
The Consumer Finance Podcast: Monumental Win in Data Breach Class Action: A Case Study

Host: Chris Willis

Guests: Ron Raether and Tim St. George

Date Aired: July 18, 2024

Chris Willis:

Welcome to *The Consumer Finance Podcast*. I'm Chris Willis, the co-leader of Troutman Pepper's consumer financial services regulatory practice, and today we're going to be presenting you with a case study of how the Troutman Pepper team delivered a huge win, defeating class certification, in a set of class actions involving a major data breach that was consolidated by the multidistrict panel into a single case. We believe it's the first time that a consumer data breach class action has ever proceeded to class certification and been won by the defendant in an MDL context, and we really are excited to tell you about it today. But before we jump into that topic, let me remind you to visit and subscribe to our blogs, [TroutmanPepperFinancialServices.com](https://www.TroutmanPepperFinancialServices.com) and [ConsumerFinancialServicesLawMonitor.com](https://www.ConsumerFinancialServicesLawMonitor.com). Don't forget about all of our other podcasts. We have the [FCRA Focus](#), all about credit reporting. We have [Unauthorized Access](#), our privacy and data security podcast, [The Crypto Exchange](#), about everything crypto. We have [Payments Pros](#), all about the payments industry, and our newest podcast, [Moving the Metal](#), which is all about the auto finance industry. All of those podcasts are available on all popular podcast platforms.

And speaking of those platforms, if you like this podcast, let us know. Leave us a review on your podcast platform of choice and let us know how we're doing. And if you enjoy reading our blogs and listening to our podcasts, a great way to do it is through our handy mobile app. It's available for both [iOS](#) and [Android](#). Just search Troutman Pepper in your app store, download it, and give it a try. Now, as I said, today we're going to be talking about a really monumental win that the Troutman Pepper team delivered to one of our clients in a major piece of data breach litigation. And joining me to talk about that today are two of my partners, Ron Raether and Tim St. George. Ron, Tim, thanks for being on the podcast today.

Ron Raether:

Chris, thanks so much for having us.

Chris Willis:

Gentlemen, why don't we just start by getting you to tell the audience a little bit about the litigation? What was the case about? What was the procedural process? What happened to lead you up to the decision that you finally obtained on behalf of our client?

Ron Raether:

Chris, in 2020, our client Blackbaud was victimized by a ransomware attack, and that ransomware attack was directed towards a software as a service provider. And as a consequence of that, this criminal element was able to get access to certain data, Blackbaud's customers, who are social good organizations throughout the United States. So you may think

The Consumer Finance Podcast: Monumental Win in Data Breach Class Action: A Case Study

of your local museum, your zoo, maybe even your college or a private school that your kid attends. Those were the customers of Blackbaud, and those customers of Blackbaud in turn had information about their constituents. This case in particular was very early on what in the cybersecurity world is called double dipping or triple extortion, and by that I mean the threat actor in this particular case was looking to ransom and extract money from Blackbaud, which it paid. Blackbaud paid that money, got assurances from the threat actor, made the notices to its customers, and its customers in turn notified its constituents.

The consequence of that were class actions filed all across the United States. In fact, we had I think almost 30 class actions filed that were eventually consolidated under the multidistrict litigation rules before a court in South Carolina. So that was in August of 2020. In the ensuing four years, our team was engaged in a very complex dance with respect to the MDL process, filing motions to dismiss to whittle down the case, engaging in extensive discovery, retention of experts, all designed to litigate the question of whether a class could be certified under Rule 23.

The operative complaint was over 400 pages long involving common law claims, state statutory claims, including the CCPA as well as New York CMIA, so there was medical information. It was just a case that was extremely complex, both at a technical level from understanding databases, the client's technology, what the threat actor did and engaged in, as well as technically from a class certification law and related issues. We went through that discovery. We had briefing. And this spring, the judge in our case issued an order denying class certification. Plaintiffs had filed a petition under Rule 23F, and that's where the case currently stands.

Chris Willis:

Got it. Thanks, Ron. We know this was a huge win for our team and for the client in getting class certification denied, as you just mentioned. Can you talk to me and the audience about what you and the team did in terms of strategy that led up to getting that great result?

Tim St. George:

Chris, this is Tim. The class certification briefing in this case came after discovery closed. In some cases, you'll have a bifurcated schedule where class certification will be due at some point earlier in the discovery period, and then the merits discovery period will then close. But we wanted to make sure that the court had as full of a factual record as possible at the class certification stage, and that the record would be fully complete and crystallized by the time that the parties were litigating class certification. That was step number one was just getting a process in place to make sure that we had a full record. And of course, there was a monumental amount of discovery that occurred within that overall discovery period, because it involved all issues of class certification and merits. It was the entire case. We then negotiated specific schedules for class certification experts, which came after the close of fact discovery, again, so that there could be no argument that those reports should be supplemented in some way, and that the record would close.

