Regions Business Radio – Business Email Compromise

Speaker1: [00:00:09] It's time for a special episode of Regions Business Radio. Now here's your host, JD Mealor.

Speaker2: [00:00:18] Thank you, Mike Sammond. And welcome to Regions Business Radio. I'm your host, JD Mealor, and you are joining us today for the third in a three-part series on fraud. And today our topic is going to be about business email compromise. What a boring set of words. But you're going to learn that if you're not heads up on this topic, it's going to cost you and your business more than you can even imagine. My guest, as has been for the previous two episodes, is my friend Jeff. You know, Jeff, Jeff Taylor is not only a great guy, but listen to this title. The head of commercial fraud forensics at Regions Commercial Fraud Forensics. Jeff, welcome to the podcast.

Speaker3: [00:01:03] Thanks, JD. Thanks so much again. I appreciate the opportunity. It's so important. You know, we talk about business email compromise. And I think it's important to note that this has consumer impact also. Oh yeah. So sure, I mean if you think about it from a consumer standpoint, if you use email for communication, it's always possible that you would receive an unwanted email from a fraudster asking you to make a payment to somebody to some account or change the terms of a payment. So, while we call it business email compromise, because that's who it impacts the most, I think it's also important to note that it has consumer implications also.

Speaker2: [00:01:43] Well, my wife had an email today from some fraudulent PayPal thing. And yeah, she texted me with a picture of it and was like, what'd you buy now? And I was like, for once, it's not anything I bought. I didn't do it. You know, it's not a new set of golf clubs or anything, right? But I could look at it right away and say, honey, that's fraud. Don't even don't even reply. I was a little concerned that she may have opened it because she saw it. But email compromise, whether it's personal or business email compromise, email compromise is, as you and I have both learned, very deeply, you're in it far more than I am. But we've worked on a couple of projects in in our area where we have customers that were victims of business email compromise. Before we go into it, I took a note in our show notes about the fact that sometimes text can be compromised as well. Yeah, so it's not just, you know, Jeff taylor@regions.com. It could be, you know, 404 whatever.

Speaker3: [00:02:42] It could be phone calls. It could be text messages, could be email. So we typically call it business email compromise because of the way that the attack vector occurs. But it could come from any one of those communications. Well tell me what you know. Well, when you think about it, JD, with all the sophisticated attacks that are out there now that fraudsters are using business email compromise continues to be the number one attack vector. So, more companies impacted by business email compromise than any of the others. The Association for Financial Professionals does a survey every year. We talked about that in one of the earlier podcasts. In their most recent survey, 71% of the companies who responded to that survey indicated that they had been targeted for business email compromise. So seven out of ten companies have reported being targeted by business email compromise. So ic3.gov is the Internet Crime and Complaint Center. They're the central reporting agency for internet crime. Okay. Last year or in 2022, they indicated having over 22,000 reports of business email compromise impacting over $2.7 billion at risk.

Speaker2: [00:03:57] So we're going to repeat that 22,000 reports of business email compromise correct, costing those companies a total of two point $7,000,000,000 billion.

Speaker3: [00:04:09] That's right.

Speaker2: [00:04:10] And again, here I am, pausing to process those numbers and to think about the individuals that I know that have been a victim of this and how it goes down. How do you know? What does it look like? What does it sound like? Describe for us business or email compromise text. What is it? How does it go down? Jeff.

Speaker3: [00:04:29] Well, I want to say too, I don't see those numbers declining. So I think when that survey comes out this year in 2024, I think we're going to see those numbers even increasing because of the because of the attack vector itself and the way that it works.

Speaker2: [00:04:43] So is it is it so is it just easier to fall victim to it, you think?

