Bret LaFontan: Hello and welcome to *Fraud Talk,* the ACFE's monthly podcast. I'm Bret LaFontan, the head of video production and podcast for the ACFE.

At the 33rd Annual ACFE Global Fraud Conference, ACFE research manager Mason Wilder CFE, and Deputy Superintendent and Director of the Intelligence Unit at the New York Department of Financial Services Roderick Chambers, sat down to discuss the importance of technical controls and knowledge to protect your organization from fraud.

Mason Wilder: Just give me a brief overview of why fraud examiners need to be aware of current cyber fraud threats and trends.

Roderick Chambers: Fraud examiners should definitely focus and hone in on their cyber security skills and knowledge because we live in a remote workforce now. Everything that we do has a digital touch to it. Everything from our phones, from our laptops, the way that we even communicate with each other. Fraud occurs now digitally. We have phishing emails, we have vishing emails with a V that comes in via text message. All those are fraud techniques. I always like to explain to my fraud examiners that while we do learn professionally how to protect our license entities, we also can do it personally as well too, protecting our own devices, our own assets as well too. It goes hand in hand, professional and personal life protection.

Mason: One thing that I've really been trying to figure out the intersection of cyber security and fraud prevention. Have you had any success there, any recommendations for doing that cross-pollination?

Roderick: Absolutely. The intersection between fraud examiners and cyber security is that it's the medium, it's the devices that we use to communicate back and forth. Fraud, we look at fraud in the traditional sense. It was always on paper. You're going through investigations looking for the connections, clusters of data anomalies, especially with things like construction or procurement orders. We're looking for those anomalies in finance's accounting. Now that it's in a digital world and cyber is involved, a lot of those accounting mechanisms are done digitally, PDF files.

Big wins for the government civil service and private sector has been in healthcare with pandemic fraud. If you look at some of the metrics, billions of dollars have been stolen on unemployment relief, fake COVID-19 sites and domains, even donations from people like the World Health Organization, WHO and the Center for Disease Control CDC. All those aspects threat actors take advantage of those.

People are hurting, they want answers. They want more information and threat actors will take and manipulate those well-known reputable organizations for their own benefit. That's where fraud takes place. Many people are aware of unemployment fraud that occurs. All of that was definitely exasperated because of the digital world that we live in. To apply for unemployment benefits you couldn't go to physical locations. It's all done digitally online where certain controls are needed. Driver's license numbers, first name, last name, even social security numbers, trying to identify and confirm each of those individuals. That's where fraud and cyber

comes into play. Where now that we can no longer go to physical locations, where profiles are built online, the security of those, that's where cyber security comes into play. Fraudsters take advantage of this new efficient way of doing business. That's why it's very important for that intersection to be reviewed by both fraud examiners and cyber security experts.

Mason: One of the things that I've said on a number of occasions about pandemic fraud, doing interviews for newspapers that call these **[unintelligible 00:03:58]** or something, it's all about just contexts and adapting tried and true fraud schemes to different contexts. The pandemic was just absolute gold mine because it's just completely unprecedented in terms of an issue or an event or something that literally affects every single person on the planet. Every single person on the planet is aware of COVID or was aware of COVID and so that context that it's going to grab people's attention. That's just like turbocharging fraud efforts.

Roderick: Exactly. That's the number one thing that people look at is they're thirsty for information. They want to know who to talk to, where to go, what information is there. Threat actors, bad guys, or I tell people all the time, they're people just like you and me. They just have fancy names. We always tag them as threat actors or some of those factor terms APT41 advanced persistent threats or Fancy Bear. They're actually humans. They have ideologies, they have motivations, they have goals just like you and I. Whenever we look at those things, those are the things that bad guys prey on. Especially during the pandemic time for healthcare relief, unemployment relief, anything that mass people, especially globally, have a vested interest in resource and assistance, you can expect there to be fraud involved with that. Bad guys taking advantage of those opportunities.

Mason: What are the most effective ways that organizations can reduce cyber fraud risks associated with the new remote work environments?

Roderick: Absolutely. I'm going to always go with this element, training is number one. I work with a lot of executives and a lot of planning and budgets, and training always seems to get the lowest amount of funds. I think it's also that, no, it's not buying on that phishing training. I do a lot of competition between different business units. We have those phishing emails that go out and it tells you if you report it or not. It's nice to build competition. How did the marketing department do versus accounting? How did the accounting do versus IT? Training really builds in that muscle memory, that practice, they know people know what do you do when I get a suspected phishing email. Would my CFO send me an email that's asking me to release a check or PO, do they normally do that? Going through that training will prepare them for the real-time event. Training is number one on that one. You have to have that there.

