Lowenstein Sandler's Insurance Recovery Podcast: Don't Take No For An Answer

Episode 71:
Call Me, Maybe? The Stealth Disappearance of Social Engineering and Fraudulent Instruction Coverage

By Lynda Bennett, Eric Jesse

AUGUST 2023

Kevin Iredell: Welcome to the Lowenstein Sandler podcast series. I'm Kevin Iredell, Chief Marketing Officer at Lowenstein Sandler. Before we begin, please take a moment to subscribe to our podcast series at lowenstein.com/podcasts. Or find us on iTunes, Spotify, Pandora, Google podcast, and SoundCloud. Now let's take a listen.

Lynda Bennett: Welcome to Don't Take No for an Answer. I'm your host, Lynda Bennett, chair of the Insurance Recovery Practice at Lowenstein Sandler. And today I'm very pleased to be joined by my co-host and partner, Eric Jesse. Glad to have you back, Eric.

Eric Jesse: Hey Lynda, thanks for having me back. Good to be here.

Lynda Bennett: Hey, I have a question for you, Eric.

Eric Jesse: All right, what do you got?

Lynda Bennett: Are you a huge Carly Rae Jepsen fan?

Eric Jesse: I don't know if I'd say huge, but maybe if no one is in the car, I might sing along to a song or two.

Lynda Bennett: She has a one hit wonder. What was her song again, Eric? I forget.

Eric Jesse: Yeah, Call Me Maybe.

Lynda Bennett: Call Me Maybe.

Eric Jesse: I need to admit I know that.

Lynda Bennett: Well, Call Me Maybe is the perfect table setter for the conversation we're going to have today about the stealth disappearance of social engineering and fraudulent instruction coverage. Now, for our listeners who may not be familiar with what that jibber-jabber means, social engineering and fraudulent instruction, what I'm talking about is that text message that you get that tells you that your Netflix account has been frozen, and you need to send a payment somewhere. Or back in the old days, the King of Zimbabwe needed

help getting a judgment that he secured, satisfied, and paid. Or maybe it was even the managing partner of Lowenstein Sandler at five o'clock on a Friday afternoon telling you that he needs a thousand $500 gift cards immediately. You got that email, didn't you, Eric?

Eric Jesse: Yeah. You weren't supposed to respond to that?

Lynda Bennett: No, you weren't.

Eric Jesse: Just kidding.

Lynda Bennett: So today we want to talk about insurance coverage that is, or I might have to say, used to be available for those kinds of claims.

Eric Jesse: Yeah. So Lynda, why don't you tell our listeners, so let's start, let's set the table, is there insurance coverage for these types of social engineering scams, the kind that you've described? The request for the gift cards.

Lynda Bennett: So for now I can say yes, and there are generally two places to look for that type of coverage. The first place to look is in your crime or sometimes it's called your fidelity bond policy. And that policy historically was designed to protect against employee theft actually. And as these types of scams started to develop, this coverage was added by endorsement to the crime policy because I think because the tie to the claim getting started had to involve your employees being negligent or getting duped and falling for the scam.

And then as standalone cyber policies came onto the market and started to really gain traction and develop, this type of coverage was also added into those policies. And that was very clear coverage in those policies. But I have to say, as we always do on Don't Take No for an Answer, that you have to look everywhere. Because in fact, I recently handled one of these scams for a client and they actually had coverage embedded in their errors and omissions policy, another endorsement that added not full coverage for the type of fraud that we were dealing with, but it did add some additional limits.

So we can't ever forget that when you get a claim presented, you literally have to look at your entire insurance program to make sure that you're not leaving coverage on the table. So crime, fidelity and cyber are your main go-tos, but make sure that you look at your other policies too because there can be endorsements added that provide this coverage.

Eric Jesse: Absolutely, yeah. You don't want to be leaving coverage on the table if you can find it somewhere. Now you're talking about these different policies. Is the policy language in the crime, the fidelity bond, the cyber, are they all created equal? I bet I know the answer but please tell us.

Lynda Bennett: You are an excellent student of Don't Take No for an Answer, Eric. Of course not. The policy language is never the same. We always have to look very carefully to see what the scope of coverage is for any type of claim. And in this particular context, these policies and some of the differences that we've seen is it may only cover losses that relate to vendors or customers, or the employee has to be involved. It can't be someone that you're in a contractual

relationship with. So the policy language differs very significantly for this type of coverage. And, we're going to get into it in a couple of minutes, it's ever-changing. So this is a coverage that you really need to have careful eyes on as your renewals are coming up this year, next year. We're seeing a significant scale back in the coverage that's being provided.