Speaker3: [00:04:48] Yeah, it is. I mean, if you think about the definition of business email compromise is use of email or text message or phone calls to create a compromise of payment data that results in funds being transferred to an account controlled by the fraudster. So it occurs in a number of different ways. There are three basic attack vectors that you think about a number of different offshoots from each of these, as we can talk through those and think through them. But the first one is called executive impersonation or executive email intrusion. And this is where the fraudster poses as an executive of the company, or a trusted partner of the company to request that a payment be made. So it might be something like we are establishing a new vendor relationship, we need to pay some money up front to this vendor. And so I need for you to create a payment to this routing and transit and account number to solidify this relationship and get us started from a from the standpoint of payment up front. Yep, yep. And so what the fraudster has done is they reach out to an individual in accounts payable in the company. The email looks like it's coming from the CEO or CFO that trusted party or authorized party to make that payment. And so the individual in accounts payable makes the payment, creates the payment the way they think they're being asked to do so later on during the day, they see the CFO or the CEO in the hallway and say, hey, I sent that payment you said was really important, and it was had to be done today. And it was had to really be kept quiet and secret. So I did that for you asked me to do. And the CEO said, I have no idea what you're talking.

Speaker2: [00:06:36] The look on. I can just imagine the look on that CEO's face. You did what?

Speaker3: [00:06:40] I imagine the look on the accounts payable person's face. You know, the first thing they're thinking is I've got to get my resume together. I know that this is not going to turn out well for me.

Speaker2: [00:06:50] Yes. Somebody basically mimicked maybe, uh, impersonation.

Speaker3: [00:06:55] Yeah. It's impersonation. So the second one is what is called vendor impersonation or vendor intrusion. And in those cases the fraudster poses as a vendor, someone that's already an established vendor and says, look, we're no longer going to be banking with this financial institution that you've been paying in the past. We're going to now change our accounts receivable to another financial institution. So here's the new routing and transit and account number we're going to use. The other option is to say we're no longer accepting checks. We want to now accept a digital payment methodology or modality. Here's the routing and transit. We want you to send the next payment to. And so the email has been spoofed in a way that maybe changes the vision of the email or the construction of the email address to maybe transpose a letter, add a letter, use a Z instead of an S, I mean an uppercase I instead of an L, and depending on the font involved in the email platform, it's going to be really, really difficult to detect.

Speaker2: [00:08:03] Oh yeah.

Speaker3: [00:08:04] And so they pose as the vendor. They send that request to the to the accounts payable or vendor management department. And when that payment gets created it's going to an account controlled by the fraudster. So the third one is, is.

Speaker2: [00:08:19] That account opens somewhere else in the name of who they think it's going to send to?

Speaker3: [00:08:24] Sure. It could be an account opened in an LLC instead of an Inc. It could be in a name similar to the maker of the payment.

Speaker2: [00:08:36] At some point these fraudsters actually set up fraudulent accounts.

Speaker3: [00:08:41] Absolutely. They're called drop accounts or mule accounts. Sometimes they use those they sometimes their accounts that they've opened in that name. Other times they are just a mule account where they're using they've convinced an individual to participate, and they typically unknowingly. But sometimes they do know. But the transaction is going into an account that is owned by one of these people that is participating and don't realize it. And then they're instructed then to wire the money out to another account or write a check for that account for the amount that they're receiving. Wow. The third one, the third one is really is the one that that hits closest to home for most of us. And it's called employee impersonation or employee intrusion. And in this case, the fraudster poses as an employee changes the email address of the employee, contacts the payroll department of the company and says basically the same thing I'm changing my banking relationship, so please send my next payroll to this routing and transit and account number. So when payday rolls around, human resources and payroll has made the change in the system based on the email request. And they're sending that payroll then to an account controlled by the fraudster.

Speaker2: [00:10:04] Oh no.

Speaker3: [00:10:05] So when the employee payday comes around, the employee doesn't get paid. They call and say, what? What's the deal? Why didn't I get paid? And they find out then that that the department acted on an email that was fraudulent.

Speaker2: [00:10:21] You know, it's interesting because email as a form of communication is, is so inadequate in regards to personal communication, really, you know, it's just words on a screen. Sure. You don't get inflection, you don't get emotion. And a lot of times as executives, as business people, as members of a of a work community, you know, we've all experienced an email that we thought sounded right, that never came across to the person we sent it to the way we thought it would. That's right. Then they're mad at you and you're like, what's wrong? Well, you sent me this email. I didn't mean it that way. We think of email in that regard. But hear this same this same business tool of email is being taken over by criminals. But how do they get there in the first place?

