Barclay Damon Live Presents *Cyber Sip*™
Season 4, Episode 3: "Recent Trends in Data Breach Class Actions," With David Lietz

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Welcome back to *Cyber Sip*. David Lietz is one of the leading data breach class action plaintiff-side lawyers in the US today. So I thought who better to bring on to *Cyber Sip* to talk to us about how these class actions work, where are they headed, and what do you need to know. So David, welcome to *Cyber Sip*.

[David]: Thank you very much, Kevin. It's a pleasure to be here.

[Kevin]: It's my pleasure to have you. Thank you for joining us. And if you had to introduce yourself to a prospective victim of a data breach, what would you say?

[David]: I would say I am currently a senior partner with Milberg, based out of Washington DC. I've been an attorney for approximately 33 years. So been at this for a while. Graduate of Georgetown University Law Center here in Washington DC. And I've been doing data breach now for going on a decade. But I have a long career, really representing plaintiffs pretty much exclusively throughout my career. So doing this data breach stuff, I feel like I wear the white hat, although, again, as I was saying before we started, my wife mentioned this morning that she thought the name of this podcast was *Cyber Sith*. And, you know, I thought, well, Dark Lord from Star Wars, you know, that seems appropriate for a plaintiff's lawyer coming on a show like this...

[Kevin]: Well, and there are ways to prevent you from looking like a Sith lord. And we'll talk about some of them, including insurance. And we are going to talk about insurance. We're going to talk about standing, the types of claims, and how they get resolved. David, but first, I want to start with this question, because I rarely get a chance to talk to someone like you certainly not on the podcast. You've been in this field, if not at its inception, certainly very close to its inception. So how has the data breach class action world evolved since the time you've been involved in it?

[David]: In the initial stages of data breach class action, I think that plaintiff's attorneys, were focusing on the big breaches. So you had some major retailers, Home Depot, you had the hotel chain, Marriott. You had Equifax, the credit reporting agency. And they were breaches that were ubiquitous; that everybody knew about, and everybody heard about. And plaintiff's lawyers thought, hey, this is something we need to get into. So you would see these really large data breach lawsuits, from breaches involving millions of people—you'd see sort of a pile-on from the plaintiff's side and, and they'd be litigated, you know, generally a little deeper than I think cases are these days. I think the sea change, in the last four or five years has been kind of number one, the explosion of breaches generally. And then number two, the explosion of lawsuits, being filed for much smaller breaches, breaches of, you know, a couple hundred thousand, under 100,000, some that are even in the, in the single digit thousands. So that has just, made the whole space change dramatically. You just have so much more litigation going on.

[Kevin]: So it sounds like the volume has increased over time. And I think that's the first lesson that I'd like to share with our audience, is that if you think because you're not a target or an Equifax, you're not going to get hit with a data breach class action, you're wrong. If you have suffered a data breach, and your reporting that to a governmental authority, then folks like you, David and Milberg and many other firms across the country, you're going to find out about it and you're going to be in a position where you start to evaluate whether there's a viable claim against that reporting entity. Right?

[David]: That's exactly right. So we will find out about it. There's a lot of attorneys on the plaintiffs' side who are actively tracking data breaches. There are public sources, because this is a public reporting requirement in many instances. And honestly, data breach has just sort of entered the public consciousness, and it's entered the public consciousness in a way that folks realize that they can get a little money, perhaps, from a data breach lawsuit. So literally, before this cyber podcast started, I got a phone call from a doctor in the northeast, saying my wife and I just received data breach notice letters, you know, can I talk to you about this? And, I said, well, I'm doing a podcast, but I'll call you back. So, people just know about data breaches. They know that there's data breach litigation going on, and they know that they should be doing something about it. They... folks are more interested in being proactive about it.

[Kevin]: So I think the first time anyone hears about a potential data breach is when they get a postcard or a letter in the mail from a trusted organization that tells them they've... their information has been bound up in a breach somehow. Before we go any further then, David, can you just give us a quick overview? Someone's listening and they're saying, well, what is a data breach and what is a data breach class action? Give us some head notes about that.

