Podcast Transcript

The SaaS Tacks – The Ins and Outs of Negotiating SaaS Contracts

Date: February 13, 2024

Guest: Matt Pearson, Craig Carpenter **Host:** Amy Kattman

Run Time: 12:59

For questions and comments contact:

Matthew D. Pearson

Partner
Costa Mesa
T: +1.714.966.8882 | mpearson@bakerlaw.com

Craig C. Carpenter

Partner
Dallas
T: +1.214.210.1224 | ccarpenter@bakerlaw.com

Kattman: As businesses transform to become more digital, the number of Software as a Service, better known as SaaS, offerings that businesses implement have grown exponentially. SaaS applications can help businesses find new revenue streams, work more efficiently, and more. However, more applications can also mean more exposure to privacy and security risks. Today, we will discuss some of the risks inherent in engaging SaaS providers and some of the ways businesses can mitigate or manage these risks. I'm Amy Kattman, and you're listening to BakerHosts.

On today's episode, we explore the urgency behind SaaS contract planning with Matt Pearson and Craig Carpenter. Matt and Craig are both partners in the Digital Assets and Data Management Group at BakerHostetler. Matt is in the group's Privacy and Digital Risk Class Action and Litigation team, and Craig is

the Practice Group Leader for the firm's Dallas office. Welcome to the show, Matt and Craig.

Pearson: Happy to be here.

Carpenter: Thanks, Amy. Happy to be here.

Kattman: Matt, you've mentioned that SaaS contracts are top of mind for your clients right now. Why are they so important, and why now?

Pearson: To be fair, SaaS contracts have always been important. They've become more top of mind lately because clients are being sued based on, and being held liable because of, their SaaS contracts. For example, in the last couple of years, two SaaS companies that provide a relatively mundane service, file transfers, were breeched. Those breeches had an incredible ripple effect. The SaaS companies who were breeched held the data of their own customers, but they also held the data of their customer's customers, they held the data of their customer's customer's customers, and so on. And when that data was compromised, it wasn't just the SaaS company that took the hit, it was also the SaaS company's customers. Those customers were under notice obligations, and it was those customers who ultimately got sued.

Clients assume that because they were not the company that was breeched, the SaaS company should indemnify and defend them. Unfortunately, that is rarely the case. In these situations, indemnity is almost always determined by what is in the SaaS contract, and almost always, the SaaS contract's indemnity and limitational liability provisions heavily favor the SaaS company. We usually see something along the lines of, the SaaS company's liability is capped at what the client paid for the service over the last three or six months and doesn't include any consequential or indirect damages. And since many of these contracts are for very small amounts of money, maybe $5,000 or $10,000 per month, that limitation of liability provision can really leave clients holding the bag when it comes to litigation.

Kattman: Craig, given SaaS contracts' importance, what can clients do going forward to protect themselves?

Carpenter: The situation described by Matt is unfortunately all too common. SaaS is so ubiquitous in business these days that unless we're talking about a major enterprise-level of software, these agreements often go overlooked. However, Matt gives some compelling reasons why these type of agreements may be more important from a risk management perspective than their dollar value would otherwise indicate.

For these reasons, businesses should take a wholistic approach to managing SaaS vendors and SaaS-related risk. It is too easy for businesses to see the dollar value of one of these agreements and realize maybe, okay, this is not a bet-the-company type situation based on the dollar value of the agreement, and just sign whatever is put in front of them to keep the negotiation moving. Or

maybe the vendor will dangle an expiring discount in order to motivate the business to move quickly on negotiation. And you cannot prevent your vendors from being breeched or having some sort of data security incident like Matt was talking about, but you can take steps to protect yourself. I think the best approach includes three practices that can lead to a better SaaS contracting. First is vetting your SaaS vendors before engaging in contract negotiations. Second, as Matt highlighted, negotiating the appropriate protections and obligations in the actual contract. And third, having some post-execution contract management practices in place.

With regard to the first practice, vendor vetting, this is a really important first step. And it is probably also the easiest step because you're not having to deal directly with a vendor in an adversarial way, and you may not be in a time crunch yet to get something signed up. So, you want to make sure that the team looking to onboard a new SaaS solution or SaaS vendor, whether that is legal, IT, procurement, or one of the business divisions, they need to fully understand who the vendor is, including understanding affiliates and parent companies and all the related entities. They need to understand where that vendor is located and where these services will be provided. And that is important from a privacy perspective whether it is local or offshoring. And also, have they had any public privacy or information security incidents in the past? These three questions are critical to understanding and quantifying the risks that Matt mentioned at the onset, especially these risks as it relates to privacy and security issues. If you don't have this information before negotiating a contract, your team should either find it or ask. It is often easier to get information out of a vendor when they think they're about to sign up a new client versus after the deal is already done.