Speaker3: [00:11:14] Well, it's just really unfortunate that you can't trust that communication. Yeah. Process anymore. I mean, you just can't trust email. You know, when you think about the free email services and the use of those, it's just not difficult for someone to acquire an email address that looks like yours with a letter transposed, or somehow other letters introduced into the email address. And we're so busy and we're so we're trying to work so hard and so fast to get these transactions processed that we may or may not notice that. And the fraudsters know that they meaning.

Speaker2: [00:11:52] An employee, an employee of a company. Yeah, exactly.

Speaker3: [00:11:55] And the fraudsters know that they play on that and they take advantage of that vulnerability. The fact that we're helpful people and we're going to try to do things that will help. And so they take advantage of that.

Speaker2: [00:12:09] Well, and I'm thinking about and it costs.

Speaker3: [00:12:10] Billions as we said.

Speaker2: [00:12:12] Easy. I mean even in our little North Georgia area it's millions. Yeah. I'm thinking about a situation that you and I both worked on, where it was initiated via text, and a victim thought they were talking to the bank and the criminals got access to their online banking system. It was it was horrible. Yeah. I mean, that's the only way to describe it is it was horrible for everybody involved. And they got access, I think, via text, you know, it was a it was a text sort of looking to have a wire approved and it just snowballs. Yeah. And it happens so frequently. How do you know that you're talking to the right people?

Speaker3: [00:12:57] I think that's what makes it so difficult. So in those situations, the fraudster, that environment you're talking about is what we call the trusted partner or imposter scam. That's a little different than business email compromise. Business email compromise is a little more anonymous in that that it's typically. Involving a spoofed email address or a spoofed text messaging platform. But it's just not difficult for a fraudster to create a phone number, a mask, a phone number to make it look like it's coming from a trusted party. Gotcha, gotcha. So, okay, from a text message standpoint, from the email standpoint, making sure or making those email addresses difficult to detect is something that the fraudsters are very good at. Okay. And, you know, they're also very good at moving the money. So they typically when those funds hit the hit the account, the unintended beneficiary is what we call a targeted account. Yeah. The target the when those when that money hits they're monitoring that activity. And they know when those transactions when that money is available to them. And then they'll typically in very short order move that money out into either another account that they control, or they'll even take that transaction and break it down into smaller dollar amounts and move it out into move the money out, then each of those individual transactions to accounts that they control just to make it more difficult to detect, make it more difficult to track.

Speaker2: [00:14:30] How does a victim find their money in recovery?

Speaker3: [00:14:35] Well, the obviously, the first thing you need to do when you realize you're a victim of business email compromise is contact your bank.

Speaker2: [00:14:41] Yes, please.

Speaker3: [00:14:42] Make sure immediately contact your bank.

Speaker2: [00:14:45] The sooner the better, the sooner the better. Every minute that passes by.

Speaker3: [00:14:49] Are, the faster you know or. And the faster you contact the bank, the greater the likelihood that that we can help. The unfortunate thing is that with all of the things that we try to do to help, to help recover funds, we're not always successful. As a matter of fact, in that same AFP survey that I talked about a moment ago, 44% of the companies who were victims of business email compromise, 44% of those companies were able to recover zero no dollars whatsoever that they were able to recover as a result of business email compromise. And 60% of those companies were able to recover less than 25%. Oh, wow. So the fraudsters are really good at this. I mean, they know that they can move the money. They've got a network of accounts that they are able to utilize to basically launder these funds and move them into accounts that they've got control over.

Speaker2: [00:15:47] And what did you call those accounts? Mule accounts. Mule accounts.

Speaker3: [00:15:50] Mule.

Speaker2: [00:15:51] In our experience working together, we were helping a client, a couple of clients through this. In one case, the fraud occurred from a Friday to a Monday. So over the weekend. Right. And the recovery process was probably more in tune with the statistics that you just mentioned from the AFP survey, the other incident that you and I worked on, we were notified within probably 30, 45 minutes. And the results were better. Yeah. Than the EFP. That's right. Survey indicated. So time is absolutely critical of the essence.

Speaker3: [00:16:30] Yeah, absolutely.

Speaker2: [00:16:31] What do you think about. And we talked about multi-factor authentication things like that within your sort of online banking or within your own financial and accounting systems. When this occurs what do you do about it.