[David]: Yeah. So you're absolutely right. Oftentimes the first that people hear about data breaches are these letters that are issued by companies, who are required to report to the people affected by a data breach, or potentially affected, that this event has occurred. And what generally has occurred is that a cybercriminal has somehow made its way into the networks or systems of a defendant company, and they have moved around within the systems, and they have, among other things, set out to harvest valuable data. And the valuable data can take different forms. It could be that they're in the system looking for financial information about a company. They could be looking for administrative level passwords to sort of wreak untold havoc on a company. But also they've found that there is valuable personally identifying information in many of these company's data sets, and they harvest it actively. They exfiltrate it. They take it out of the system, and they may try and monetize it in many different ways, including selling it to other bad actors, but also using it directly to commit identity theft and fraud. So data breach takes many different forms. But kind of the ones we're talking about generally involve cybercriminals. And it generally involves personally identifiable information or, protected health information, which is also very valuable and potentially damages to normal people. And then this information being exfiltrated and the companies giving notice to people that, hey, this event has occurred, and you need to be on guard about it. And when you get these letters, the companies say, here are some steps you should take to protect yourself and possibly even here's some free identity theft protection, credit monitoring, other forms of identity theft protection, because we know you're now at risk. So that's sort of how these cases come about. A cohort of people identified by the defendant, get these letters, and then folks sort of throw up their hands and say, what do I do? And they reach out to folks like me, to try and help them through the question of what do I do next?

[Kevin]: Before we get to that, I want to take you back to that personally identifiable information, we'll set aside PHI. The question I have for you is rooted in this, I think, I think this and a lot of people think, well, I mean the most important information to me might be my financial information, my bank account information and anything... credit card information, and anything short of that I'm not worried about. But the truth is, the threat actor can steal far less than the financial keys to the kingdom and use it as a basis for identity theft. So, David, I wonder if you could just spend a moment talking to our audience about how little it actually takes to

place an individual at risk for identity theft? What...how little information does the threat actor actually need in order to try to apply for a loan or apply for a mortgage, or do those things that can be very, very bad when they do happen.

[David]: Very little, certainly any breach that, involves a Social Security number, is one where the folks who were impacted by it, are at risk of identity theft. One court, in the northeast has said, that a Social Security number is the gold standard for identity theft and fraud. And so armed with just a name and a Social Security number, a cybercriminal can go in and masquerade as you in many different areas of the world and undertake steps to really steal your identity. They can apply for loans in your name. They can open credit cards in your name. They can get your tax returns. They could apply for your workers compensation benefits. They could go to a hospital and seek medical care, and get prescription drugs, all armed with just a Social Security number and a name. And folks are like, well, they don't have my address. They don't have the other pieces of the puzzle. Number one, if you're going to commit fraud, say you're committing tax fraud—you don't want the fraudulent tax return check to go to the address of the legitimate person who has the Social Security number. You want it to go to the cybercriminal's address. So they put in a fake address, you know, one that's advantageous to them. These companies... and the government doesn't really cross-check, Social Security numbers and addresses when it comes to that. But the cybercriminals also, are very advanced, and they work to commit something, that we refer to as "fullz packages." F-U-L-L-Z, and a fullz package is where they have like a single piece of information about you, and then they sort of leverage that to find out additional pieces of personal information about you. And they create sort of a whole dossier on you just with sort of one linchpin piece. So it's a simple matter. Again, armed with a Social Security number to go out and get the corresponding address, the corresponding phone number, an email address, relatives, mother's maiden name, all sorts of things that are typically deemed as sort of gatekeeping functions for preventing identity theft and fraud. It's not hard to gather that data and the cybercriminals do it. Also, you know, there are things that, folks don't think is as sensitive, from an identity theft standpoint, and because of technology, it's become very sensitive. So an example of that would be driver's license numbers. Right. There has been an auto-populate function, that a lot of auto insurance companies have placed on their websites for putting in an application for car insurance. So what happens is you... the cybercriminal gets your driver's license number. You... then they take your name, and they take your driver's license number, and they input it into the application screen. And because of the computer functionality of that screen, the applications screen, all of a sudden all of your other personal information will auto-populate and all the other fields just because you've entered the accurate driver's license number and then the cybercriminal has your address, has your phone number, has your Social Security number, everything else that you've ever inputted on an auto insurance application before just shows up on a screen just by that one piece of information. So it isn't the case that the cyber criminals need to get your whole identity to commit identity theft. Really, just one critical piece of information can be the linchpin to, unlocking your whole life and turning it upside down.

[Kevin]: Yeah, no. Very important. Thank you for sharing that with us, David. So let's skip ahead. I'm not going to ask you how you or your clients decide to bring a data breach class action, because I think that's probably protected information itself. But let's say you've reached a point where the client will reach out to you. You will decide that it makes sense to bring a lawsuit not only on behalf of your client, but on behalf of, a purported class of individuals who have—at least allegedly—suffered the same sort of loss or damage. So you filed the lawsuit, and we know, you and I have been on different sides of this issue, but we know that one of the early questions that comes up is the question of standing. And so I thought we'd talk about that. Now, tell us, please, what is standing. And then, you know, give us a sense of how the litigation of that issue has evolved over time. I know, for example, early on, those of us on my side were arguing, and we still do, that there has to be an injury in fact, you have to have suffered an actual loss. But there's a question whether, for example, the fear of... the maybe a well-grounded fear of future identity theft based on, a data breach is sufficient to confer standing. So that's a really long question. Take it wherever you'd like.

