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

Episode 31 -
Wait, that's covered? Insurability of Fines and Penalties Flowing From a Cyber Security Breach

By Lynda A. Bennett, Mary J. Hildebrand CIPP/US/E, David Anderson CIPP/US
JANUARY 2022

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 here at Lowenstein Sandler. And as we kick off 2022, we have to pick up where everything left off. We've need to start talking about cyber related risks, security breaches, and the availability of insurance covers for that. So we know that companies have come a long way in terms of getting their insurance policies in place to provide coverage in the event of the inevitable security breaches and hacking events that too many companies of every size, shape and industry have.

They've also started to understand that constant vigilance and training and spend on security upgrades are essential to minimizing the impact of the inevitable security breaches and hacking events. But unfortunately for our clients and our network contacts, hackers have come a longer way in terms of always seeming to be two steps ahead of what is considered to be state-of-the-art security and finding new and even more intrusive ways into our systems to inflict pain, chaos, and costs to come from.

But that's not what we're going to talk about today. Our focus is going to be that third leg of the stool. What are regulators doing to incentivize companies to avoid security breaches and to prompt reporting, hacking events in a timely manner? We're going to dive into what the current state of play is regarding what fines and penalties are being imposed.

And then we're going to transition to the important question of whether insurers are willing to provide coverage for those fines and penalties today. And whether they'll continue to do that in the future. So I'm very pleased today to be joined by my partner, Mary Hildebrand, who heads up our Privacy and Cybersecurity practice group here at Lowenstein Sandler.

And I've got David Anderson, who is the US Head of Cyber at McGill and Partners. So Mary, welcome and thanks for joining us.

Mary Hildebrand: That's my pleasure. Thank you very much, Lynda, for having me.

© 2022 Lowenstein Sandler LLP
The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.

Lynda Bennett: Happy to have you and, and David were very happy to have you back. You've joined us, uh, once before to discuss the world of cyber insurance, but you're with a new company.

Tell us a little bit about what's going on with you.

David Anderson: Lynda, thank you so much for having me. I love having these discussions with the Lowenstein team, going down these rabbit holes, they are dangerously fun. I just joined McGill and Partners in November of 2021 to lead the charge here in the US for cyber-related risks.

McGill is a really, really cool company. We're really focused on tough to place risks. Working with clients who have unusual exposures, if you're thinking about energy clients, aviation clients, aerospace, which is sort of a topic de jour these days is also a big focus of ours. And then obviously cyber. Our goal is not to be everything to everyone, but really bring the specializations to the table. If it's something that we focus on and, and I'm happy to just sort of bring that to the table, to you all today, as we talk about cyber-related risks.

Lynda Bennett: Well welcome. I mean, it really is a perfect transition. Talk about hard to place. We're going to get to you in a minute, but, uh, but I'm going to start with Mary. Let's kick things off with you.

I've heard that it's pretty much the wild west out there in terms of the approach that local, state, federal, and international regulators are taking in terms of assessing fines and penalties against companies that suffer a security breach. Do you agree with my assessment and if so, why? And if not, why?

Mary Hildebrand: Lynda, I agree with you a hundred percent from where we sit—which is as after-the-fact guests, various disaster involving security breaches, and significant data leaks and ransomware attacks—the regulatory landscape changes I used to say weekly. I used to say daily now sometimes it's hourly. In the United States, we have 50 different data breach law, actually it's 54, if you count Puerto Rico and the other territories.

So over 50 different data breach laws. Individuals are entitled to whatever rights they're recorded in the states where they live. And those same laws determine the obligations of the companies that sustain the security incident. There are also in the United States specialty, federal statutes. That deal with specific industries or specific types of data.

The two easiest to remember are HIPAA with respect to protected health information. And of course, uh, the Greenleaf Bliley act for financial services, I would be remiss not to mention the Cybersecurity Act in the state of New York, which governs banking institutions, all of these statutes encompass a variety of different civil compensation, including fines and penalties. The state of California also offers individuals a private cause of action in the event of a data breach. And that is notable because even if there is no economic or emotional damage, folks who are entitled to statutory damages there. So that's important in the various states, we're seeing little tiny tsunami, which is

© 2022 Lowenstein Sandler LLP
The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.

going to grow of state laws as the legislature stepped into the void left because we have no federal privacy law.

Canada has a very well-developed privacy law, um, and also defers to their provinces on certain things. They have also a, now a national data breach law with penalties and fines assessed. Um, Europe of course is what everyone thinks about in terms of large fines. Those can be anywhere up to 4% of gross annual revenue of an organization.

I think it's also important to mention in terms of the fines and penalties, we tend to think of that in monetary terms, there is also an economic cost associated with loss of the use of the data involved in these breaches. And many times that's just a loss that's accepted, but the data loss, especially for our commercial organization can be significant.