Speaker3: [00:16:43] Well, while we said contact the bank, you need to make sure that you contact them quickly. You know, some ways to help prevent is to think about having dual control. So you want to have more than one person who is responsible for that payment. So, you've got one individual who can create the payment. And then a second individual who then approves that payment.

Speaker2: [00:17:04] Are the criminals typically requesting wire or do they request ACH.

Speaker3: [00:17:10] Originally back in, in the initial days of the popularity of business email compromise wire was the more the chosen modality for most fraudsters because of the finality of a wire, the speed at which a wire is typically processed, they felt that wire was a greater a greater opportunity. But I think more and more controls have been put in place from a company standpoint, on wire and from financial institutions perspectives around wire, so that the fraudsters pivoted to ACH. And when they oftentimes will embed a fraudulent payment into a batch of ACH payments to make it more difficult to detect. And so if you think about payroll, you may be paying 1000 employees. And only one of those or two of those may be the fraudulent an actual fraudulent payment. So it's very difficult to detect those. But dual control will definitely help in those situations because you've got. One individual who is creating the payment, and then that second set of eyes to review that payment and maybe ask some questions. So maybe that person who's responsible for the secondary control is going to ask the question about how did we get this information? I noticed that the banking instructions have changed. How did we get that information. And just again, not a fail-safe, but at least a way to notify and to evaluate and monitor those payments before they're ever before they ever leave.

Speaker2: [00:18:50] Yeah. And you mentioned this in a previous episode. You know, in our world of productivity, we got to be we got to be fast. We got to be accurate. We got to be always on. And a lot of times we feel inconvenienced if something changes and we have to exercise a greater amount of just intellectual curiosity when we see that things are changing or if something doesn't look like it used to, and that's just got to trigger some alarm within us that goes, hmm, you know, something, something doesn't look right. I mean, if you came home from your house and the front door was wide open, wouldn't you sort of wonder who was in there? You opened the front door of your business when you become, unfortunately, a victim of business email compromise?

Speaker3: [00:19:31] I think if you have sensed a common theme in all three of these podcasts, it's about education and awareness. Yes. So the more you educate individuals in your company about these fraud attack vectors, how to recognize them, things to be aware of and just thinking about, I need to be more cognizant of what that email address looks like, and I need to slow my process down and figure out, is this legitimate? Is this a legitimate request or not? Because I can promise you in many cases, your gut feel about that, about that situation is going to lead you to do a little more investigation into that request. How often? Just think about it, JD. How often do vendors actually change their banking relationship?

Speaker2: [00:20:20] I would think it's pretty rare, actually.

Speaker3: [00:20:22] Yeah, it doesn't happen that often unless someone.

Speaker2: [00:20:25] From my team is calling on them. If a Regions banker is calling on you, you should change the. That's right away. Right. Because we're going to look out for I interrupted you. I'm sorry. I had I had to make a little commercial for how I understand completely. We're going to take good care of you. We're going to protect you from fraud. So, yes, if it's moving to Regions, it's a good thing.

Speaker3: [00:20:43] I would expect nothing less. Yeah. I think when you think about the, the, just the likelihood of those kind of situations occurring very, very rare. Yeah. And you think about how a, how that the tone of the email, did it sound like the person that you've communicated with all along does the wording look right. How's the Senate structure? How are our words embedded in the email that just don't really make sense from a standpoint, from a communication standpoint. So just things like that to just to be thinking about and be aware of and, and in my mind, JD, being aware of these kinds of attack vectors make people think. And it's this is all about slowing down and being able to think through these requests before you originate that payment. Yeah.

Speaker2: [00:21:40] That is so good. That is so good. And don't look if, if, if the boss comes and says I want dual authentication or, you know, I want another set of eyes to approve this thing. Hey, you know, Mike, you initiate it and Jeff, you approve it. It's not a slight at anybody. It's about protecting the assets of the company. That's right. And beating the bad guys.

Speaker3: [00:21:59] Yep, that's exactly right. There are tons of different opportunities that are provided for this education and awareness. You know, we send emails to our clients on a regular basis, helping them to know what attack vectors, what what's what I call the vector of the day. You know, the things that are out there that we're that we're hearing about to try to help them understand what's what is what they're facing every day. Videos that we produce, podcasts like this, the information that we try to provide to help employees and companies understand what they're facing on a regular basis, and how these fraudsters are going about carrying this out.