[David]: So standing is a legal concept that essentially means that the doors to a court are open to you as a plaintiff, somebody who's filing a lawsuit. And standing is different for federal courts, the courts of the United

States versus the state courts and the key distinction is that in federal courts, the federal courts, by law and by the US Constitution, are courts of limited jurisdiction, meaning that there are only certain types of cases that can be heard in the courts of the United States. And you start at the US district court level. That's the trial court in the federal court system. So what swings open the door to federal court? Well, it's just what you said. It's this idea that you have to have an injury in fact. And normally in the data breach sphere, the most common form of injury in fact, would be that you suffered identity theft or fraud as a consequence of the data breach. And so that's the easy case, because generally folks who have suffered actual identity theft or fraud, there just isn't a question about whether or not they're injured. In fact, there's a quote from a federal court in the District of Columbia that basically says, no one argues that someone who suffered identity theft has an injury. Where things get a little more murky is the question of, well, nothing's happened yet, but something really bad could happen because again, just hearkening back to what I just said about what a cybercriminal can do with a name and Social Security number. If the breach has a stolen name and a Social Security number, well, that just gives the cybercriminal everything they need to eventually do something really bad to you; to steal your identity or commit fraud against you. And when you're talking about data sets where hundreds of thousands of people's Social Security numbers are stolen all at once, it might be a while before the cybercriminals work through the list to get down to your Social Security number and actually do anything. So the courts have basically said, the federal courts have said we're not just going to limit the times when the doors to federal courts swing open to ones where there's actually identity theft and fraud, we're going to open that up to also instances where there is an imminent or impending risk that something bad is going to happen, imminent impending risk of harm. And courts look at different things to determine whether or not there actually is an imminent and impending risk of harm. And they kind of boil it down to three factors. And one is whether or not there are cybercriminals involved. If there are, if there's bad actors involved, that tends to indicate that people are at risk. Also, the type of information that is compromised, makes a big difference whether or not you're at the risk of future harm. Interestingly, you mentioned, you know, credit cards and financial information that people often think of that as the scariest thing to have stolen. Actually, in some ways, if you have a stolen credit card, you might suffer some credit card fraud, but it's going to be kind of one and done, because everybody knows when your credit card gets stolen and you have some fraudulent charges, it's immediately canceled, and the damage stops. And also generally, credit card companies, banks will make you whole for that. They don't hold you accountable necessarily for the fraudulent charges. So the courts have said, hey, if it's a credit card, generally that's not going to lead to any future harm down the road. We can't really envision that somebody is going to steal your identity or somehow backward engineer your total identity from your credit card number. But if it's your Social Security number, well, that's really bad, really sensitive information, that, again, is sort of the gold standard for identity theft and fraud. So they look at whether or not ...or the nature of the information that was stolen to determine whether or not there's this imminent or impending risk of harm. And then the last thing is, maybe you didn't suffer personally some misuse of your data, but maybe somebody else did arising out of this breach. So the third factor is whether or not there's been some misuse of the data stolen. And you know that... what that entails has been evolving to, some misuse of the data set could be posting the data set on the dark web, where it could be subject to anybody walking along buying it. That's a form of misuse that some of the courts have said sort of tends to show, again, that you're at a risk of harm happening not today, but pretty close to today, like imminent and impending. So. So that's the battleground, that we fight with the defense counsel about, particularly in federal court. You know, can you even be in this court? Have you suffered either that actual injury or you have an imminent injury, and if not, you're out. You don't get to proceed with your lawsuit. So we've gone round and round with defense counsel about that with mixed results. It's different across the country as different federal courts interpreted differently. And it remains a really big question. I was just in front of the Eighth Circuit Court of Appeal in St. Paul, Minnesota last week arguing that very issue. So, and then you get to state courts and state courts have kind of taken on the federal standard, although my attitude is they shouldn't because state courts are courts have general jurisdiction will hear any dispute as long as you have a personal dog in the fight. But for some reason, clever defense counsel have sort of gotten them to believe that, the federal standard for a limited court... limited jurisdiction should apply in state court. So we have the same fights in state court. But I think the plaintiffs' lawyers generally do better in state court, at least with the standing question. Right. That long answer. Sorry about that.

[Kevin]: No, no, I appreciate it. And I think you touched on this already, but I wanted to circle back and ask you. So in the course of the last several years, do you see any trend lines? Are...is the plaintiff's side getting better at defeating the standing challenge? Are defendants making those arguments more frequently or less frequently, or does it just matter whether you're in federal or state court or which part of the country you're in?

