FRAUD TALK – EPISODE 106

Navigating the Threat Landscape in Today's Tech-Driven World

Four panelists from the 2021 *ACFE Women's Summit* session titled "Upping Your Tech Game in Times of Extraordinary Change" discuss the ever-evolving threat landscape and how it has affected fraud trends throughout the past year.

Transcript

Bret: Hello, and welcome to this month's episode of *Fraud Talk*. I'm Bret LaFontan for the ACFE. In a few moments, you'll hear an excerpt from a recent panel at the 2021 *[ACFE] Women's Summit* titled "Upping Your Tech Game in Times of Extraordinary Change." The panel of speakers include our moderator, Amber Mac, along with Amy Chang, Cynthia Herrington and Amber Schroeder

Amber Mac: I want to start with this question and I'll throw this one at you, Cynthia. What have you found to be the most challenging part of dealing with digital data when it comes to fraud investigations, and feel free to expand on that a little bit to some of the work that you're working on now.

Cynthia: The digital landscape is so fast and so changing. I think the hardest part is just keeping up when you're a user and not the producer. Our job as end-users is to stay on top of and current with all the data. We try to do our best with it, but we can't … I think if you can admit to yourself that you'll never be on top of it as much as you wish, then at least know what you know and know it well.

Then have friends like Amber who can help you through all the other pieces, or reach out to buddies like Amy, who can annunciate on a particular aspect of financial fraud and these particular accounting features in this new document. I've seen this over and over again with this system, and it looks like we're never going to be in front of it.

That's great because that means that we're progressing and we're marching forward. Never admit that you know everything in this field. You will be toppled like a bad set of Legos that aren't put together.

Then once you do get into the groove, I find my little trick here is teach what you've learned immediately because that cements into you whatever new system, process. It also asks you to start questioning whatever that system or process is just in case any holes in a software or system update aren't there. As you're teaching it, it'll become apparent. I find that to be very helpful in that way.

Amber Mac: Just as you were talking, Cynthia, it reminded me of a quote that I share a lot when I'm speaking at events, from Graeme Wood, which is that change has never happened this fast before, and it will never be this slow again. I think about that all the time with the technological change that we're experiencing right now.

Amy, I'll throw that one over to you. How do you know in this age of acceleration with technology, when is the right time to walk away from a tech application? How do you keep up on what other options exist out there as well?

Amy: Oh, that's a great question. I think when the overhead and the burden of a specific application becomes more work than the actual outcome of that work, then it's time to think, “There's got to be a better way to do this.” I'll keep that answer pretty short and simple is that if it takes more work to utilize a specific business application or tool and you're not getting that much out of it, there are definitely other tools out there that can help you.

Amber Mac: Amber, if I can come to you with a similar question in terms of when is it time to walk away or even just building on both Cynthia's point as well as Amy's, as far as just knowing that right time to pursue something different.

I think Amber is maybe frozen right now. If we want to add just if you guys want me to move along with the questioning, I will move along to the next question. I think this is a really good one and, Cynthia, I'm going to start with you. How do you connect current and upcoming technological advancements to your anti-fraud work? What would you say to that question?

Cynthia: Oh, well, we're always trying to find a more efficient way to conduct anti-fraud investigations and to stay informed to new fraud trends, especially during COVID. We're not meeting. We're having great conferences online with our fraud chapters and our international meetings, but you're still not having that one-to-one where you're like, “What tools are you using?” And “What do you guys up to?” Seeing the vendors, having those vendors in front of you, while they're pressing your news stuff. I spend a lot more time now reading literature and following the threads and the chat rooms to see what people are talking about and what they’re excited on.

I actually do — and I’m going to really hate myself for saying this — but when the vendor sends us unsolicited emails, I actually stop and read them now, just because it's like, is this the same old thing from last year or are they addressing an issue that we're really challenged with? I find that that becomes a good avenue. Like Amber said earlier, and I'm sorry she's frozen, but it happens. Right? Technology happens when you're trying to get the job done.

But she said it earlier. You've got to constantly stay in front of it as much as you can and what you can't, you just got to smile and walk through it.

