# The Growth of Class Action Lawsuits Involving Data Breaches - Episode #152

Posted: Thur., Apr. 25, 2019

**Hosted by:** John Czuba, Managing Editor

**Guest Attorneys:** Matthew Berkowitz and Brian O'Shea of Carr Maloney P.C.

Qualified Member in *Best's Recommended Insurance Attorneys* since: 1984

CARR MALONEY PC

**John Czuba:** Welcome to "Best's Insurance Law Podcast," the broadcast about timely and important legal issues affecting the insurance industry. I'm John Czuba, managing editor of *Best's Insurance Professional Resources.*

We're pleased to have with us today attorneys Matthew Berkowitz and Brian O'Shea from the law firm Carr Maloney P.C. in Washington, DC.

Matthew Berkowitz is a member of the firm with significant class action experience, regularly representing national, regional, local corporations, employers, retailers, manufacturers, automobile dealerships, credit reporting agencies, financial institutions, debt collection agencies, law firms and among others in class action and federal and states laws.

With the help of associate Brian O'Shea, Carr Maloney has successfully defended class action lawsuits involving mass torts, products liability, defective design and warranty claims, cyber security and data breach, and consumer protection claims.

Gentlemen, we're very pleased to have you both with us this morning.

**Matthew Berkowitz**: Thank you.

**Brian O'Shea**: Thank you very much.

**John**: Matt, we'll start our questions with you today. Can you talk about the growth of class action lawsuits involving data breaches?

**Matthew**: Sure, absolutely. This is an area where breaches and data breaches have exponentially increased over the last few years. Recent statistics show that only 37 percent of businesses actually track and control the sensitive data that they have. As a result, that's part of the main reason why data breaches have increased so much.

For example, in 2014 2015, there was an increase in data breaches by almost 40 percent. Then, in 2018 alone the United States had 1.244 million recorded data breaches with over 446 million records exposed.

The scary thing about this is, with all these records exposed, 80 percent of the companies that were hacked or that had the breach, it took them at least a week to discover that there was a breach. This becomes significantly

dangerous because during that week's time, certainly if it happened, if it was discovered within 24 hours, they could have pulled information back.

They could have put remedial measures in place, but because it took so long to discover, by then the information was gone. The hacker, perhaps, is using someone's credit card information, or gaining financial access, or changing or stealing a person's identity.

Currently, there's no comprehensive federal law, but the federal law to guard against that companies need to abide by is in the works.

**Brian**: I'll just add on to what Matt was saying. Data breaches and data breach class actions are becoming more and more newsworthy. Hardly a week or a month goes by without us hearing about a significant data breach.

Just for example, companies like Equifax, Target, Yahoo, and Facebook have all recently faced significant data breaches and data breach class action litigation just in recent months. These class actions are becoming more and more newsworthy and a greater part of the class action environment.

**John**: Thank you, Brian. We'll continue a little bit with you. These are all large, and national, and international companies that you've mentioned. What about smaller or medium sized businesses? Do they also have to be worried?

**Brian**: Absolutely they need to be worried. Any company that keeps customer data on a computer needs to be concerned about data breaches and potential litigation arising out of these data breaches. These companies could be law firms, doctor's offices, mom and pop retailers, as well.

Often, these smaller to medium sized companies don't have the resources to protect themselves from a data breach like a company like Target or Facebook might have. They don't have the expertise and they're not as tech savvy. That can potentially create even greater problems for them.

**John**: Matt, what are some of the hot or topical issues in data breach class actions now?

**Matthew**: That's a really good question. There are three areas in class actions involving data breaches specifically that often arises as far as legal issues that the parties often fight over. There are standing issues, something known as ascertainability, and predominancy.

Brian and I will talk about them very briefly. The first one is standing. In order to bring a class action lawsuit, the lead plaintiff needs to have standing. That means...The Supreme Court recently in Spokeo reaffirmed that the lead plaintiff needs to suffer a concrete and particularized harm.

There needs to be a tangible harm to the plaintiff himself or herself. A lot of times, you can bring these class actions based upon a data breach. A lot of these class members, their harm or the injury that they've suffered is merely fear that their data was exposed.

The plaintiff might be claiming that my data was taken today, but sometime in the future somebody might use my identity. The majority of jurisdictions say that's not enough. It's the idea that if a tree falls in a forest but nobody hears, does it make a sound? It's that analogous.Some courts have ruled that's enough, the mere fear that your data was taken is enough to give a plaintiff standing, but the majority of jurisdictions say that fear itself is not enough. Often, defendants can get out of those lawsuits by arguing that the plaintiff lacks a concrete injury, enough to give that lead plaintiff standing to represent an entire class.

Brian, I think, is going to talk about ascertainability.