[David]: All of the above. So defendants definitely are still fighting it tooth and nail. And I would say the incidence of, motions being filed challenging the plaintiffs standing has increased, along with sort of the overall flow of, additional cases. I think that you just have companies and insurers who are saying we want to take every stand that we can, and we want to take our shot. There is a distinction about where you are in the country, certain parts of the country, the trend seems to be going the plaintiffs' way. So New England, New York, Pennsylvania, everything up the Northeast Corridor tends to be trending more in the plaintiffs' direction. The southeast and the southwest. You know, Texas in particular, definitely trending toward the defendants and courts being a lot more... giving a lot more scrutiny to the allegations that plaintiffs made about whether or not they have an injury that lets the doors to court swing open. Is this battle going to be resolved today? No. It's not. There was a case in 2021 that the Supreme Court handed down the...Ramirez versus TransUnion case. Everybody thought that was going to answer the question of standing once and for all. And every case was going to be thrust into state court. Which was ironic to me because, you know, there was an act in 2005 that tried to push all class actions into federal court. And, now, all of a sudden we want out of federal court.

[David]: Yeah, yeah. Now, now we want, you know, out of federal court. So, but TransUnion didn't have that clarifying effect. If anything, it's kind of spawned a second wave of, appellate litigation, and the courts are still figuring it out. What does TransUnion really mean? From my perspective, it's a good case for the plaintiffs. And there's a lot of defense attorneys who say just the opposite.

[Kevin]: So. Right. Open questions. So let's turn now, a little bit to where the rubber meets the road, I want to talk about settlements? But before we do that, I want to ask you about your clients who came to you recently, but let's pretend I come to you. I just got a notice of class action settlement, and I come to you, and I say, you know, Dave, I don't know what to do. Is there a possible class action here? We can help more people? I know I'm putting it in reverse because the notice presupposes that there's been a class action. So I should amend my thought. I've been breached, and I'm wondering if I have a claim. What sorts of legal claims could someone like me have against the organization that held my data and for whatever reason, did not safeguard it?

[David]: Yeah. So then... the first notice letter is actually not a notice of the class action. It's just a notice of the breach that the companies send out. But it does sort of define a class because there's only a certain group of people who get these letters. You know, my first questions when somebody approaches me are, well, what does your letter tell you? And, you know, the first thing I want to know is what has the company revealed about what data was impacted? That will make an impact on whether or not I think there's any viable lawsuit to bring. Because there are plenty of breaches that happen where, despite the cybercriminals trying to be opportunistic and getting useful and valuable information, they get a lot of dreck. They get a lot of stuff that's not useful for any purpose. And so it's still the breach. But if you get a letter saying, you know, your name, address, and email address has been compromised, while all that information's generally available in the public sphere on the internet, you know, directory assistance, different places, public websites that you can go to, to readily find out that information. That's not a very sensitive data breach and not one that's going to make for a successful lawsuit. So the first thing that I would always look at is what data set are we talking about. And then assuming it's something very sensitive, I will ask, what does the letter say about the facts of the incident? And unfortunately, for the plaintiffs' side, the companies are typically assisted by defense counsel in writing these breach notice letters, and they are very carefully worded letters, where nothing is really admitted. And you have to sort of read between the lines. It's fairly rare that you get like a really fulsome disclosure of "this is what really happened." It does happen sometimes, but more not as much as we'd like to see, because we actually would like to know, I've had cases where I've kind of gotten to the point where I've

actually filed a lawsuit, and I've had defense counsel call me up and say, hey, if I told you all these additional facts, would you just go away? And I'm like, well, tell them to me and I will let you know. And they've told them to me. And I've said, by gosh, you're right. You know, it was a zero-day event that couldn't be sort of prevented. You know, that the data breach couldn't be prevented. You know, yes. I will fold my tent and go away. I'm assuming that, like, the facts are there and there's some basis to bring a claim, and the data set is, something that's sensitive, we'll look to bring claims for negligence, which is really just sort of the failure to exercise due care. What would the reasonable company do in similar circumstances? We will bring in generally a claim for breach of implied contract, because, as one court has said, in this day and age, it's just not really credible to believe that somebody would hand over their data without at least an implied promise that the data is going to be protected. We will bring, claims for invasion of privacy, which is kind of an old tort, an old legal claim that has found some new life in this data breach sphere. And, you know, we say at least in our pleadings, that's an injury unto itself, that your privacy, your private data, has been sort of breached, by this, this data breach and, and a company failing to protect it. There are statutes, consumer law statutes, and all the states will bring the consumer claims, under different state laws, the most noteworthy being California, where they've, basically instituted laws that not only allow for private rights of action, meaning that normal people can bring these claims, but they will give statutory damages if your personal data is breached under the California Consumer Privacy Act, you can get statutory damages, legal damages between $100 and $750 per person. So, we look at, you know, different claims, and, different plaintiffs' attorneys have a broader aperture in terms of what they think is going to fly. So you'll see things like bailment, you'll see things like, breach of fiduciary duty or breach of confidence. There's a laundry list of claims and, we try and keep it simple and only bring the ones that we think will really be viable. Other plaintiffs' attorneys take a kitchen sink approach.

