and you know so it's like my country for a horse for those of you who are literature majors. It's a moment where you want to have those multiple layers of defense but you also know that humans are a huge part of your defensive ecosystem and whether it's your customers, the corporations that you're doing business with or your employees, it's just a human part, a huge part, of the overall program. So, you can invest all that money and I encourage you to invest all that money but don't forget about the human factor.

Kate Rush: So, Miranda, if you could get a hold of Dave, that poor guy in the boxing ring and tell them anything, right, in terms of how he can participate in protecting that ring, what would you tell him?

Miranda Creel: I would probably say the one thing is, just making sure that you're utilizing the fraud potential tools because a lot of times people hear about, hey, you need to be thinking about investing in this or investing in a tool that can kind of safeguard your information but a lot of times we'll hear clients say, well, I haven't had fraud, it hasn't happened to me, I do all these different processes, procedures, I reconcile my accounts. So, I'm fine. But then as soon as the fraud hits [they're] the first one to pick up the phone, like hey, what about that tool?

So think about actually getting those fraud protection tools before it actually happens. I think the other piece too is just being able to empower your employees to question the suspicious activities that come about and not be afraid; to kind of come back and think about what are we doing, how are we doing it, why are we doing it and being able to have that conversation because that red flag is there. It's in your gut, you're feeling it but sometimes you don't want to say something because you're too afraid that your CEO or your manager will question like why are you asking me this?

So that would be my additional.

Kate Rush: Yeah; see something, say something, right? So that's even more real as we move into faster paces of business. We've hit on this a couple of times. Everything is speeding up. We all want real time decisions, we want real time payments. We want everything to be kind of that instant gratification and that's a great enabler for a lot of our business owners out there and a lot of our employers but it also opens up thoughts where there's added risk.

So talk about some of the considerations and advice that you both would have as you kind of think about doing business at the speed of light.

Miranda Creel: Yes, I'll start Debbie and I'll just pass it over to you. So think about understanding where you're sending your money to. Think about those -- and I know there's those of you who use Zelle personally and being able to kind of send money instantaneously and being able to -- once that money's out of the account, it's gone. But, they do have ways to try to help recover almost like you think about when you send out a wire and I know wires been out there forever. Think about that when you think about a real-time payment as well. Because, again, when a wire goes, its final, but we have the ability to at least reach out to our banking partners to ask for that money to come back if it is fraudulent but that's not always the case.

So as you think about even when you're sending a Zelle payment out, understand who you're sending it to. If it's a family member, relative, friend, but just make sure you understand where that money is going, double check before you send it because when the money's gone, it's gone. We will help you as your banking partners to retrieve that money but that's not always the case and we cannot always get that money back.

So, again, my one major thought that I want to share is, just make sure you understand who is receiving the money and then making sure that the data is correct before you send it.

Debbie Guild: Miranda hit the nail on the head. In any payment relationship with the -- I would say a modern payment relationship, there's three parties. There's the sending party, there's the clearinghouse or the [rails] or Zelle in that case, and then there's the receiving party. And it's important to understand where the liability, generally speaking, is relative to that ecosystem.

The receiving party is like, woo-ho, I just got paid. The clearinghouse is like we're just rails so we have no liability and it's the sending party that has 100% of the liability of getting that wrong. So if you are sending -- if you are -- you're about to hit that send button, if you're the sending entity, whether it's on your phone, Zelle, or whether it's in your role, you know, authorizing money movement, if you're that sending party you are likely 100% liability [to get it right]. So, it makes sense for

you to take that extra step to make sure that you've got everything correct to Miranda's point.

The other thing that's interesting in a real-time payments ecosystem that, as Kate mentioned, you know, societally we want the money to move fast, we want to settle faster, these are definitely societal demands that we have to keep pace with but up until -- before real-time payments we had 72 hours to do a lot of that claw-back. Now we have seven seconds. Is this something that we really want to go out and that's a really big difference. So, understanding where the liability is and now the speed in which we have to respond and be able to decide, is this a payment that's going to the intended recipient for the intended reasons, for the right amount, we have now seven seconds to do that where before we really didn't have more like a 72 hour window that doesn't exist anymore.

Kate Rush: Yeah, that's very different, right? So, as we talk about speed, its partner in crime, pun intended, sorry bad joke, it's often talking bout automation, right? And so as we think about ways to automate business processes, as we look to optimize the way that we use our working cash flow, making distributions easier, accelerating collections on topics that are front of mind for a lot of our business owners that are listening today. We've got to think about, you know, what that automation could do. So as you look for efficiency, what are some of those controls that you want to make sure that you don't automate away?

Miranda, any thoughts on that one?