The second one I would tell people to look at is that, because we live in a remote working world, there's a lot of third parties that are involved now. Third parties have taken our VPNs, virtual private networks that we look at, support for your laptops. Not even the fact that you have cell phones now that are provisioned for certain

access to government systems or private sector systems as well too. When we look at our third partner, our vendors, it's going to lean on them. Your vendors should be providing you training for these devices. They should be reviewing their security protocols as well how they respond to incident response. Leaning on your vendors, engaging with your vendors, just not bringing them on board.

Then lastly, continuing education for everyone from the leadership all the way down to your new entry-level staff members. This virtual training that's joining your information sharing analysis centers, information sharing analysis organizations, exchange information, cyber changes. You could almost say literally every day, so new threat emerging, other new attack vector emerging as well too. That'll be the next one. Training is huge step all the way down, leadership all down to entry-level. Then it's going to be now looking at your third-party vendors, looking at them as well too, evaluating them. Of course, technology as well to bring that on board.

Mason: Can you just walk me through the basics of what should happen when an organization determines that they either suffered a data breach or any kind of cyber fraud incident?

Roderick: We look at incident response planning when there has been a cyber incident, a data breach, even a security event. I always tell people I've hoped that you've done a tabletop exercise. I hope that you have practiced this. When an incident occurs, wrong time to deploy this. When you look at that, you want to bring in the right business units into the situation if a cyber event occurred and it's true. There's a lot of investigation knowing that you have to go out for your physical security, your IT security, your managed service security provider, your board if needed, your CSOs, bringing the right people to the table is the first thing that should occur. Meanwhile, each business unit has their operations going on. IT is looking at forensics through reviewing. You have your other IT group that's keeping operations flowing.

You can't stop operations from moving on. That's how you make money but at the same time an investigation is going on. You're bringing your shareholders, your stakeholders, your board members involved as needed, preparing for maybe a public relations message going out to those consumers impacted. Your attorneys as well who should be looking at cyber security insurance. It's been talked about quite heavily with ransomware and they're going to have to be a part of the incident response plan as well, reading and going through that fine print. What are my entitlements? What areas are we liable for and where can we leverage cyber security insurance to help us out?

When looking at incident response, first things first, you should practice this every year. Every single year you should run a tabletop exercise. Then two, bringing the right business units to the table to discuss the incident. The impact, how severe it is, if they need to bring anybody else on board.

Mason: Why would it be important for a fraud examiner or why is it important to have the anti-fraud perspective involved in incident response?

Roderick: Absolutely. Usually, with incident response, there's been a cyber security, a cyber event going on, and usually that's for fraud, gaining PII personal identifiable information, PHI personal healthcare information that we have going on. Fraud is taking place. We have to think about why did the threat actor gain unauthorized access to a system? What was their purpose? To gain information to deploy another attack.

A lot of times with fraud, we look at a financially motivated crimes, but there's also the run-in-the-mill espionage as well too, like SolarWinds and Microsoft Exchange that need to gather information for large nation-states. Fraud examiners come into play to look at, why did this particular threat actor go for this database? What was the purpose of taking the phone numbers or driver's license numbers, or even the Social Security numbers of this select database, because it's almost like a cookie, a trail of crumbs, one crumb that the next will lead you to in the line the big cookie that's out there, but fraud examiner can see those data points. They can put that analysis together.

A lot of times, these threat actors use recycled tactics, techniques, and procedures. Fraud examiners have seen quite a bit over time. They have seen where would Social Security members be used, where would driver's license numbers be used. They're able to look at that and contact the other sister and brother organizations that are out there to alert them, maybe an attack that's coming, maybe a fraud scheme that's being developed or continuously has been going on for quite some time. Fraud examiners have the ability to see the past, what has been useful, present, how that past actions by threat actors can be used now in a fraud environment, and hopefully begin to be proactive and predict what fraudsters will be doing with information in the future.

Mason: Do you deal a lot of tabletop exercises?

Roderick: For tabletop exercises, I promote them because, and part of New York state's Regulation 23 NYCRR 500, we do recommend a regulation to have annual penetration tests as well as incident response plans as well. One, I'm an advocate of telling small, medium, and large size companies to do tabletop exercises. I also help those small, medium, in business size, execute and deploy tabletop exercises. I think many times when we think tabletop, we think that it's an expensive endeavor. You got to call in a third party or a contractor.