Second, you're going to want to have your attorney review all of the applicable terms for the agreement. And I say terms instead of contract here purposefully because these days, SaaS contracts typically have multiple documents. And the agreements, they may be spread out over several different links or attached to other versions of the agreement. And some of the really expensive issues and risks that Matt discussed will often be found in some of these ancillary agreements, so it might not be in the main agreement. And it may seem like overkill at times to do a full legal review of some of these smaller SaaS deals, like Matt talked about the $10,000 a month deal. But typically, a good SaaS attorney knows where to focus and where to spend their time on the big-ticket items like indemnification, limitational liability, and the data privacy and security controls. A good SaaS attorney will also understand how these provisions work together and how negotiating one of these provisions, like indemnification, might impact the others, like limitations of liability and privacy controls. Or might impact, ultimately, future litigation like Matt alluded to.

Finally, a good vendor management program doesn't end when you sign on the dotted line. You want to make sure that you're aware of your audit rights and notice obligations. In today's privacy and security environment, it is more critical than ever to make sure you have audit rights. But not only that, but also to exercise them when necessary. For example, California's privacy law requires that businesses not only obligate their service providers to provide audit rights,

but also that the businesses take reasonable steps to ensure compliance by exercising these rights to audit as needed.

Kattman: Thanks, Craig. Matt, assuming a client does proactively work to negotiate their SaaS contracts, how does that change the posture of litigation if and when a client is sued?

Pearson: It can change it drastically. There are some obvious benefits, many of which Craig just mentioned. If a client has negotiated a favorable indemnification and limitation of liability provision, the client may be able to avoid having to pay for the breech investigation, the response, including notification, and the inevitable litigation that follows.

But there are also some that are a little less obvious. For example, even if a client couldn't negotiate the most favorable indemnity or limitation of liability provision, just the act of negotiating them on the front end can provide some benefits. Boiler plate contractual provisions often leave clients wondering who pays for what, when, and how. Paying attention to negotiating a SaaS contract on the front end can make answering these questions much easier if and when they ever come into play.

It also changes the optics of the litigation. When a client gets sued for something a SaaS company did, the first question it has to answer is, what did you, the company, do to make sure this SaaS company was secure before providing them your data? Craig can build into these contracts certain reporting requirements and audit requirements that, at the very least, show that the client was taking seriously and actively monitoring the companies to which it was sharing its data. Which can be very helpful in defending negligence claims.

Moreover, Craig can build into the contract reporting and audit requirements that make sense. We often see audit and reporting requirements that are either completely over the top or entirely lacking. With the former, the client is inundated with information and rarely reviews it. For the latter, even if the client does review it, nothing in those reports is going to adequately inform the client. In truth, there are an innumerable amount of benefits to paying attention and negotiating SaaS contracts on the front end. The only real drawback of doing so is the time and money required. But our firm has been able to develop for clients procedures that limit the cost of SaaS negotiations while protecting the client should litigation ever result.

Kattman: Thanks Matt. Craig, as a final question, for folks listening today who want to do something right now, what are the top three things they should consider doing?

Carpenter: Yeah. As I talked about before, I really think the best protection is to have a wholistic vendor management program. And I know that sounds like a big undertaking, especially for smaller companies or mid-size companies that are dealing with some of these smaller SaaS agreements, a lot of them may be click _____ or online terms and conditions. But I really think you can right size a vendor management program to suit your needs. Not every business will need a

full suite of vendor management tools, or a formal, documented, written program, although we would always recommend that.

But you can always start by implementing the three steps that Matt and I have discussed. Namely vendor vetting, contract negotiation, including special attention on the provisions that Matt talked about, like indemnification, limitations of liability, and data security controls. And also keeping track of your vendors after you sign and the audit rights that Matt discussed. And so, doing those things, those three things, combined with making sure that you have trial counsel, someone like Matt that understands SaaS and SaaS agreements; that is teed up for when there is a problem, and you need to understand your rights and obligations. You want to make sure your trial counsel is aware of the positions that you typically take in SaaS agreements with respect to some of these critical provisions like indemnification.

Besides that, I think the best thing that businesses can do is really take time to do a little bit of what we're doing here today and educate relevant stakeholders as to why today's consumer privacy environment SaaS agreements may have risks that are really disproportionate to their dollar value. And that is why we may need to spend a little extra time and legal muscle understanding these, negotiating these, and making sure that we're comfortable with our positions.

Kattman: Matt and Craig, thanks so much for joining us today.

Pearson: Thank you very much.

Carpenter: Thanks, Amy.

Kattman: If you have any questions for Matt or Craig, their contact information is in the show notes. As always, thanks for listening to BakerHosts.