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

Episode 27 -
Takeaways From Recent Claims Against Mark Zuckerberg and Facebook – Mitigating the Heightened Risk of Privacy Suits Against Individual Directors and Officers

By Lynda Bennett, Kathleen McGee, Joseph Saka, and Garrett Droege
NOVEMBER 2021

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: Hello and 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 am very thrilled to have three guests with me to discuss some of the legal liability issues that are swirling around Facebook. We are very honored and pleased to have Garrett Droege with IMA Financial Group, he's the director of innovation and strategy. So, welcome Garrett. Thanks for joining us today. I've got my partner, Kathleen McGee, who is in our White Collar Defense and Tech Group. Welcome Kathleen. And, I've got Joe Saka, who is Senior Counsel in our Insurance Recovery Group and a wonderful policy holder advocate. So, as I mentioned in today's episode, we're going to be talking about that swirl of legal liability surrounding Facebook. We've all been following this now for a couple of years, and we know that regulators have been very actively looking into some of the trade practices that Facebook has engaged in.

Facebook is also facing a number of consumer protection suits. And, many of us saw in the last month or so that they now have added employment litigation to their list of legal concerns to have, as a whistleblower left the company with a cash of documents that included some very difficult emails for Mark Zuckerberg to have to wade his way through, that has potentially expanded the circle of liability for him to face personal liability. So, that's really what we're going to be focusing in on today. And, looking at not only what is the nature of that personal liability that he faces, but because this is an insurance recovery podcast, we're also going to be talking about potential insurance that may be available to address some of those legal liabilities. So, I'd like to start today with Kathleen. Why don't you give us an overview of this new development with Mr. Zuckerberg facing personal liability? What are the nature of the claims and what's he looking at here?

Kathleen McGee: Absolutely. And, thank you so much for having me today. It's truly an honor to be part of your podcast. So, this is a really interesting update from the district of Washington, DC, from their attorney general's office, Karl Racine, who

had, along with several other attorneys general in the United States, opened investigations into Facebook, surrounding their partnership with Cambridge Analytica. Which we all remember fondly from around 2018 to 2017. But after engaging in several years worth of depositions and discovery, the Washington DC attorney general's office decided that they were going to name Zuckerberg personally. And, they did that because they said that they saw real personal knowledge and personal control over actions taken involving Cambridge Analytica. The knowing element here is really important. And so, I want to just take a step back and talk about the statute under which there are operating.

Kathleen McGee: Virtually, I think every single attorney general's office in the United States and its territories is going to have some version of what's called UDAP law. It's an unfair and deceptive practices law. The FTC has their own version of that. And, that was in fact used in part and parcel to pursue Facebook several years previously, that was that famous $5 billion dollar fine. So, here when Washington, DC decides to pursue Facebook, they're doing it under their version of a UDAP law, it's DC's Consumer Protection Procedures Act, which requires truthful information to consumers. And like most UDAP laws, it's a broad umbrella. You can fit a lot underneath it.

So, here they're taking a look at whether or not Facebook made truthful disclosures to their consumers about their privacy practices and how their data was being used. Most broadly, Cambridge Analytica is not the only instance that they're going to be looking at here, but it was certainly the most famous. And, what they're basically alleging in a nutshell is that, Facebook and Zuckerberg who had personal knowledge and helped to control this program in particular, understood and knew that on the face what they were representing to consumers about those glossy big type letters, how we use your data was not in fact the practice. And it looks like, they have information now sufficient to add him to the banner.

Lynda Bennett: So, Kathleen, let me interrupt you there and ask, why is this a game changer though? Is this a game changer, because there was an administration change and the regulators are more focused on individuals, or is it really particular to what Facebook was doing and what the regulators are trying to accomplish in the social media space in particular?

Kathleen McGee: So, it's not so much a change in regime from Washington, DC's perspective, but I think it's a product of they're having conducted extensive discovery over a period of years, getting deep into the documents, and then taking a look at the really scope and breadth of their alleged harm. And, if you see that there, what they I think are claiming, is really alleged deep harm to consumers in DC, with respect to their privacy, and real hands-on knowledge from an executive, they're going to put those two together.