**Brian**: Ascertainability is another potential defense that's often used. All ascertainability is, is determining who is a member of the class and who is not a member of the class. Generally, for a class to be ascertainable, the class needs to be formed from objective criteria. This is usually done by looking at the company's records, who's the defendant in the lawsuit.

With data breaches, this ascertainability becomes especially complex because we could be talking about, potentially, thousands, tens of thousands, or even millions of potential class plaintiffs. Additionally, with data breaches, it can be very hard to identify whose data was actually breached.

This can take a significant amount of time. It's possible that a clear answer might never be reached. It can be very difficult in the data breach space to determine who is actually a member of the class, who is not. This is why this is such a common issue in defense that comes up in these cases.

**Matthew**: Dovetailing off that is the predominancy. This predominancy issue comes right out in Rule 23, which governs class action. Rule 23(b) talks about common questions must predominate over individual questions. Often, in class actions, there may be some individual questions that vary from class member to class member.

The idea is there needs to be commonality. The common questions must predominate. In a data breach, you may have what Bryan was talking about and what I was talking about earlier, especially with respect to damages, that there are a lot of different questions about individual harms, for example.

We have a data breach, but who? You start asking questions of whose information was exposed. Of those people whose information was exposed or breached, how many of those people are just based on suffering damages based on fear alone? How many of those people had actual damages themselves other than fear?

It leads to what's called individual inquires. We have these individual inquires, whether it may be for economic harm. You start asking, "What is the harm?" Each person's harm is different. Once you get into a place of each harm is different, you start resulting in, essentially, mini trials. You start having to have a trial on everybody's damages or everybody's individual question.

It's these mini trials that class actions seek to avoid. The idea is to do, for a class wide resolution, you want to be able to handle this case in one fell swoop.

Courts, on the other hand, often will, for purposes of liability, can run it as a class action but then bifurcate and have individual cases in terms of damages.

Those are the three hot topics in the class action arena when the underlying matter involves a data breach.

**John**: Matt, what can companies do to guard against data breaches and protect their businesses from significant exposure?

**Matthew**: There's a lot of things that companies not only can do but they should be doing, no matter how big their size.

The first thing, and Brian talked about it a little bit, about the resources that, yes, the smaller businesses, the mid-sized businesses, they may not be as tech savvy, but every business that holds sensitive data

should hire an IT consultant or an in house expert to help guide them. It's important, in doing that, that person that you hire or retain can help identify the sensitive data.

What procedures and policies you need to put in place to protect that data. The first step is identifying what data is it that you have that is sensitive. Are you a doctor's office that has medical information that's going to be sensitive? A law firm that has attorney client privileged information. A business that has credit card records.

What data do you have? Where is that data stored? Who has access to that data? Just because you have access to the data doesn't mean that everybody in the company needs to have access to it.

That gets to the next thing, making sure that there's proper training, policies, and procedures, that employees are aware of the data and you can go through that, especially with having security measures. That leads to training about passwords, that passwords should constantly be changed every 30, 60, 90 days. At most 90 days.

Employees should be trained not to use common passwords. Also, should be trained about a lot of big things. Hacks today occur through phishing emails, where it looks like it's an email intended. Employees should be trained how to respond and react to that if they're not sure if the email's intended for them.

In addition, talking about physical lock up of security, maybe their laptops, firewalls, who has access. Limited access to certain employees. Separate networks. Keeping the server locked up. Having the server located at a third-party vendor.

A lot of different things, little things that I've mentioned in a few minutes with the help of an IT consultant or an in house expert could protect the company from a data breach, as well as liability and significant exposure.

The other thing, in the event there is exposure, one of the best pieces of advice for a business is to make sure that they have a cyber-security policy in place, especially for smaller businesses. A lot of them, they'll get a CGL policy or think their standard policy's going to cover a data breach. Often, they don't.

It's important for businesses to contact their broker and ask about a specific policy with respect to data breaches.

**Brian**: I'll just make one last point based on what Matt said. Just like companies take seriously the possibility of someone physically breaking in and taking files out of a file cabinet or medical records out of a doctor's office, data breaches are essentially the same thing.

They should take it just as seriously, even though the breach itself happens in cyberspace and is not actually a physical break in.

**John**: Gentlemen, thank you both so much for joining us today.

**Matthew**: Thank you very much.

**Brian**: Thank you.

**John**: That was Matthew Berkowitz and Brian O'Shea from the Carr Maloney Law Firm in Washington, DC. Special thanks to today's producer, Frank Vowinkel.

Thank you all for joining us for "Best's Insurance Law Podcast." To subscribe to this audio program, go to our web page, www.ambest.com/claimsresource. If you have any suggestions for a future topic regarding an insurance law case or issue, please email us at lawpodcast@ambest.com.

I'm John Czuba, and now this message.

Transcription by CastingWords

To find out more about becoming a Qualified Member in *Best's Insurance Professional Resources*, contact claimsresource@ambest.com or visit our Learn More page to start the application process.