[Kevin]: Right. So all right, so that's helpful. Thank you, David. So let's say we've reached a point where you have decided to represent me. We bring a data breach class action lawsuit. You assert these claims—negligence, breach of implied contract, privacy, maybe some others. And the other side, the defense side makes what we call a motion to dismiss. They ask the court, you can dismiss this lawsuit without any further proceedings because there hasn't been a concrete injury to confer standing. But let's also assume this ...we'll cut to the chase. Let's also assume that the court denies that motion. And so now you're facing the prospect of conducting discovery, which can be expensive for plaintiffs who are not... you're not earning anything until you settle the case or win a judgment and certainly can be expensive for the defense. So at some point, and you tell me, I think fairly early on after that motion to dismiss is denied. The parties sort of look at themselves and each other and say, is this the right time to start talking about a settlement? Can you walk us through that? How does that issue come up? And then what's the process of settling? And then we'll talk. We'll maybe spend a little more time on what are the key features of a data breach class action settlement.

[David]: Sure. So we're actually even more audacious than, waiting until, the motion to dismiss is fought out. And we will raise, the prospect of settlement at the earliest juncture possible. Because, you know, we believe that actually we're in the same business in some sense as the defendants and their insurers, which is the risk management business. So we realize that data breach cases are risky propositions from the plaintiffs' side and that, there's plenty of pitfalls, that will trip up a plaintiff and will result in no recovery at all. So, you know, we sometimes just go to the defendants very early in the process and we say, what would you like to do with this lawsuit? You know, we know the breach has happened and, you know, we've done our pre-suit investigation. We feel there's a good-faith basis for our claims. We've got some clients here who have, you know, kind of strong misuse, some actual fraud or identity theft, that generally will support the allegations. You know, do you have any interest in resolving it early? And sometimes the defendants will say, yes, that seems like the prudent course of action. And so then we will generally, do some voluntary pre-mediation discovery. We will generally commission the services of a private mediator. We'll schedule it. We'll all get in a room and have the assistance of a trained neutral and we'll try and come to some reasonable resolution. And more often than not, that's successful. And, the whole thing goes away. Now, you could say. Well, that seems too simple, but, you know, it's in everybody's best interest because the defendant is managing their risk. You know, and then at that stage, at least while I'm not suggesting that defendants are forthcoming in their pre-

mediation discovery. They still hold most of the cards in terms of knowing really the extent of the breach and how bad it was. And how their systems failed, and what degree of potential culpability they might have. So there might be some reasons, you know, that, it's just going to get worse. If we really open up the hood of the car and look underneath, it might be better to just leave that hood down and go try and resolve this and take care of it early, without too much fuss or muss. The same thing happens after the motion to dismiss stage and my typical sort of description of this data breach litigation sometimes is: it's like a bare knuckle boxing match where each side throws one punch. So the defendant throws their punch, their motion to dismiss. We throw our opposition into the motion to dismiss. And we hope that, we're still standing after the first punches are thrown. If, we are successful, basically, you know, we will then get the defendant to come to the table. If they're successful, we're kind of out. And we have to decide whether or not just to go away or to appeal and try and fight another day or in another forum. But as you said, plaintiffs' attorneys don't get paid until there's a resolution. And so we're always keen to try and resolve these cases, and not to drag out litigation, which is very expensive from the plaintiffs' side as well. And can take a long time. You know, we do kind of hand-select some cases to take deeper and let's just say they go on for years and, you see assessments on the plaintiff's side, you know, in the tens, hundreds of thousands of dollars and you're carrying quite a, a load of expenses in the meantime.

[Kevin]: Yeah. I want to get to the benefits of the settlement, but you mentioned, you didn't say roadblocks or challenges, but, you know, some of the barriers to plaintiffs in bringing these class action claims. And one of the ones I wanted to highlight and get your take on it is causation, because, of course, we've all gotten more than one notice of a data breach, notice of a class action settlement. And so in this day and age, it can sometimes be very difficult to know. Let's say my data is out there on the dark web. How did it get out there? If I come to you and say, I would be interested in suing this business, it's hard for me sometimes to prove whether my data is out there because of something this business did, or whether it's something that happened to me a year or more ago. How do you sort through that David, and where do you see that issue of causation landing in the next year or two years in litigation?