And for companies that have been found to have caused a data breach because they violated applicable data protection. Among those penalties can be the loss abuse of the data.

Lynda Bennett: So Mary, let me jump in there though. So what are the regulators trying to do through the imposition of these fines and penalties?

Is it really an intention to punish? Is it an intention to deter? Is there any compensatory element to what the regulators are doing through this process? What's driving this?

Mary Hildebrand: All of the above. In my ideal world, everyone would coordinate. And the law that might pass in New York State would be aligned with the law in California, or perhaps in Canada, maybe Europe, nothing of the kind is happening.

We have new laws really globally. There's a new law in Brazil. China just passed a law there. Singapore, South Korea, all of them have really comprehensive laws. There and throughout the United States, the regulators have different goals. I would say it's punitive most of the time. I think there are situations where the regulators are perhaps more thoughtful about it and they pick particular situations to pursue in order to create examples for the public in terms of what they need to be looking for. But you know many times…

Lynda Bennett: Yeah, let me interrupt you there, Mary. So what is a company to do when they're facing a regulator and they're getting the vibe that this is more to set an example for others? Are there things that can be done to negotiate that fine down? To plead your case? To demonstrate why you shouldn't be the poster child that's going to get hammered on that?

Mary Hildebrand: I think I would highly recommend being, uh, being proactive and presenting to the regulators and the powers that be all the different things that you've done internally and externally to protect against the incident that's bound to occur and, you know, and go for your company in some fashion.

So that would mean not only incorporating and continuing to monitor security measures, including I think prominently encryption. Significantly, particularly

© 2022 Lowenstein Sandler LLP
The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.

in California, for example, encryption as a defense to civil causes of action and extremely, um, you know, persuasive with the regulators. But be able to demonstrate paper is fine.

I've seen many clients, my goodness. They have just beautiful policies. Have they ever read them or implemented them, or maybe done a dry run or a tabletop exercise and figured out how in the event of a data breach, they're going to keep so many important work streams running simultaneously. The answer is a resounding “no”.

So you can pay your lawyers for beautiful policies. I got plenty of them and you want the policy at the bottom, but none of it is going to do you any good unless you know what they mean and you can demonstrate that you have followed them and you are really attentive to it. So I think demonstrating the absence of, I was going to say the absence of negligence but demonstrating, you know, attentiveness to the issues I think can go a long way.

Lynda Bennett: All right. So Mary you've got us good and terrified. David, let me turn to you. We need insurance like STAT. What kind of insurance is available? And again, I want to particularly focus on the fines and penalty aspect here.

David Anderson: Yes.

Lynda Bennett: I'm just going to start at the highest level. Is there coverage for that?

David Anderson: So there is, right. There definitely is the ability to, uh, to purchase coverage in the marketplace. You can, you can seek it through just the traditional cyber policy, right Lynda, where you just have to make sure that the privacy, regulatory fines and penalties ensuring agreement is part of the insuring agreement. So you've purchased for those that don't know a cyber policy is generally going to be modular. So you'll have the ransomware insuring agreement, the business interruption insurance, pretty much. You got to make sure that regulatory fines and penalties box is checked on the policy as well. This is a really good…

Lynda Bennett: Hold on Dave, I want to pause right there because cyber policies require the secret decoder ring. And a lot of companies don't read their policy until after the breach. So say what you just said again, about regulatory fines and penalties. What do they need to look at?

David Anderson: So you need to make sure that on your quote where your binder or whatever your document is that you're looking at affirmatively has a coverage rate for regulatory fines and penalties associated with a data breach.

If it's not checked, if that box isn't checked as part of the coverage, you're going to have not a chance in hell to get coverage at all, but we can sort of jump down the rabbit hole, negotiating, getting coverage for that too.

Lynda Bennett: No the point I wanted to make. Cause it's one of our bedrock principles here at “Don't Take No For An Answer”: you better read that policy before you have the loss. So let me ask you this though, Dave, when, when a client has done it, right, and they've got the fines and penalties box checked, is that a

© 2022 Lowenstein Sandler LLP
The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.

box that's going to be capable of being checked as we head deeper into 2022 here and it's 2023.

What's the appetite of the carriers to continue to offer that coverage as Mary keeps telling us that the risk, the risk profile is growing every single day and it's the wild west and they don't even know what risk they're underwriting at that point?

David Anderson: Sure. So I think that we heard some rumblings about insurers getting a little tired of seeing regulatory fines and penalties discussions, frankly, Mary and Lynda, just the defense costs in terms of defending these investigations and inquiries, insurers are getting tired of it, you know, fortunately…

Lynda Bennett: Mary likes to get paid. I'm just saying.