Even before the plaintiffs engaged their experts and we knew who they were going to be, we launched on an extensive campaign and strategy to make sure that we would have the preeminent experts in the field to address the theories that we knew were going to be forthcoming. We had experts that considered the technical side of the case, so information security, ascertainability, and whether the database and customizable structure of the

databases could lead to an ascertainable class. We had expert economists to counter their economic damages theories because we knew that those would lie at the heart of their attempts for class certification. They were going to claim damages through to the exposure, both the value of the information and the claimed ongoing risk of that exposure. We had dark web experts, because we knew that they were going to make claims about what and was not on the dark web, so we engaged cybersecurity firms to do contrary and rebuttal dark web analysis.

And then we had rebuttal experts as well on information security, ascertainability, as well as the statistician to rebut the claims that they had selected a representative sample of data on which to claim ascertainability. So, there was substantial expert practice and rebuttal expert practice that went into the class certification decision. The court actually held a multi-day Daubert and class certification hearing for three days down in Charleston. The court even went so far as to retain an expert consultant, including based on some of the recommendations that Blackbaud had provided to assist in the technical side of the case, and the court then examined in open court experts with the assistance of the independent technical consultant.

All of that led to a very extensive and complete class certification record and substantial expert practice, which ultimately was successful as well in the decision that the judge reached. I'll also mention we even had two judges, just to make this as complex as possible. The MDL started off with Michelle Childs as our judge. During the middle of the case, she was elevated to the DC Circuit. And then the case went to Judge John Anderson, who ultimately issued the decision on class certification.

Ron Raether:

I think it's important to acknowledge what a commendable job both jurists did in managing this very complex and sophisticated case. The hearing that Judge Anderson oversaw with respect to the class certification hearing was conducted in a way that demonstrated this court's acumen with respect to not just the issues that we were litigating, but just managing the courtroom in a very efficient, effective, and fair way.

Tim St. George:

The court made some smart strategic moves as well. Judge Childs on the front end appointed a mediator to oversee the prospects for settlement in the case, and obviously that was not successful re certification, but there was a structure in place. There was also a special master appointed, that was Maura Grossman, who actually is in Canada, to help manage the discovery process, and she was instrumental in making sure that the case did proceed on the path that the parties had agreed to. As I mentioned, the full discovery period happened and she was involved in dozens of discreet discovery disputes, only a handful of which ultimately bubbled up to the district court for further resolution. So to Rob's point, there was very intelligent and effective case management that went in on the front end, which paid a lot of dividends to make sure that both parties would be fully heard on the merits at the appropriate time.

Chris Willis:

Gentlemen, you've talked some about the very complex nature of the case and all the discovery and the very intense expert practice in the case. Talk to me a little bit about what it took from a lawyer team standpoint to make all that work, because obviously it wasn't just the two of you

representing the defendant in this case. Talk to me about the team that you put together and how they worked together here at Troutman.

Ron Raether:

Very proud of this team and the way that we collaborated and worked together over the past four years. It really begins with having individuals with a varied set of backgrounds, experiences, insights, and knowledge. At the beginning of the case, I think we had an advantage of understanding this area of not just the law, but also the technology as well if not better than any other lawyers in the United States. As you know, Chris, our firm was involved in both of the first two incidents that occurred in 2005. Each of those went to litigation, and we had involvement in at least one of them. Understanding incident response, understanding the forensic review, the technology data and the flow of data allowed us to quickly surmise what was going to be our best defenses and pull together a strategy that we then needed to execute on.

And executing on that, we brought in a variety of individuals. Tim, for example, had extensive experience with the OSCA one data breach MDL, and specifically with respect to dealing with damage and damage models. And so he very effectively was able to address those issues in the context of both discovery expert and fact, as well as our briefings on those issues. We likewise had groups, partner/associate teams, that were dealing with issues that then recounted such as the dark web and whether there was any evidence causally linking alleged consumer harm to the Blackbaud incident. We had teams focused on analyzing the data itself with our experts to counter any ascertainability arguments, including the referential database model that their expert claimed to have developed, and that worked very effectively. But we likewise had teams on issues such as electronic discovery, constitutional law challenges, or standing issues, or the substantive claims when we filed our motions to dismiss. And coordinating all of those moving parts with a structure that allowed us to work harmoniously, without any inefficiency, but more importantly, with an efficacy towards obtaining the best result we could for our client.

Chris Willis:

So I think I have to ask, Ron, obviously this case thus far has a happy ending in terms of class certification being denied. What was the requested amount in terms of relief that the plaintiffs were seeking in the case, so that the audience has an idea of the magnitude of the case?

Ron Raether:

It was a little unclear, Chris, but eventually in their class certification motion and in what they've said publicly, they estimated the class to be 1.2 billion people. They never really articulated what the common law damage amount would be, but I can tell you, if everyone just got a dollar, that's \$1.2 billion. I don't know how many were in California, but the CTPA provides for statutory damages of a thousand dollars per class member per incident, so the potential numbers could be ruinous if this case were to go to trial under class proposed by plaintiffs.

Chris Willis:

That certainly underscores the magnitude of the case and of course the magnitude of the result that you delivered to the client. I wanted to ask the two of you also, is there anything about the

class certification decision in this case that might be influential or important for future data breach class action litigation?