Speaker2: [00:22:38] They keep finding new and innovative ways they do this, don't they?

Speaker3: [00:22:41] They do.

Speaker2: [00:22:42] I wonder if they have like an R&D group down at the, at the, at the local criminal, uh, criminal enterprise where they think about how can we deceive, you know, people more frequently and more easily? I guess they do.

Speaker3: [00:22:53] My guess is they do and they.

Speaker2: [00:22:55] Test it out. And when it works, man, they'll just they'll just hit it hard.

Speaker3: [00:22:58] They're definitely communicating amongst the criminal enterprise network. They know how to go about doing these things. They know which attack vectors work the best, how to go about penetrating or vulnerabilities around particular individuals and departments. But. In many cases. Jade. It's random. You know, they've acquired, uh, email addresses and they use those email addresses because they know if they get one out of a thousand, it's still free money.

Speaker2: [00:23:29] Well, their leads essentially in this world. Now, you mentioned something there that makes me want to ask a question. And what you mentioned was sort of what I heard you say. The indication was that sort of the criminals share best practices. I know that's do banks work together in the back office to identify, I don't know, individual's IP addresses? Do they work together to collect funds from one bank to the other? Absolutely. Is that common?

Speaker3: [00:23:57] Yeah. Oh, absolutely. I'm involved in a number of those groups nationwide where we work with other financial institutions. Okay. To not only talk about the recovery of funds, but also to talk about the attack vector itself and, and things that what are you doing to help, you know, how are you educating your clients? Because one of the most important things is for financial institutions to speak with one voice is what I call it. Okay. And it's using the same kind of terminology. It's helping make it as simple as possible for people to understand what they're facing and then recognize that, see those red flags and be able to recognize what, what this looks like and what the essence of this is to be able to help prevent it.

Speaker2: [00:24:43] This is such a good conversation. How is this isn't in our notes, by the way, how have these fraud vectors impacted the banking experience for commercial and consumer clients? Let me see if I can figure out another way to say it. Fraud has impacted banking to such an extent that we now have to institute maybe more protections. Maybe we have to ask more questions. Do you see that fraud is impacting account opening agreements? Do you see that fraud is impacting how we verify people on different systems? Does that make sense? I mean, absolutely, it's impact. We think of banking as something that should be quick and easy because the rampant voluminous fraud vectors to use that time again, it's impacting how we do business. Maybe that's a better way to say it.

Speaker3: [00:25:32] Yeah, I think it does, Jody. I mean, and I think it impacts all of those areas that you're talking about, because the more friction you can introduce into those kind of situations, the greater the likelihood is that it's going to slow down the process and potentially catch something. Yeah. That's true. Um, now you've got a balance that, you know, you balance the friction with the customer experience. And so you've got to make sure that that how we go about introducing that friction is not going to create a lot of negative impact on the customer experience.

Speaker2: [00:26:08] Customer experience, relationship bankers, commercial bankers, business bankers typically aren't in the loop of what's going on behind the scenes with criminal investigations, recoveries, and things of that nature. Fraud investigators aren't trained in customer service, and they're not they're not used to dealing directly with customers. There's a little bit of a there's a little bit of a disconnect about where responsibility lies with communication. How can clients know the best way to communicate with their bank when they've been a victim of fraud?

Speaker3: [00:26:45] I think there are two, two ways that I would say, okay. The first is when you know that you've become a victim, you've got to contact the bank. In many cases, you do that through contacting a client services group or someone who is available and schooled and knowledgeable in being able to, to help with remediating that situation. Yeah. From going forward, once you become, you know, that you're a victim. The second way I would think is, is working with your relationship banker, as you said, we're working really hard to try to provide the relationship bankers with as much information as we can possibly provide them.

Speaker2: [00:27:27] Okay.

Speaker3: [00:27:28] So that they're in the know, they understand what's going on. Unfortunately, JD, many of these situations, especially business email compromise, may take months to resolve.

Speaker2: [00:27:40] Yes, months. We've seen that. I mean.