I'm going to note some of the articles that have been written about Washington, DC's latest action here. And, it just took place in October of 2021, are that the Washington, DC law allows that jurisdiction to sue individuals? Well, frankly, all UDAP laws do. As individuals and corporations, you can just be an individual running your own corporate entity. This piercing of the corporate veil though, and going after Zuckerberg independently as a

defendant is unique, in terms of larger corporate. I'm going to call them cross executions for UDAP infractions. And, I think it signals a willingness to hold executives accountable when they are personally liable for things that they know or should have known are misleading or deceptive. And that is going to have broader implications, especially now that there are more and more indications, for example, board members and executives have to sign off on things like data security policies for companies, and those sorts of things.

Lynda Bennett: Yeah. So, that was going to be my question. If I don't have Zuckerberg's balance sheet, and I'm serving on a board, am I okay? Is he just a big juicy flashy target here? Or, if you're serving on any board, do you need to have a little bit of a chill going down your spine that this step is being taken to assert personal liability?

Kathleen McGee: I think it really depends on how much you're rolling up your sleeves and getting involved with something that or should have known would be perceived as deceptive by government. So, let's just start there. But, I do think that this should be a wake up call for boards and the C-suite that it's time to make sure that your practices and procedures are aligned with law. Especially, where laws requiring that you sign off on practices. When I think about financial or insurance companies, for example, where those boards have to sign off on privacy procedures in order to comply with Gramm-Leach-Bliley, that's a great example of where those executives and board members need to make sure that they are holding their companies accountable and that their knowledge is reflective of lawful action.

Lynda Bennett: Great. Well, that's a good segue too. So, Mr. Saka, tell us about where insurance lies and the middle of all of this? Are these directors and officers going to be safe in the assumption that if they do get sued, their insurance company is going to immediately step-up and defend these cases?

Joe Saka: Never assume that you're definitely going to be covered, but I think insurance has to be part of the picture. I think one of the clear points that comes away from Kathleen's discussion is, don't underestimate the ingenuity of if the plaintiff borrow our regulators and we're dealing with new technologies, new regulations, and unknown risks. And, Kathleen can talk to you a lot about solid risk mitigation practices, but it's not realistic to think that you're going to completely eliminate the risk of claims. So, I think insurance serves that important role of backstop, after you've really implemented a lot of Kathleen's recommendations.

Lynda Bennett: One of the things that Kathleen emphasized is that this liability is arising out of or from a statute, number one. So, I want you to comment on, our statutory liability is covered under insurance policies in this instance. And then, number two, Kathleen emphasized a couple of times that this is coming under an unfair trade practices act. So, Joe comment a little bit on the uniqueness of how this liability is arising, and where we'll find ourselves on the coverage picture for that.

Joe Saka: So, let's start with the types of insurance policies that may respond. And, I think there, if listeners take away one thing, it's the notion that one insurance policy may respond, should not enter your mind. Because, you need to be

looking and considering coverage in a number of different places. So, we'll talk about CGL. That's going to cover personal and advertising injury. You want to look at cyber insurance policies, of course. You want to look at D&O policies. If a claim is being asserted by an employee, you want to consider EPL coverage. So, depending on the nature of the allegations and who's asserting them, any number of those policies could potentially respond. And, emphasizing just the nature of regulatory claims or claims alleging unfair trade practices. One of the recent trends that we're seeing for cyber insurance policies is carriers trying to really reduce limits for regulatory claims.

So, you want to try to get as much regulatory coverage as possible. You want to make sure that your D&O policy extends to claim by regulators at as high of a limit as possible. When you talk about unfair trade practices claims, I think one of the immediate things that come to mind is, are there going to be allegations of intentional wrongdoing? And if there are, you want to make sure that your policy's going to at least provide defense coverage, unless and until, there's been a final adjudication, that your conduct was intentionally or deliberately wrongful.

Lynda Bennett: Yeah. Key point there, that just because you're accused of intentional or potentially fraudulent conduct doesn't mean you don't get your defense. So Garrett, jump in the game here and tell us how you think the insurance industry is going to respond to this potential expanded liability, recognizing that D&O and cyber, two of the products that Joe just talked about are the most underwater and swamped with other types of claims already. So, give us a bead into what you think the insurance industry is going to do with this latest development.