Tim St. George:

Sure. I think the class certification decision should be highly influential in data breach class actions moving forward. It's important to note that although the parties had a full-throated dispute over class certification in all of its elements, predominance, typicality, adequacy, superiority, et cetera, it's notable that this court in issuing its 60-plus-page decision, felt that the plaintiffs had not even satisfied the threshold implicit element of Rule 23, which was ascertainability. Now, the court signaled that a lot of the ascertainability problems would also give rise to hurdles with respect to all of the other Rule 23 elements. But this was blocking the door on the front end of the class inquiry because they couldn't satisfy ascertainability. And in doing so, the court conducted a really rigorous analysis. Under both Rule 23 and 702, it held that the plaintiff's ascertainability theories were a moving target. Those were the court's words. A moving target throughout the litigation and even as briefing commenced.

But the court very methodically went through each one of those moving targets and shot them down. It started with Rule 702, and again, an extensive application of what a ascertainability expert would have to prove. And that's things like error rates, the ability to scale replicability, demonstrating and documenting the work that was performed, accounting for various variables that had been introduced, accounting for the various issues that we had pointed out in our rebuttal. So there were a lot of issues that an ascertainability expert would need to account for that simply weren't accounted for here.

And then with respect to the other ascertainability proposals that we were taking on as they were being lodged at us, the court again went through each one of those, including some really common ascertainability arguments that are lodged not just in data breach cases, but in consumer cases more generally, such as the fact that data companies generally shouldn't be able to claim that classes aren't ascertainability. Or the use of certain products for other purposes has no bearing on whether or not a class would be ascertainable and the procedural requirements, for instance, that are in place to make sure that litigation is fair, adequately presenting your ascertainability theories in discovery and through expert reports so that they can be tested and briefed. And that they can't be briefed on the fly.

The district court really made sure that all of those requirements were held firm, and the district court re-emphasized that the Fourth Circuit imposes stringent and real ascertainability requirements, and that there does reach a point where administrative feasibility is simply not possible. And so all of these things are very important to class certification more generally, and certainly in the data breach context. And obviously, we were very pleased with the result on ascertainability alone.

Ron Raether:

Chris, Tim gave a very technical Rule 23 response. Let me generalize it a little bit more in terms of what I think is the importance of our experience at this stage. So the first thing is, historically in data breach cases, standing in Article III has been the preeminent issue. Could plaintiffs proceed in federal court? And starting in 2006, we got positive decisions that started to erode. And then we got *Concepcion* from the Supreme Court and we went through that pattern again

until, skipping forward, two more decisions from the Supreme Court, we got Ramirez. And I think that in data breach litigation, there's always been a limit or an eye towards if the plaintiff can stay in federal court and get past Article III, it's time to write a check. And I think our efforts in this case have proven that's not the case, that you can do more in litigation on these data breach issues, even in an MDL, other than just to coming to whatever number plaintiffs and plaintiffs' counsel put forward in settlement.

The second thing is making sure that you're looking at each case individually and understanding the facts and circumstances with respect to that breach, which goes to my third point, which is we need to start doing a better job of anticipating what cases are going to resolve in litigation as we're walking through the incident response, and the attorneys and the company are shaping their efforts as well as their communication strategies and plans with respect to those incidents. And I think that the decision that Judge Anderson issued, as well as the work that we've done in this case, begins to provide some thinking and some insight into how that infinite response plan, when activated and implemented, things that need to be considered to make sure that we're not all being just put in a position of having to write a check whenever one of these complaints is filed.

Chris Willis:

Gentlemen, this has been a fascinating discussion, and I'm so proud to have the opportunity to tell our podcast listeners about the tremendous victory that you and our Troutman Pepper team won in this incredibly important case. So, thank you both for being on the podcast today, and of course, thanks to our audience for tuning into today's episode as well. Don't forget to visit and subscribe to our blogs, TroutmanPepperFinancialServices.com and ConsumerFinancialServicesLawMonitor.com. And while you're at it, why not visit us over at troutman.com and add yourself to our Consumer Financial Services email list? That way, we can send you copies of our alerts and advisories, as well as invitations to our industry-only webinars that we put on from time to time. And as I mentioned at the top of the podcast, don't forget to check out our mobile app. Just search for Troutman Pepper in your app store, download it, and give it a try. And of course, stay tuned for a great new episode of this podcast every Thursday afternoon. Thank you all for listening.

Copyright, Troutman Pepper Hamilton Sanders LLP. These recorded materials are designed for educational purposes only. This podcast is not legal advice and does not create an attorney-client relationship. The views and opinions expressed in this podcast are solely those of the individual participants. Troutman Pepper does not make any representations or warranties, express or implied, regarding the contents of this podcast. Information on previous case results does not guarantee a similar future result. Users of this podcast may save and use the podcast only for personal or other non-commercial, educational purposes. No other use, including, without limitation, reproduction, retransmission or editing of this podcast may be made without the prior written permission of Troutman Pepper. If you have any questions, please contact us at troutman.com.