[David]: So causation, and another concept called traceability, are closely related concepts but slightly different. Traceability is this concept that you can trace the injury to the particular event. And that's kind of become the new battleground or one of the new battlegrounds in these data breach cases for just the reasons that you said, Kevin, which are how do you trace what's happened here, even if you suffer fraud or identity theft to this particular data breach, where, data breaches are ubiquitous, where every single person in the country probably has had their Social Security number compromised in a huge recent breach. Where, you can go on a , really, pithily named, website called "have I been poned.com" and type your name in and find the 20 or 30 or 40 breaches that you've been involved in, where your iPhone will tell you, that half your passwords have already been compromised and you need to change them because they've been compromised in some data breach that you didn't even know about it. It's a real question of how you trace any particular injury to a particular breach. And, you know, for our purposes, at the beginning of a case, we use a real common-sense approach, which is, number one, is there sort of a temporal connection? The breach happened, and the data was compromised and exfiltrated, stolen out of the defendant's system, and then immediately after some fraud occurred. That's a pretty strong temporal connection. This happened right after this. Also, there needs to be, ideally, kind of a logical connection between what data was stolen and what happened. So, you know, somebody says, well, I had, you know, fraudulent payment card charges. And then the defendant says, well, you never gave us your payment card. How do you trace that back to our data breach? Ideally, we have those sort of logical connections and the standard for what plaintiffs have to show changes over the course of the case. So at the initial stages when you just filed the case, it's a real low standard for traceability and really just kind of that logical, plausible connection. But later on, as the case goes deeper into litigation, you know, the plaintiffs are really put to their proof. And you see this in, really high-profile cases like the Blackbaud breach, where the plaintiff sort of survived the initial motions to dismiss the initial challenges. But eventually, after a lot of discovery and after expert disclosures, where you the parties were already into the very expensive battle, the experts, the defendants really won on traceability, that the injuries that were being complained

about by these particular plaintiffs couldn't be traced back to the Blackbaud breach. And so, you might say, from a defendant standpoint, well, we should fight all those cases because we're always going to win. We're eventually going to, you know, beat the plaintiffs when they're really put to their proof. But, you know, there's a huge expense to that in terms of just out of pocket dollars for paying defense costs. The expense of, you know, having all your own people dragged in for depositions, having your entire company turned upside down as plaintiffs' lawyers look at everything and anything that could have led to this data breach, you know, all your policies and procedures, all of your systems, it gets very expensive, very time consuming, very invasive. And, you know, yeah, you might ultimately win, but you kind of lose because, you spent tens of thousands of person hours to prove your point.

[Kevin]: [garbled] So, if you haven't spent that time trying to upgrade, you know, you're fighting a class action, but you also ought to be focused internally on what are your policies and procedures, what is your training, what are the right, how are you going to upgrade your physical, electronic and legal safeguards? So you're really fighting two battles at once? Yeah, it has to do that. We we've had clients who have done that. But let's say you decide, well, we prefer the settlement process because we can come to an arrangement. Maybe it's covered by insurance, maybe it's not. And so when you reach that point, David, what are the key elements of a settlement? What benefits are you looking for? And how have those evolved over time? I think they have a little bit, yeah. What are you looking for?

[David]: Well, so there are certain "buckets" of relief if you will, or, you know, types of relief that can be offered to the victims of data breaches, that will really address the harms or the potential harms that they have suffered or will likely suffer without some relief. Kind of key among that, and kind of, you know, not necessarily a controversial one, but one that is, you know, we go back and forth on... is some sort of form of identity theft protection, credit monitoring. And there are new products being rolled out all the time. So there's no specialized monitoring for minors. There's specialized monitoring for medical information. And so there's just this whole host of products out there that, are intended to sort of protect you from what might happen down the road. You know, and we offered those routinely in our data breach settlements, that we did three, four, five years ago. And, and before that time, having the ability to sign up for some sort of identity theft protection was kind of de rigueur, for a data breach settlement. These days, though, what we found is, again, as there's been so many breaches, most people who want some form of identity theft protection already have it. And so when you offer that or make that the centerpiece of a settlement, you run into this situation where a lot of people say, I don't want that. I don't need it, I already have it. So, a personal story, I actually have data protection through the US government because my wife applied for some security clearances for her job, and then I was the co-subject of the investigation. And then when the Office of Personnel Management breach happened, I all of a sudden had my data bound up in a big data breach. And I have gotten credit monitoring, identity theft protection from the US government now for going on a decade. And so if I—and I do... I have had my data breached recently, I've gotten three or four data breach letters just this year. And, you know, credit monitoring is offered to me. I don't need it. I already have it. So we've had to kind of adjust and sort of go a different way. And I had a really interesting colloquy with the federal judge in Georgia where she said, you know, I've had some of these data breach settlements. And, my gosh, in this settlement, you got five years of three Bureau of Credit monitoring. And that's the good stuff. That's the gold standard. And nobody took it. What happened, Mr. Lietz? And so I had to tell the judge, well, people already have it, so we have to look another way. And so where we've gone is now offering, trying to offer more of a cash benefit to people, just to get people to basically take the benefits. And also with cash they can do whatever they want, like maybe they don't like the kind of monitoring that we got for them. Maybe they'd rather have a different product. Maybe they already have a product they pay for where they want to extend the term. Maybe they want to use it for something like Norton Antivirus that has dark web monitoring and dark web protection. So giving people cash just gives sort of flexibility. So we've been saying, we'll still offer you the monitoring, but let's do an alternative cash payment where, if you've already got the monitoring, you don't want it for whatever reason, you can just take some money. And that will compensate you for the losses that you've had. We also generally try and offer people the ability to claim for documented out-of-pocket losses. That's really important because we want