Eric Jesse: Yeah, absolutely. And I think the way I would describe it is with, because the words do matter and the words can vary from policy form to policy form and endorsement to endorsement, it's critical that policy holders make sure that policy is right sized to the nature of their business so that there's no gap. Now you mentioned crime and cyber as two main sources of coverage. Now I'm just curious, as between those two, where do you generally prefer to see the social engineering coverage? Would you rather have it in one type of policy over the other?

Lynda Bennett: I think that the broader coverage that I've seen is actually still sitting in the crime and fidelity and it's fine to sit there. My expectation, though, is that it's going to end up getting moved over into the cyber form because the insurance industry is still trying to figure out how to manage all of the new and different scams and how it fits within the insurance program. We talk about it all the time on this podcast that an insurance program is really a patchwork quilt and one of your main goals is to make sure you don't have holes in the quilt, but the carriers are trying to figure out where they want this to sit.

And it sits right now in crime, as I mentioned, one, because it involves employee negligence and two, it involves a first party loss. It's loss of the policy holder's money. And the cyber policies are more of the hodgepodge regulatory third-party claims and business interruption, the shutdown from the hack that came that allowed the scam to happen in the first place. But I think that ultimately it will port over to the cyber policy so that all cyber-related risks will sit under one roof, if you will.

Eric Jesse: Yeah, I agree with you. I mean, we've worked on claims in the past where we've tried to get social engineering coverage under a crime policy that was very clearly covered. And I think you have the crime claims handlers still stuck in the 1990s where they were insuring the forged check and that's not really the risk of the day. So I think the cyber policy claim handlers are much more just tuned to the cyber risk. So I agree with you that that coverage is going to transition over. All right, so since you have companies of all different sizes, industries, geographies, they're getting swamped by these types of claims, no one's really immune, how are the insurance companies reacting?

Lynda Bennett: In a phrase, not well, not well. The core of the problem is that it is companies of every size, shape, industry, geography, and many companies have had more than one claim at this point. And COVID really didn't help. As we all transitioned into work from anywhere and started using our own devices, it really created quite an opening for scammers and fraudsters to have success with these types of claims. So when this first really started to take hold, and actually let me back up. Probably five, six years ago, you would have very healthy, if not full limits available for this type of a scam. And then as these scams continued to proliferate and got larger, the insurance industry reacted

by putting sub-limits to the policy. And a sub-limit means, so when you look at your declaration page, if you have $10 million of coverage, when you went to look at your social engineering endorsement on your crime policy, what you might see is they'll only cover up to $5 million or $1 million, something like that.

So we started to see more and more sub-limits, and then as the claims continued and as the nature of the claim pivoted, as I mentioned at the top here, went from scanning the employees saying it's the managing partner law firm, now it's gotten far more sophisticated. They're posing as your vendors, they're getting onto your systems and sitting there for 200 days to see who authorizes checks and wire transfers and all of these things. The carriers have now really brought those sub-limits down significantly. It's not uncommon now to see a $250,000 sub-limit, which is certainly going to leave you underinsured for many of these types of scams.

Eric Jesse: All right, so in addition to the sub-limits, take us through, that was a few years ago, what are you seeing more recently?

Lynda Bennett: So what I'm even more concerned about, and this is why I mentioned at the top as well, we're seeing a stealth disappearance of this social engineering and fraudulent instruction coverage, is carriers are not putting exclusions on the policy. Right now, you will be hard-pressed to see a fraudulent instruction or social engineering exclusion in any policy. They're being far less transparent about it. What they're doing is saying you can have coverage for social engineering or fraudulent instruction as long as somebody has orally verified the change in the payment instructions. Or they may even say, "Hey, you have to do independent verification of the change in payment instructions."

So I think here an example might be helpful. So Eric, you are one of my suppliers. I have to pay you every month a hundred thousand dollars for services that you're providing to me. And I'm the person in charge of issuing that wire transfer or that manual check every month to you. I then get an email that appears to be from you except there's actually three S's in your last name, Jesse, not just two. And I don't notice that. And you tell me, "Oh, we used to use Bank of America, but we're now going to start using this bank in Spain. Here are the new payment instructions." And I don't pick up the phone and call you and say, "Hey, Eric, are you sure that you want me to start sending this money to the bank in Spain instead of the Bank of America?" I don't do that. Well, if my policy requires me to orally verify the change in payment instructions, I don't have coverage. And Eric, please make the obvious point.

Eric Jesse: Yes, that's exactly the issue these policies should be designed to insure against, the negligence, the risk, right? What's the point, right?