Amber Mac: We all have tech challenges, right? And I think the more tech-savvy you are, the more challenges you have because the more you push the boundaries of what's possible. You never get to the point where you're totally comfortable, which is a nice lead-in to this next part of the conversation.

We're going to talk about the threat landscape as well as the opportunities that exist because of new and emerging technologies. Amy, I'm going to go back to you in terms of what threats are influencing the threat landscape right now and changing the way firms are defending against fraud.

Amy: From a fraud perspective, I think the movement towards fully digital solutions, you know, things that are away from username, password combinations, or even the use of account numbers, create this urgency to develop a way that we can get an understanding of the fraud landscape and how we can develop solutions to counter the potentially fraudulent activity that would stem from that. Then I think another challenge is that, it's been alluded to many times throughout this conversation, is as soon as we advance in our defenses, the bad people and threat actors are also speaking freely and they're collaborating and they're sharing and selling sensitive information.

They can do it with more impunity because we are bound by our legal compliance and regulatory mandates, as well as we have to interpret these guidelines that are given to us and are enforced upon us as well as in terms of how we conduct fraud, how we report fraud. Sorry, not how we conduct fraud, how we *counter* fraud. And how we report fraud and things like that. I think that to move more into the threat landscape, I think the ease with which individuals and criminal organizations now can get into a network or a person's account is evidence and showcases just how far that bar has been lowered for entry.

It's not just the large organizations like JP Morgans that are being targeted. They're targeting … you know, no one had heard of SolarWinds before December when it was compromised, and you look at the supply chain over time and that has been targeted continuously to try to get insights into. Because they're in the supply chain, they will be connected to other larger organizations and entities that have larger systemic value.

I think that also down the line where you can conduct small-scale fraud from these types of intrusions and things like that. But if you think about it on the large scale, and you also correlate that with the rapid rise of ransomware activity that's occurred over the past several years or so. Even just last year, there was a 700% increase from 2019 of ransomware activity. And that's just what's been reported. We don't know how many people have been paying off these organizations and entities. I think that all of these things really complicate the defender's perspective and influence the way that we that the way that we defend our organizations.

Amber Mac: Thank you for that thorough answer. I was going to check in and see if we have Amber back. Amber, are you back yet? Not quite.

So, Cynthia, I'm going to throw this one at you then in terms of some of the threats that you see today, as far as the threat landscape and how that is changing the way firms are defending against fraud, knowing, like Amy says, that it's not as though things are going to get easier and better overnight. It will likely just be more complex.

Cynthia: As we're going through the questions … and Amy, I think she really nailed it. I can't say it better and she's very much the expert in this part of the section on technology and emerging threats, but how do you learn about new tech that's coming at you? How do we deal with the threats that are on a platform? An email came through from a gal out in the field that I've known since the early 2000s, and she says, "Hey, Cynthia, have you ever heard of this company? They keep emailing me and other analysts. In this day of phishing and other scams, I'm hesitant to open up a response."

You know, I'm giving you my patent answer for "How do we stay on top of things" to be a good host and a good panelist. But this is the truth of it, Amber. I get to meet Amy, and Amy meets me and we know respect because we're both part of the ACFE. We've learned that we've gathered this intelligence over the years and respect each other. What happens? We communicate.

This gal that emailed me about a company that she's unsure of. She says, "Have you heard of them?" She's both leaning on me because I'm an expert in an area that can answer that question and b) because she trusts me and I'm a vetted expert to help in that area. I'm also a girl fraud examiner with her. That's really the truth of it.

I don't want to make it sound like we go through some sort of big process to vet this stuff out. When it comes down to the threat landscape and what we're being presented with today in my world, it's not just tech on tech. My threats are more along the lines of individuals being targeted and then exposed on social media accounts. We're hunting down anonymous posters, antagonists, disenfranchised terrorists. We're all over the map looking for people with old-school online detective skills.

When I need to know more about tech and specific technology platforms, I go to the tech experts like the other panelists, but when I need to throw on my cyber hat and get into it, you just do the job.