Miranda Creel: Absolutely. So, you know, you try to think about automation and then that automate the controls away. So we're not trying to take everything away from you as the business owner, but let us work for you. So, I just want to share, we have a process called Intelligent Routing. So, what we can do is basically you just tell us where you want the money to go and we can decide how we send it so we can either send in a wire, real time payment, ACH, we can do same-day ACH. So then we take that off your plate, so you're not thinking about doing that at all. All you know you need to do is to send a payment and then we figure out how that payment is sent but then you get the visibility through your information reporting to be able to see it.

So just think about, you don't have to think of how you need to send that wire out or all the information you need to gather. Just as long as you have enough information for us to be able to determine how we send the monies, you should be fine as knowing the money's going and then basically we will send it the best way possible but then we also give you the opportunity to view it online so you can see how we sent it.

So in essence, we're providing that efficiency for you and let us take on the ability to be able to get that money moving.

Kate Rush: Yeah, so let the bank work for you, right? Debbie, you [just heard it out] as a coder right, so you know that hard coding anything is kind of the worst thing that you can do, right? And so as you -- as we think about process automation, how do we think about still achieving flexibility within that -- the efficiency goals?

Debbie Guild: Yeah, it's a really good point. So, what we have to now automate is the decision frameworks that are going to dynamically do what I call adjust the aperture. So, if you think about a camera aperture that sort of, you know, is smaller in certain lights and larger in less, how do we automate the decision framework that can detect when

money is moving for the wrong reasons to the wrong recipient and close the aperture when it's bad and open it when it's good. And that's what we've been investing in is really making sure that we had that dynamic aperture. It really came into play when we were distributing our -- the sort of federal funding loan program, the PPP loan program. The Payment Protection Program. And what we were able to do is say what's this signature that says that this is actually good money going to the intended recipient and we were able to program the aperture to be able to detect what that looks like on a recipient by recipient basis with some macro level controls.

And Miranda mentioned this, you know, make sure that you're not automating your controls away. This actually augments your controls and it allows us to basically ensure that the macro level controls are -- none of the recipients are going to be international. So we're able to sort of box that in. The type of payment that we would be expecting is sort of one per corporate entity, those types of things. We put some checks in that would allow us to, again, make sure that the good money was going to intended rate recipients and that we were, you know, good stewards of that process.

So we leveraged automation heavily to do that for the entire program to make sure that we responded very quickly to companies in dire need.

Kate Rush: That's great and a really good recent example from how the bank was able to help. So we've talked about you've got to kind of know who you're sending money to but we also know that we all kind of are connected in this Internet world, right? So we have a digital identity. What exactly is that and how should we be thinking about our own personal digital identity, you know, as we proceed forward?

So, Miranda, what is a digital ID?

Miranda Creel: So you think about a digital ID, it's a juicy target for bad actors. You know, it consists of varied pieces of information about you in digital form that when you put it all together it points to you. So this can be obvious like a social security number or a user ID, password or something less obvious like Internet search activity or online comment. So you kind of think about that digital from going from a social security number to a multitude of different ways that people are able to identify you. Even when you think about your thumbprint. Like there's all different kind of ways where people can identify who you are not just from a social security number.

Kate Rush: Makes sense. So, Debbie, how are we thinking about digital identity at PNC and maybe using that footprint, or fingerprint, to -- yeah -- to better --

Debbie Guild: Yeah, I think what we do -- I think what we're doing is we're pivoting from using some of those single factor -- what is sort of secret-based technology. So, i.e., what you know such as your social security number or your date of birth, your mother's maiden name, those shared secrets and we're saying, those had their time, they served their purpose but they're now not good enough.

And so what we're doing to prove you are who you say you are is we're leveraging three factors, right? So it's what you know, which are those passwords, it's what you have which might be a phone or a hard token and what you are which might be your fingerprints and your facial recognition, iris scanning, those types of things and what we're doing is we're codifying all of that in a token that resides with you on your personal device. So there is no longer this honey pot of data that you need to worry about being breached. So, like, i.e., your biometric data is never sent to a company

like PNC in this model. Your biometric data all stays very local in your device, it's your data, it's your device, you get to keep it. And once you authenticate we actually allow you to send a token to PNC that says that that authentication ceremony happened and it happened successfully and you want to now interact with PNC.

But the strength of that program is making sure that you have two of those three factors at any given time when you authenticate. The things that Miranda outlined have been good at identifying who you are, right? So, it's -- if you want to distinguish between Debbie Guild in Pittsburgh and Debbie Guild in Florida, I can give you the last four of my SSN, that's good for identifying me. But it's not good enough to authenticate me to authorize a financial transaction. That's a completely different relationship and that requires what we call strong authentication which requires at least two of those factors.