David Anderson: Sure, absolutely. The ransomware scourge that we've seen over the last 18 to 24 months has kind of made regulatory fines and penalties, a little bit of old news, which is good. And I think that fundamentally cyber was developed as a liability policy. So it would be a little bit disingenuous for the insurers (as I get hate mail from them now) to carve out that coverage really, cause it sort of cuts one of the legs off with the policy. The other thing that I would add, and I'm going to ask for your forgiveness ahead of time, Lynda, for going as far in the weeds. Remember, most insurance policies are written to cover fortuitous events.

So while your policy will absolutely say yes, regulatory fines and penalties are covered, a lot of the policies will draw the line at the intersection of moral hazard and your data. So unauthorized collection, undisclosed monitoring, any of those sort of gray area data practices that you see, you will definitely have a harder time getting your insurer to just immediately acquiesce to cover those fines and penalties. Whereas if you are truly able to demonstrate to that privacy regulator and say “Hey, this was a zero day vulnerability that we didn't have time to put in place. We really were a victim here. We weren't collecting information from people without their consent.” You're probably going to have a better time A), to Mary's point, convincing that regulator to not make an example out of you and B) getting the insurer to cover that final penalty, because you're not going to run into any unfair or deceptive trade practices exclusions. Which are there. And I think we'll always be there. The work around for that sort of discussion if you're talking about a regulator saying that your fines and penalties are not insurable like ICO or GDPR to Mary's point is to buy a fines and penalties or punitive wrap in Bermuda. I've only ever placed one in my career.

And I don't think they've been tested in the marketplace yet, but that is where people go for employment practices punitive damages, general liability punitive damages. So if you're that concerned about it, there, there is a marketplace for it.

Lynda Bennett: And you see, loyal listeners, this is why we need Mr. Dave Anderson on our team.

© 2022 Lowenstein Sandler LLP
The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.

He's got the creativity. He knows how to get you to the places that you need. So hopefully get that coverage, but, but Dave, you're really touching on something that I think is interesting about the coverage that's available today under cyber policies. And it does overlay with what Mary was talking about, which is, and these are all bedrock principles, listeners, for “Don't Take No For An Answer”: The facts matter. The policy language matters. The reason for the imposition of the finer penalty in the statute matters. And these are all things that you need to carefully consider before you have your first conversation with that regulator to start framing up what is going to be your case, what is going to be your plea for leniency?

Um, and how does that overlay with your insurance? All right. Well, we've got just a couple of minutes left here, so I'd like each of you to identify the biggest change or impact that 2022 is going to bring for us with respect to this fines and penalty issue. Mary, I'll kick it over to you first. What do you think this is on the horizon for us as we start this new year?

Mary Hildebrand: I think when companies given the global nature of business these days, when companies sustain a data breach, it is becoming every day that when we look at the universe of data that's been impacted, they will come from not only the 50 states, but from multiple countries as well. So you're going to see enhanced complexity in terms of response and also multiple layers of potential fines and penalties.

Lynda Bennett: Right, Dave, I hope that you're going to say your biggest impact is going to be, you're going to get coverage for every single thing that Mary just said, but I'm not going to prejudge your answer. So I'll throw it over to you.

David Anderson: We'll try our hardest, but Mary is exactly right. That's going to be, that's going to be hurdle.

Number one, the complexity of a global environment is going to continue to change the battlefield on which you're trying to seek coverage. I think that underwriters will continue to try to distance themselves from having to decide whether or not a fine or penalty should be covered in the guise of some sort of gray area or moral hazard.

So for example, with CCPA, there is a private right to action. There's also the statutory fines within that statute as well. If it's a rising out of a four fortuitous data breach, I think underwriters will continue to stand behind covering those fines and penalties. But if it's arising out of, you know, shady, unlawful, or deceptive collection of data practices, we are seeing exclusions are already on the policy now for the privacy, regulatory, fines and penalties, when it's arising out of unsavory data practices.

And I think that's going to be the key accelerator in terms of how we get a couple more hurdles in the complex environment that we’re in.

Lynda Bennett: Well, that's great. I really want to thank both of you. You've covered a very complex topic in a very short period of time and really given some wonderful tips. And I think given us some great suggestions for things to look out on the horizon.

© 2022 Lowenstein Sandler LLP
The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.

And we're certainly going to have you come back and we're going to see if your predictions were true. So thanks for joining us today. Thank you, Mary. Thank you, David. And we'll see you all next time.

Kevin Iredell: Thank you for listening to today's episode. Please subscribe to our podcast series at lowenstein.com/podcasts, 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. It is not legal advice or a substitute for the advice of counsel. Prior results do not guarantee a similar outcome. The 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.

© 2022 Lowenstein Sandler LLP
The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.