Amber Mac: Cynthia, maybe instead, building on that a little bit, what new tech, gadget or enhancement have you found that has come up in fraud enhancements? I know I'm talking about gadgets or enhancements, but just because you touched on social media. I thought that would be interesting, especially this is a space that I know pretty well, where many of the social channels are going into these spaces that aren't necessarily public spaces anymore. Can you talk a little bit about that changing world?

Cynthia: Well, it's funny because the software developers that are coming out and presenting to the social media awareness model. Some may call “monitoring.” There's so many. They're tripping over each other. Then the last, since 2015, there's got to be at least 20 companies that have come to market and are all pretty much selling the same thing. Then all it takes is a Facebook or a Twitter to change the API, and their software platform, you know, it wobbles a bit. What we've actually done … We use these tools because they make us efficient. They make us faster and better able to handle our client needs. Frankly, you really still need to know the fundamentals to get the job done.

You still need to know how to do searches directly. You still need to understand the platforms themselves to get into and understand because when the tools fail, you need to know how to do this. I ask accountants all the time. I'm like, “Great. You have five different software programs that will help you take large volumes of data and compress it into one report, but if you didn't have the software, could you still do it?

"Well, yeah, it'd take us longer." Well fine. The software platform is just whatever fits your needs so long as you're getting the end results that you find are factual and good for what you need, that's really going to be in the end result.

Amber Mac: Excellent. Amber, I think we have you back at least with voice. We've had quite a thorough conversation so far with Amy and Cynthia about the threat landscape, what's happening right now in terms of some of those threats, as well as what's taking place in social media.

Maybe I can throw that one to you just knowing that we have covered a little bit about some of the issues that exist right now, as far as the threat landscape, and your opinion on what threats are influencing the threat landscape today in 2021.

Amber: I think obviously … I'm hoping you guys can hear me because I'll be voice for the rest of the thing, the panel. I think the big change that I'm seeing is that so many more transactions in general are done almost exclusively electronically. The variety that's happening with, specifically with some of the fraud. I joke about like Venmo and everything else and the emergence of that for payment.

As you see different generations come in, I'm seeing a change in just how they're using that technology, how they're using it with money, how they're using it with their data. You look at generation Z versus I'm a Gen-Xer, and I have a totally different perspective on it than my kids do. It changed the way that I look at an investigation and the type of data I'm looking for based on the age of the person I'm investigating. That’s changed even more so now that everyone is remote and you're not seeing as much of each other. They're relying much heavier on that technology.

Amber Mac: I love that you brought that up, Amber, because that is the last question for this section before we move on to talking about opportunities, where to look, how to build your networks.

Amy, I'm going to start this one over to you talking about what Amber just mentioned as far as work from home and the shift that's taken place talking about things like unemployment theft, updated or creative fraud techniques. Can you talk a little bit about this new way that people are working and how potentially that has just totally changed the landscape?

Amy: When COVID-19 first hit and we were tracking a lot of the new fraud pieces that were coming up, especially with PPP and a lot of the other, a lot of the developments that happened within the United States, and you look at the correlated fraud that occurred after as well. A lot of it's still occurred in the tried and true methods, through phishing, vishing smishing. Vishing being voiced phishing, if you're impersonating someone over the phone, and smishing is over SMS text, things like that.

It's that they've adopted this theme of COVID-19, and rightly so, because it was scary and we didn't know what was happening. We were having a lot of different types of inputs of information from different sources. No one really knew what the clear picture was of the landscape from a work-from-home perspective. It was ripe for opportunity for these fraudsters to really take advantage of it. By capitalizing on COVID-19 in their email, their phishing emails, their spear phishes, and their links and their PDFs, and all of these things really amplified a lot of the fraud that we saw in the early to mid of last year when COVID first hit.

Amber Mac: I think that pretty much wraps up section B in terms of having this conversation around the threat landscape. I think just ending on that thought, Amy, as far as those changes, especially with work from home and remote work. Again, as I mentioned, that acceleration that's taking place, it's a good time to shift our focus for the last 10 minutes or so to talking about the opportunity that exists, more specifically just getting each of you to share your advice as far as those places where you go, whether it's a message board or Twitter account to follow what's happening and stay up to date on everything.

Amber, I'm going to with you how do you stay on top of all of those technological changes that are happening so quickly right now. Again, that are in really a state of being on fast-forward at this point.