Speaker3: [00:27:42] Yes, we have seen it. If you think about the typical payments and receivables cycle, it may be 60 to 90 days before the vendor notifies you that they didn't get paid. Um, now we're in a situation where we've got to do everything we can to try to recover. I think it's important to note that going back to the percentages of recovery, the opportunities for recovery, these things just take a long time. And so it requires patience and it requires while you need to react quickly. When you find out. You also have to have some patience on the other side to know that there are a lot of investigative actions that have to take place. So I would secondly say, when you talk to you, after you talk to the banker and let them know, contact law enforcement.

Speaker2: [00:28:31] Local sheriff's office, police department.

Speaker3: [00:28:33] FBI reporting it to IC3 gov.

Speaker2: [00:28:37] So can a can a commercial business or a consumer. Can they individually go to ic3.gov.

Speaker3: [00:28:43] Absolutely. As a matter of fact they need to we can't report on your behalf okay. Because we're not the victim. That's good. So the victim is the one who actually has to report to ic3.gov and complete that information. So it's really important that they let federal law enforcement know. In some instances, the faster that they can get involved the greater the likelihood of recovery.

Speaker2: [00:29:07] Are there any stories of the bad guys getting caught?

Speaker3: [00:29:10] Oh yeah. We see those more and more now. That's good. Yeah.

Speaker2: [00:29:14] We're I'm over here thinking these guys never get caught. I'm glad to know. They do know.

Speaker3: [00:29:19] There have been a number of cases that are you know, all this information is publicly available, but cases where individuals who were long time participants in business email compromise schemes were discovered and tracked down and identified in a lot of these cases, JD, we think about these being nation state actors or they're international actors. They're not domestic. But unfortunately, a lot of these a lot of this activity occurs domestically.

Speaker2: [00:29:50] Oh, wow.

Speaker3: [00:29:51] And so federal law enforcement then is able because if it is a domestic situation, they're able to better able to prosecute individuals who they who are who are they're able to catch.

Speaker2: [00:30:03] That's good news. Yeah. That's good news. In our show notes you have a question and we've already answered the question. But I want to I want to bring the question up because I've experienced it. It's the question is how do fraudsters deceive people into involvement? Um, the question is interesting because the victim doesn't know that they're a victim when this occurs, in my experience with victims of business, email compromise or impersonation or account takeover, it is traumatic. Yeah. The way you ask that deceive people into involvement. These people that are victims, the individuals I'm talking about, they're hard workers. They're early, they stay late. They take pride in their jobs. And when they fall victim, it's gut wrenching. It's heartbreaking for them. And I just want to touch on the emotional part of it because, you know, as the bankers in a room, we're going to talk about the numbers and the recovery. But I've seen firsthand the angst. Yeah. And the anxiety and the fear that comes from somebody that's been a victim of these fraudsters. And it's not fun to see. No.

Speaker3: [00:31:15] Absolutely not. And you think about the psychological aspect of that, as we mentioned earlier about, gosh, this is going to this is not going to end up well for me. I have cost the company a lot of money as a result of this. And so, you know, I think JD, in a business email compromise environment or attack vector, it requires a human to be involved. There's no if you think through this, there's really not a systemic way that this occurs necessarily.

Speaker2: [00:31:43] Oh good point. Yes.

Speaker3: [00:31:44] So it involves a human. So a human had to get that email. They had to receive that text message. They had to get that phone call and, and really had to become a participant in that transaction. Yeah. The fraudsters know that. They know that we are helpful people. They know how busy we are, like in the executive impersonation thing. We know the fraudsters know we want to impress the boss. Yeah. You know, they know we want to do. That's right. And because if you think about it, the way that these are often captured and pictured is that you mentioned the t~~h~~e case that involved late Friday afternoon to over the weekend to Monday. Well the fraudsters know that. And so they time they know what the payment cycles typically are. You know first and 15th right. You know we typically make payments on the first and 15th. So they know that. And they send that information late on a Friday. They do they know they create a lot of urgency around that request. This has to be done today, JD. It has this money has to go out today. And so all of that, combined with the psychological aspect of pleasing the boss and getting this transaction off of the off of your plate and off of your desk and get it done. Along with that urgency typically causes people to go ahead and react and not follow the kind of protocols that. We suggest that you slow down and investigate and evaluate whether or not this really sounds legitimate.