Garrett Droege: Yeah. And Linda, thanks so much for having me on. I think I'm the only non-attorney on the call. I'm but a humble insurance broker. Thanks for having me. Yeah, the D&O and cyber markets have been hardening rapidly for the past two to three years. D&O especially, for a little bit longer, a number of factors there. Me Too movement kicked that off, a lot of M&A activity, the spec, D-spec environment, and then cyber rates have increased dramatically since 2019, mostly related to ransomware. And, I know this discussion's around privacy, but I'll say, that individual directors and officers are at risk of being named in lawsuits for both privacy and cybersecurity failures. And, we're focused on Facebook here, but SolarWinds also just announced claims against a mix of current and former directors for knowing about and failing to monitor cybersecurity risks.

So, the risk is real for being named individually. With the market already strained, I don't think more litigation's going to help. Joe mentioned some of the challenges there, you're dealing with non-standardized markets, both. So, it's not traditional insurance CGL, where many policies look the same. Here, you've got 31 flavors and then some. Each structured individually quite differently. So, it's a giant puzzle to fit your D&O and your cyber, making sure they dovetail. Most of the time they don't. So, for example, one of hundreds that I could give, privacy incidents are often excluded on D&O, which for the purposes of today's discussion, that's a problem. And, on the converse securities claims often excluded on the cyber policy. Also, a bit of an issue.

Lynda Bennett: Right. Both you and Joe have really driven home the point that we talk a lot about on this podcast, which is, your insurance program is a patchwork quilt, and you better make sure that it's tightly sewn, and that there aren't any holes in the quilt. So, my question though is, based on what you just said, is it higher prices and higher retentions that will be the answer here, and I just need to go buy more limits? Or, are you anticipating that there'll be a capacity squeeze in even getting what you want and need, because the liabilities are expanding, the claims keep coming, et cetera?

Garrett Droege: Yes. Is the answer. What we're advising clients with regards to cyber is, "Whatever your limits were last year, count on getting that cut in half and paying the exact same or plus 20%." That's just the reality of the marketplace right now. Capacity is an issue across the board. If you're building a large D&O tower, you're used to building layers in $5 and $10 million dollar blocks. Now, you're putting it together in 2.5 million blocks, and it becomes much more complex. Retentions are getting higher. Premiums are getting higher. Coverage is getting constricted. It's not a buyer-friendly market right now. But, as a good insurance broker, I would always recommend buy as much limit as you can get right now.

Lynda Bennett: Absolutely. All right. Well, we've got just a couple of minutes left here. So, I want to go back around the horn and ask each of you the same question, which is what is your one or two pieces of advice to companies to put themselves in the best position to mitigate this risk exposure that certainly existed before, but is much larger today than it was a month ago? So, Kathleen, why don't you go ahead and start?

Kathleen McGee: I would say, don't avoid knowing what's happening within the company, just because you think that way you can avoid liability. You need to know what the policies and procedures are for your company. You need to own them. And, your job is to make sure that you are doing the right thing, because regardless if something bad happens, someone's going to take a second look at you. I know that seems a little harsh, but that is where we're at this point.

Lynda Bennett: Well, that's great risk management before you ever tap into your insurance policy. So, that's a great tip. Joe, what's your two cents?

Joe Saka: Yeah. I mean, assuming the insurers are tightening up language, there's commonly a lag between the claims activity to when the insurer is actually put in those restrictions. So, you want to think broadly about out your insurance policies and you want to think broadly about the allegations that are being asserted against you. And remember, at least when it comes to the defense, if there are even single allegations or single claims that are covered, then the insurer may have an obligation to provide a 100% of defense coverage.

Lynda Bennett: And, don't forget to notice everybody, every policy that may potentially get triggered here, send out the letter first and sort it out later, right? All right, Garrett, bring it home for us. Other than putting more money in our Piggy bank to pay our premium increases, what can we do?

Garrett Droege: I once heard a GDPR supervisor say that, "The best defense for a privacy violation is just to show that you're trying." Make a plan to protect users' privacy and make some effort at enacting that plan. It does not have to be a 100%. It likely never will be, regulations and emerging risk are going to continue to evolve, but be able to point to something, anything.

Lynda Bennett: All right. Great. Well, there's obviously going to be more to come on this we'll carefully watch and wait and see what happens to Mr. Zuckerberg and now SolarWinds. And I'm sure there'll be five more before the end of the year. So, we'll be very happy to have you three back together, polish-up your crystal ball for us in another six months or so. But, thank you for your time today and look forward to seeing you all again soon, and same with our listeners. Take care.

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.