Lynda Bennett: Right. If I orally verify the change in instructions, I will find out I've been scammed and not send the money. There's other language that says that you need to have independent verification. And I was involved in a claim probably about six months ago now, and this is one of the core problems of our digital society that we live in, it required independent verification. And the person

who received the change in payment instructions very dutifully sent an email, a separate email, to the person saying, "Got this change in instructions. I'm going to need a bank verification letter that this is real." And they sent an email.

Well, they sent the email to the scammer, who still had control of the email system and people didn't realize it. So they got a very official looking bank letter and everything looked up to snuff and sent it out. And that carrier denied coverage because the independent verification isn't sending an email back to the person that sent you the original change in payment instruction. So these words really matter and you really have to be careful on renewal looking at this because a lot of these carriers are stealthily taking this coverage away and by the way, not reducing your premium while they're taking away the coverage.

Eric Jesse: I'm shocked. I've never seen that movie before. Well, all right, so let's see. What can our policy holders do to manage this risk if the insurance coverage for it is eroding? What can they do?

Lynda Bennett: Well, unfortunately, I usually like to have an insurance policy answer for our clients. My very first piece of advice though, on this particular risk, is you've got to invest in training your employees. For this particular type of claim, your employees are your weakest link. And that's not to be critical of employees. We all get literally hundreds of emails a day and trying to continue to play whack-a-mole with your inbox all day long is very challenging for every one of us. But we really need to be vigilant in training every one of our employees, but particularly the employees that are in charge of sending money out, paying your vendors, suppliers, customers. For those of our clients that hold money for other people, you really need to have the people trained up very well. You need to have best practices in place that there can't be any changes to payment instructions without live human contact. We actually have to go back to using telephones and picking up the phone and speaking to somebody live and in person before you're going to make a change to any type of payment instructions.

Second, and again, this is not an insurance solution, but it is a risk management solution, there's got to be continued investment in firewalls and monitoring traffic on the computer systems. As I mentioned, one of the things that stands out to me with these claims in particular, it is amazing how many days these scammers spend on our clients' email systems before they actually execute the scam. They're very patient, they get on there and after the client has done the recon of where did the breach happen, how did it happen, what we find out is that these scammers have been on the system for over 200 days!

And what are they looking at? They're looking at who are the people responsible for sending and receiving wire instructions. They are looking at the internal chain of command. So who are the people that are giving approvals? They look at the language that people use, how do they talk about approvals, so that when that email comes in, it looks and sounds and seems perfectly fine and normal. And so I'm just going to bounce through that very quickly. So getting better firewall protection in place and keeping those

hackers off your system is a significant risk management tool. And last... Go ahead, Eric.

Eric Jesse: Yeah, I was going to ask, is there an insurance solution that you see here? What would you advise our clients to still do on the insurance front?

Lynda Bennett: Well, on Don't Take No for an Answer, we have a few bedrock principles. First one is read your policy language, read the policy language. Eric, you made reference to it a couple of minutes ago. Insurers are denying these social engineering claims on a regular basis. And the facts matter. The policy language matters. And so when you get a denial, you got to call us because we have had success in getting carriers to pay. And as you said, particularly on the crime policies, you have claims representatives who don't even understand how these policies work, or how this endorsement works to their policies.

Eric Jesse: All right, well, we're almost out of time here, but Lynda, I'm going to ask you just last question here. Why don't you take a look into your crystal ball? What do you see in the future for this coverage as maybe the cyber market is starting to soften a little bit? Do you see it coming back?

Lynda Bennett: I think that we've got a real problem having it come back, unless the training and the firewall protection and the other risk management tools get put in place and are effective. It's going to be a challenge. What about you, Eric? You going to take the opposing view?

Eric Jesse: No, I think you're right. I think there needs to be this widespread risk management that addresses this issue. And I think once the carriers start to see that, maybe that will relax these requirements. But I think it's going to be a little while before we get there, but time will tell.

Lynda Bennett: Well, if nothing else, we're going to have everybody humming Call Me Maybe for the rest of the day.

Eric Jesse: Yeah, exactly.

Lynda Bennett: Thanks for joining me, and we'll look forward to seeing everybody next time.

Eric Jesse: Absolutely. Take care, everyone.

Kevin Iredell: Thank you for listening to today's episode. Please subscribe to our podcast series at lowenstein.com/podcast or find us on iTunes, Spotify, Pandora, Google Podcasts and SoundCloud. Lowenstein Sandler Podcast series is presented by Lowenstein Sandler and cannot be copied or rebroadcast without consent. The information provided is intended for a general audience and is not legal advice or a substitute for the advice of counsel. Prior results do not guarantee a similar outcome. Content reflects the personal views and opinions of the participants. No attorney-client relationship is being created by this podcast and all rights are reserved.