Speaker2: [00:33:21] Yeah, stop, call, and confirm. I mean, that's.

Speaker3: [00:33:23] One of the first red flags is urgency. If I get a note that says this has to be done today, then I'm going to have to question, does it really have to be done today? Yeah. You know, what is it about this that has to that makes it have to be done today? Yeah.

Speaker2: [00:33:40] Almost to the point that you really need the boss to come stand in your doorway and see them and hear them to know that it's legitimate.

Speaker3: [00:33:47] I say this all the time. It's a five-minute phone call. And if you pick up the phone and validate this, and I will get to this in a minute because it's one of the controls. But if you validate that, it's a whole lot easier to explain why I'm calling and validating this transaction than it is to explain a half $1 million loss.

Speaker2: [00:34:07] Oh for sure. Yeah for sure. And by the way, I think this is probably where you're going in regards to the controls. Please do not call the number in the text or the email. Right. Call the number that you know. That's right. You're going to talk to somebody that works at that location at that business. What other what other controls would you talk about?

Speaker3: [00:34:28] Well, we talked about dual control. You know, having the dual control process in place. You've got to establish what your risk tolerances are. You've got to establish as an executive committee. You've got to determine what do I do.

What's my what is my recovery plan. So as we talked about earlier, it's just like your business continuity plan. You've got to have a recovery plan in place to know who you're going to call. What are they going to do to help me recover? How much information do I need to provide to them? And contacts like executive management, your legal counsel, your insurance agent? I mean, all those folks we talked about earlier that need to be aware of these kind of situations, because it's going to be important as they help you to recover. I think the most important and the most impactful control that a that a company can put in place is something we call stop, call, and confirm. It's a play on words, a stop, drop and roll from. If you were the good old days. Yeah. If you were to be experience a fire. But we call it stop call and confirm and it stop your process. Pick up the phone and call the requester at a number that you know to your point. Don't call the number in the email. Don't call the number in the text message but call them at a number that you know and validate that transaction. Ensure that the request is legitimate. And again, it's a short phone call, but it will save you a ton of grief down the road if you would just put that control in place.

Speaker2: [00:36:03] What other what other we've talked before about, you know, making sure that all employees are aware, educated even to some extent probably tested on this content again business email compromise. You can find that topic at our YouTube page. You can find it on some of our resources at the bank. We'll go over that in a second. What else could you share about business email compromise? I feel like we could talk about this all afternoon. Exactly. Because we've not only my experience with you, but you've seen all the variations of it.

Speaker3: [00:36:33] Yeah, there's so many different ways that the fraudsters use this. And, and I think JD knowing that humans are involved, it increases that psychological aspect. It increases the angst involved. It's just a really, really difficult environment. And knowing that recovery is difficult to that, you know, these funds may or may not be recoverable or the stats.

Speaker2: [00:36:59] Tell us that they're not likely to be. And real quick, let's talk about why. Remember, Jeff mentioned over and over that when the funds leave your account, they go to the destination to the target account. And then they're distributed to mule accounts. And, and then they're distributed even more. And it's gone. The money is gone. Yeah. And, you know, heaven forbid you have you have a lady that's worked in the office for 20 years and she's been there every day. She even works when she's sick. She she's given her heart to this company, and she's fell prey to a criminal, and it destroys her heart. And now she's let the boss down, and that's so real. Yeah. And it can be avoided. You got to be proactive. You got to stop calling. Confirm. I would say that we're getting the point in this podcast where I got to say, your banker has to be talking to you about this. Yeah. In many cases, the banker may not have the answers or the ability to call the other bank and collect or recover, but we can get that process going. When you find out that you've been compromised, call your banker, call law enforcement, go to ic3.org or is it gov.

Speaker3: [00:38:15] Azure. Gov. Gov.

Speaker2: [00:38:16] Gov. Yeah log it in there. Jeff I'm impressed too that that you're part of a group with other banks to share ideas share information. Does that also allow for recoveries to transact a little more easily or. Okay. That's good. Yeah.