Kate Rush: Yeah, so as we give away more and more information about us, you know, it can create those strong controls because of the complex algorithms that we can create but you're also giving away a lot of your data. So, I'm sure that a lot of our clients out there have daughters and sons. Miranda, I know you have two sons, Debbie has four. What advice would you have for the next generation, for our kids, about safeguarding their digital identity?

Miranda Creel: You know what's so interesting to me is how much information is shared on social media. You know, it's amazing that even on Facebook, if you look on Facebook and individuals saying, hey, I'm going on vacation or I'm doing this or -- and I think that's where the challenge lies because you have to think about how much information you're sharing, who you're sharing it to because a lot of times you put it on Facebook or some of these other social medias; everybody has access to it.

Talk about a vacation that you're going on. Now you know that the bad actors know that -- okay, nobody is going to be home for this week or that week. So I would say, especially to the younger generation, think about what you're sharing and once it's out there, it's out there. So you want to kind of just keep some of the things maybe more personal and not share everything but I do get you want to be able to be on social media, be able to share things, being able to have people kind of connect and interact with you because that's how -- that's what we do today but just be thoughtful about what you share and how much you share.

Debbie Guild: That's good advice. So, for my kids, you know, we spend a lot of time -- so most moms teach their kids, you know, hygiene about washing their hands, and believe me obviously right now it's really important, I teach my kids security hygiene. So, you know, like is your antivirus up-to-date? Those types of things and I also practice -- you know, we talk about stranger danger, right and that applies online as well and it means, you know, if you got an email from somebody with that link, you know, and you don't know it, you weren't expecting it, don't click on it. Those types of things.

And what was funny is that actually parlayed into a conversation that we had with my kids at the dinner table one night, and they were like, mom, this is such a proud mom moment, they're like, mom, did you know that if you download the app TikTok on your phone and you -- you're copying and if you're pasting from your clipboard, they can actually read what's in your clipboard. Did you know that? And they literally, on their own, all deleted the TikTok app. They were like, that -- you know, and they get, they got, why that was an issue without me saying anything and it was just -- I mean, I was so proud and I'm sorry that I'm shocking all of you with your

TikTok apps right now. You're all like, what, what? What's going on with that but it -- you should research it if you haven't already but I love the fact that my kids are growing up security aware and it's a really important factor to know, Miranda, to your point, when they're actively giving it away but there's also a passive moment when you sign up for a free service that you might be giving your data away and you don't even know it.

Miranda Creel: Yeah, absolutely.

Kate Rush: Security aware, I think that that's a really takeaway from all of this. So, with that, our audience is made up of business owners and professionals. They serve those dual roles as both kind of the professional side as well as the personal side, maybe the CEO or CFO of their households, right? What personal tips would you provide as kind of final thoughts to keep professional and personal safe?

Debbie Guild: You start, Miranda.

Miranda Creel: Okay. So, you know, I would think about safeguarding your information and again, I kind of always talk about the fraud tools, utilizing fraud tools, because it's the one thing that we're always talking to clients about is being able to utilize those tools and ask about them. I know a lot of times for all your bankers, where you do your business with, should be talking to you about it. And if not, feel free to give us a call for sure. But they can show you how to set up alerts on your accounts and ensuring your employees are practicing smart social media because I think that's something that's really, really important but I think lastly, do not click on email when you don't know where it's coming from or who's sending it to you because your gut sometimes will tell you something is not right but then sometimes because we're all so busy and we're all moving at the speed of light, we go ahead and do it anyway, that's how you get caught.

Kate Rush: Debbie, I'll turn it over to you.

Debbie Guild: As you -- I'm going to be on panel with you all the time Miranda, you're just fabulous. You know, I think if I had to leave people with one bit of advice is, don't be afraid of just a little bit of healthy paranoia. Don't be afraid to ask the questions why. You know, as I mentioned, defer to a higher authority, phone a friend, get advice, we all need that and as much as Miranda and I are spending our days immersed in this, we still need to ask for help and to phone a friend and to seek guidance. It is hard. Sort of like, you know, you definitely want everyone to stay safe and we're only going to stay safe if we work together and leverage each other.

And so, first, congratulations for joining this session and I think that's the step in the right direction but reach out, form a network. There's people like us out here who are happy to have conversations. So --

Miranda Creel: Absolutely.

Kate Rush: Well, thank you both. I think this has been a wonderful awareness session but I'm going away with a lot of takeaways myself and really enjoyed hearing some of your personal stories as well as some of the battle scars that you both have lived helping to protect our firm and to keep our clients safe and educated.

So, thank you all for joining this session on fighting financial fraud and, as Miranda said, there's help -- and Debbie said, there's help available so feel free to reach out and continue the conversation. Thank you so much.

Debbie Guild: My pleasure.

Miranda Creel: Yes.