people who have really suffered losses to be able to be made whole for that. And, those are kind of the typical mine run, of, of things that we offer people. We also have in the past offered people the ability to claim for lost time. And, and that's a good one, too, because sometimes the real damage to people, as a consequence of the data breach is just spending your time sorting out the effects of it. Calling your credit card companies to check your... whether or not your accounts have been, compromised. Changing your numbers, putting a credit freeze on, you know, if you do have some fraudulent charges, sorting that out, it's all time-consuming, and it seems to make sense in a real logical way that people could be made whole for that time spent. So it's like, well, we'll offer you five hours at, you know, $25 an hour, and folks can just claim for that. So those are kind of, how we structure the settlements, and we do it differently for different cases. Again, to try and target the relief at what people have actually suffered.

[Kevin]: Right. I want to ask you about insurance, but before we move to that, let me ask you about the claims rates. So you put together this means of credit monitoring, alternate cash benefits, the ability to claim for actual losses. And yet many times, the claim rates are fairly low, less than 10%. We can make up reasons why that's the case. People really haven't suffered injury, they haven't suffered injury, they're not going to make a claim. At the other end you could say, well, people have suffered injury, but you and I and the folks that are there are watching or listening right now, I would say it's just very time-consuming and I just choose not to do it. Why do you think those rates are where they are, and is there any effort afoot to improve that?

[David]: We're constantly trying to improve the rates and really we have a big vested interest in having high claims rates. We want these settlements to be approved by courts. And courts are routinely scrutinizing the claims rates and saying, if you have some tiny claims rate, that's evidence that you don't have a good settlement and we're not going to approve it and you're not going to get paid. So, I think the days of, plaintiffs' lawyers really not caring about the claims rates or maybe even doing things where they try to keep the claims rates low. Those are gone. And we are constantly looking for ways to boost the claims rates. One of the tools that has been very effective is, to do what we call a... use a tear-off claim form. And it basically if you've if you've ever gotten a class action settlement notice that takes the form of a little postcard. Imagine that the postcard has a panel on it that you can just tear off, sign your name to, check a couple boxes, and drop it back in the mail. Postage prepaid, and you've made a successful claim. You'd be amazed, at how having that tear-off claim form plus the return postage so people that don't have to go scrounge up a stamp. How that increases the claims rate. It's just astonishing. You know, you will double or triple your claims rate by using something as simple and common sensical as that. I don't know why people don't make claims. I know for my own self like that, you know, it's as you say, I just don't want to take the time or can't be bothered. And, and I think there's a lot of people in that boat. I think that there is some skepticism about settlements these days. You know, people, particularly if they get, like an email notice of a settlement, they might think that that's fraud or an attempt to, like, steal their identity in and of itself, and they don't recognize it as something valid. And again, talking about a very recent experience, I was on the phone today with, a class member, an absent class member from a settlement I have down in Maryland. And the woman was like, I don't want to give up any of my personal information to make a claim in a data breach case where my personal information has been breached. So there are reasons for everything. So but we have seen the claims rates rising generally. Again, data breach is on the minds of Americans. And so people know that they can make a claim and that they can get some money, or they can get some credit monitoring, and people like that. So we've just generally been seeing the claims rates go up. And I hope to see more of it. You know, it doesn't hurt, I think either party, once a settlement has been reached to see the claims rate, at a robust level.

[Kevin]: So we're getting to the end of our time. Let's, I hope, unless you want to say something about insurance, I welcome it, but, what I thought I would close with, if it's all right with you, is, we have this opportunity. You're here. So I thought, what's one piece of advice you would give to an individual who experienced a data breach? And then what's one piece of advice you would give to an organization out there, what should you be doing right now to minimize the risk? Right. And I think it may be it may be awkward to have you give advice to a business, but I'm sure that you'd be the first to say, well, I'd obviously rather my

clients never suffer a breach. So what would you say to the individual? And then if you had do turn around and give some, good thoughts to the businesses themselves, what would you say?