Many times just by the creativity of your team, understanding, we're going to run through our process. How do we respond to an event, any event, and uncovering those security gaps? To me, it's not so much money or monetary effort, it's timing. How much time was a team willing to take, to develop a tabletop exercise, and then taking that process and repeating it, getting better each time. You can internally develop your own incident response and tabletop exercise, but a 100% advocate of

at least doing it once a year and then, of course, bringing your teams involved in helping develop these tabletop exercises.

Mason: What about, how do you think cyber fraud risks have really evolved?

Roderick: Cyber fraud risk in the last 5 to 10 years has evolved due to efficient technology. I'll tell people before we look at technology as being efficient, the easier it is to purchase something, the easier it is to market. It's going to draw people in there. With efficiency doesn't always include security in mind. We look at our study with the software development life cycle. We don't really build security in mind. We want our shareholders to see the benefit, they want to sell it, go IPO, and move on to the next one.

There's lots of security flaws. Even from just the idea phase, we should be embedding security at the very beginning, everything from the development of the app or the domain or the technology all the way to the end goal, because we live in this digital world and again, the pandemic really exponentially sped up this process, which we've evolved in probably the last 2 years faster than anybody ever thought in the last 10. The last two years have really expanded. We have apps just about everything and the apps were designed to keep businesses afloat. You couldn't wait 6 to 12 months to develop the app. You need the app now, we are now in pandemic lockdown mode. We need to get our product out there, develop it, deploy it and go. That had missing security flaws.

When we look at cyber fraud risk and the importance of it, it's expanded so quickly in a short amount of time, which is why cyber security professionalism and fraud examiners are really at a crossroads right now where our skills overlap. If you're really good at fraud techniques and you build it into a cyber technique, you've just really created almost a new position, very valuable position that's able to see both angles of that. Likewise, for somebody who's very talented as cyber security or IT work and can see fraud trends, you've now created a new position that's very valuable simply because efficient application, efficient technology. We as humans want things very easy and very quickly, forgetting everything with security.

If you ever reuse the same password, because you're just tired of building a username and password for an app, that's part of efficiency. We just want it now, we want it easy, we want to get into our account. We missed the whole security aspect. Why is it different and unique? When we look back in the way that we navigate our own lives as far as efficiency, we can begin to see security flaws, reused passwords and user names, using professional credentials instead of your personal credentials, going ahead and not updating your PCs, if you have PCs with antivirus software, or relying on things such as MacBooks, that don't require antivirus software thinking that it's perfectly safe but there's still threats.

In our personal lives, we circumvent security. Why should that change the professional setting? We're going to circumvent security there as well, too. It really is a good time that evolution of the threats that are out there, that go hand in hand with

technology, is bringing together fraud examiners and cyber security together to evolve the process.

Mason: Can you talk a little bit about what are the best ways for fraud examiners that might not necessarily have as much of a technical background, but are curious to do threat intel?

Roderick: Absolutely. Fraud examiners, when they're curious, just the first step, they're curious about cyber security, about IT. I like to encourage those rotational assignment, having a fraud examiner go to the IT department and just dedicate to work with them two to three weeks, learn IT, have them show them the ropes. Likewise, IT gets to go to fraud examiners as well too. Those that have the aptitude, have a desire, the curiosity, go to that unit and work two to three weeks. The cross-pollination of those work, those business units, will really help develop both sides on for fraud examiners and cyber security.

A lot of times it's do-it-yourself videos. You've seen it before, YouTube, your Google searches, and so forth. You learn a lot just by the instructions that are out there. It's funny when I tell people before, though threat actors aren't geniuses that come up with this on their own, sometimes there's basic tutorials and instructions on the internet. You can just Google search and find out how to do it, but it always starts when I tell the team that I work with and examiners, it's initiating the curiosity. If you're curious about the craft, I'm going to support that and I want to definitely grow that seed of curiosity. I think a lot of both private and public sector has to do is, begin to find those that are curious and then feeding that curiosity. You really can drive up the workforce and that knowledge pool as well.

Mason: Any other ones?

Roderick: Last point is, just continue learning, the education. Threat actors change tactics seem like every single day and they deploy all their changes on holidays [chuckles]. Pay your staff a little bit more on the holidays because we need them. Summer vacation that's when they usually spring up and do their work. That'd be the big point.

Mason: Perfect.

Bret: Thank you to Roderick Chambers and thank you for listening. You can find this podcast along with all other episodes of *Fraud Talk* on acfe.com, Spotify, iTunes, or wherever you listen to your podcast. This is Bret LaFontan signing off.

[00:19:28] [END OF AUDIO]