Speaker3: [00:38:34] Just because you have those contacts and know those individuals that other financial institutions that there are processes in place. I mean, there are there are systemic, repeatable processes that all just about all I shouldn't say all most financial institutions use to be able to process a request for return of funds when they know it's fraudulent. But anything all the information you've got helps. So oh.

Speaker2: [00:39:00] That's a great point. And in the in the instances that that we've shared, it's really important for you to collect, write down, dictate into your phone all the information times, names, how it happened. We want you to avoid this situation by being aware. We're begging you to be aware, but in the case when it does happen, collect the information. It may be traumatic for some, depending on their, you know, how they approach it or the thickness of their skin, so to say in regards to difficult things. But collect the information, write it down.

Speaker3: [00:39:38] Oh yeah. The more you can provide to law enforcement, the greater the it enhances their investigation. I saw a case the other day, JD, where the company emailed the email domain was like XYZ company.com and all the fraudster did was add an s at the end. So if you think about that, that's misspelled number one. But it was XYZ companies with is at the end.com. And that's all they did.

Speaker2: [00:40:03] Incorrect.

Speaker3: [00:40:04] Exactly. But the individual the victim didn't pick up on that. And so as a result they went ahead and sent the transaction. It's a very simple way to play on our desire to help and that business.

Speaker2: [00:40:20] The boss as you mentioned. That's right. You know it. It all comes at us so fast. Yeah. The data that comes at us, all the media that comes at us and stop calling confirm is really a good little mantra to have. You should we should have stickers and put it on people's computers or something like that. Closing comments on business email compromise.

Speaker3: [00:40:41] You know, I think to your point, I mean, we could talk about business email compromise for a long time. And I think it's important to note, as I've said before, all of the things that we've talked about and the remediation techniques we've talked about, none of those are going to keep you from becoming a victim 100%. Yeah, because the likelihood of becoming a victim is when you think about the number of emails that are received on a regular basis, our dependence on the email for business communication, all those things and those factors, the fraudsters know all of that. And so as a result, they are going to continue to use those platforms and those communications protocols to try to carry this out. So education and awareness is so important. It's creating that fraud awareness mindset to think about is this right? Does this seem right or does it not. And you said.

Speaker2: [00:41:35] Before trust your instinct.

Speaker3: [00:41:36] Exactly, exactly. You know, I always say this about from a consumer standpoint, we talk about consumer scams and, and fraud is that, that if the deal seems too good to be true, it's probably it probably is.

Speaker2: [00:41:48] Yeah. That's right. Well, Jeff, we can't thank you enough. You know, if you're listening to this and you need help, if your banker is not talking to you about fraud, then you can ask them about it. If we can help you, we're happy to do that. If there's an opportunity for us to serve our business community in some way by bringing this content, whether it's Jeff and I helping you out, maybe through a webinar or our Next Step program has content, we mentioned our YouTube page. Additionally, you can find resources on our websites at regions.com/stopfraud, regions.com/fraudprevention, and www.doingmoretoday.com under the financial wellness tab. We mentioned it before in a previous episode but I feel obligated. Also stop ransomware.gov is a resource that may contain continuity plans. Sure that you could use in this situation. Jeff I don't know if you realize it or not, but episode three. Episode two. Episode one. You're helping people by sharing your knowledge.

Speaker3: [00:42:58] That's my passion.

Speaker2: [00:42:59] And you're good at it. Thank you. And you're a good friend. You're a great banker, and you're an asset to our clients. People don't understand. They don't realize that there's a Jeff Taylor that's helping them. So on their behalf, let me say thank you. And for those listening today. Let me say thank you for listening to Regions Business Radio.

Speaker1: [00:43:22] Regions Bank, member FDIC equal housing lender. This information is general in nature and is not intended to be accounting, legal, tax, investment or financial advice. Regions believes this information to be accurate when recorded, but it cannot ensure that it will remain up to date, consultant, appropriate professional concerning your specific situation. The information should not be construed as a recommendation of a specific course of action for any individual or business. All Regions products and services are subject to qualification requirements, terms, conditions, fees, and credit approval. Regions reminds its customers that they should be vigilant about fraud and security, and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices. As the threat evolves daily, there is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit regions.com backslash stop fraud or speak with your banker for further information on how you can prevent fraud.