[David]: For the individual, I would say, be proactive. That's my piece of advice. So again, the, notice letters that come from the companies often do offer some form of credit monitoring, identity theft protection. You'd be amazed at how few people take up the companies on that offer. And I'm like, why don't you? I mean, this is being offered to you for no cost. You should do this. This is going to help you because again, folks may think, oh, well, I want to sue. I want to be part of a lawsuit. You'll be much happier if you're...credit cards aren't misused if your identity isn't stolen, if you don't have to try and change your Social Security number, protecting yourself from the ill effects of a data breach is absolutely critical. And, you know, the keys to doing that are generally laid right at your doorstep via the notice letter. And does that undercut my ability to make a successful legal claim? It sure does. But again, my clients are ultimately going to be a lot happier if they don't suffer identity theft or fraud. So. So I'm a big proponent that like, people should be proactive and not necessarily jump to filing a lawsuit as sort of the default thing that you do on a hair trigger. As for companies, I would say, use basic common sense for like, you know, good cyber practices and hygiene and—the thing that blows my mind is when I do get into those cases where I go deeper into discovery and lift the hood on, like what's underneath, I am just amazed at how common sense doesn't prevail within companies. The things that the companies do, I just shake my head at, like, for example, storing administrator level passwords on a share file site. You know, a share file is like a shared database that everybody in the company can dump their documents on. And to have people who have administrator level passwords, which can unlock everything within a defendant's network and system, just hanging out on that share file where folks can come along and just grab it. I just I'm astonished. You know, multifactor authentication has been talked about a lot. And, everybody who cares about cyber hygiene in their personal life does some form of multifactor authentication these days. You get that secondary code on your phone. The fact that companies still routinely don't use that and, you know, deem it as an impediment to getting business done, again, astonishes me. Like this is common sense. Everybody should know this stuff. And so, you don't even need cyber experts really to come in and tell you what to do. Just looking at your own environment, yourself as a defendant and saying, oh my gosh, like dumb things that we are doing or aren't doing are kind of obvious. And we should just fix that, use common sense and fix some of that stuff and you'll fix a lot of the problems. But, you know, again, I think there's this sentiment among companies sometimes that doing all this stuff, just impedes the flow of business, and therefore we can't be bothered. Well, just wait until the cyber-actor gets in and, you know, has a multi-pronged attack, the first aspect of which is to steal a bunch of personal information, the second aspect of which is to drop the hammer and encrypt all your systems, and disrupt your business that way and hold you for ransom, and then to come back for the second ransom to try and get your critical information back. You don't want to do that. You you're much better...like ounce of prevention worth a pound of cure.

[Kevin]: Sage advice we're going to I'm going to have our producer Kyla Hanley, just snip this part of our discussion and release it separately. I completely agree with you. Sometimes I think we get caught up in comparing ourselves to another person, and what we ought to be doing is comparing ourselves in the future with where we are today. And you know, you don't need to worry about, do I have the best endpoint detection, do I have the best MFA do at the best this or that? If you don't have any of it, then anything you do will be an improvement. Of course, I've been advocating now, David, that businesses undertake a risk assessment. How, you know, you can do you can do it big. You can do it small. But there's a world out there now where I think organizations think, well, if I just check the box with these three things, I've done everything I can do. And unless you're evaluating your own system, I think that can be problematic. But.

[David]: I think so, too. Risk assessment is key. You know, people should treat cybersecurity like they treat their personal health like, you know, go get regular checkups. Look for problems ahead of times. Address them if you find them. Don't let them fester. Cancer detection is a great, great corollary. If you go get that very uncomfortable colonoscopy and get any polyps snipped out, your incidents of colon cancer goes down dramatically. The same thing is true for cybersecurity. If you find a couple of warts within your network and you snip them out, you're going to have a lot less problems.

[Kevin]: Yeah. No. And it's a great, analogy because you... your business can die. You can lose your reputation, you can lose hundreds of thousands, if not millions of dollars. And you don't want to find out the state of your cyber hygiene in the minute following a ransomware attack. So that's good stuff. Well, David, I have kept you for a long time. I really appreciate your coming on *Cyber Sip*. I think this is just an invaluable discussion and, I hope to have you back on.

[David]: Kevin, I would be delighted to come back on and thank you so much for giving me the opportunity. And, you know, this is an evolving space and, there's always more to talk about.

[Kevin]: David Lietz, senior partner at Milberg. So glad you could join us. I really appreciate it.

[David]: Thank you, Kevin.

[Kevin]: And thanks to all of you for joining us here on *Cyber Sip*. We're back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, and Spotify. Like, follow, share, and continue to listen.