Amber: I do have to say that it is terribly hard, especially where most of what I'm choosing to do every day and part of what we do in digital forensics is we have to find a way to investigate each piece of technology that comes out. It is overwhelming because there's so much of it. You'll probably laugh in the fact that one of the ways that I stay up to date on it is I actually talk to my kids, and I follow all of the people on Twitter. I follow all of the LinkedIn messaging and everything else, and I practice the technology by using it in my life to really understand it, but I'll find that my kids will end up finding out about a trend well before I do.

It's just that different generation of perspective that I brought up before. It makes a huge impact on it and I don't think that we maybe even talk to our kids. It doesn't matter how old they are. Your 12-year-old might know about one new thing that came out that way before you find out about it anywhere else. I know more about e-gaming now because of my son being competitive in those sports and what that landscape does and how much money goes through that particular industry. I never would have found out about that before. I've been motion six and video gaming for a very long time.

So these are things that as long as you have their conversation with the right people … I also participate with a lot of universities because again, a different generation and talking with them, offering for myself to come in and talk to their students. In return, the students to talk to me, I'm going to find out a lot just by opening that dialogue.

Amber Mac: I see that in my house, definitely with a 12-year-old at home, that he is always a little bit ahead, as far as the tech that he is using. I definitely have those conversations with him. While some of us in the tech industry may be obsessed with Facebook and Instagram or WhatsApp, he's on totally different platforms, a little bit ahead.

Cynthia, let's talk for a second about good habits that you follow to identify opportunities and resources to improve your tech savvy, whether that waking up in the morning, and maybe you have a routine of sites you go to visit or people you follow on social media. What are some of your habits that you can share?

Cynthia: I'm going to kind of riff right off of what Amber said, because I call her kids up, no. I talk to my staff. Much of my staff here is younger than me because I'm as old as dirt, and my analysts are all — I won't say their ages — but they're significantly younger, so they're using new tech themselves to stay apprised as to what their role is. They're also open source investigators so it's also their job, but they’re really using it for their own sake. I keep in touch with them and just regular communications with them.

And this platform here using Zoom, I'm getting in touch with … I used to be traveling every single week for training, every week. Now that we're all doing this all remotely, I get in front of a lot more customers and a lot more technology developers, a lot more sales reps, and even my own staff. There's 10 minutes, you could sit down in front of your own computer at the office. You'll make time for it. So I find that just being open to communications, my schedule is a lot busier because of it. I feel like I'm not actually getting enough downtime, but I am learning a lot more in this last year than I have in the prior five years. Being a leader, I didn't have time to learn.

So keeping my calendar open, listening to those who were younger, who were experimenting, and tapping into the vendors to see what they're developing.

Amber Mac: I love that you talk about just having that space and that time to learn. I mean, that's what we're doing today. Sorry, I'm full of quotes, but this one is from the late futurist Alvin Toffler. One of the things that he talks a lot about how people right now to be able to survive and thrive and really build their dream career, they need to be able to learn, relearn and unlearn and that is the path of learning. You learn something and then a month later you got to relearn it because it's totally different. Then you've got to unlearn that and you've got to move on.

Amy, maybe I'll throw this one over to you as far as that learning path. How do you stay on top of everything that's going on and knowing that we are in fact all online more now, especially during remote work?

Amy: It's insane. I think that Cynthia and Amber both nailed it in terms of just how quickly technology changes. Even though my job is to stay on top of the threats and technology changes, there's still so much going on at the same time that I'm not aware of.

I don't get to tap into Gen Zers as much, unless I've downloaded TikTok or something.

In terms of staying on top of everything, I think making sure that when I'm consuming information on social media, it's not that I'm just reading quotes from CEOs and things like that and other large-scale public figures.

But looking more at the people who are on the ground doing the work, dealing with the changes in the tech landscape, and talking about it because I think there's where you really get some of the insight into how technology is truly affecting people and how work is going to be done and how work is changing.

Bret: Thank you so much to our panelists. You can find more episodes of *Fraud Talk* at ACFE.com/podcast or wherever you listen to podcasts.