Barclay Damon Live Presents *Cyber Sip*™ Episode 28: "What's Up With BIPA?," With Bryan McCarthy

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Bryan McCarthy,** Transatlantic Reinsurance Company

[Kevin Szczepanski]: Hey, everyone, this is a *Barclay Damon Live* broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Welcome back everyone. Today, I'm so pleased to have Bryan McCarthy, senior claims examiner with Trans Re, one of the world's leading reinsurers, with headquarters in New York. Bryan joins us from his office this morning. Good morning, Bryan.

[Bryan]: Hey, Kevin, good morning and thank you so much for the opportunity.

[Kevin]: No, thank you for being here. And I know before we start, you have something that you need to read for us, so go right ahead.

[Bryan]: Thanks, Kevin. Yeah. In terms of a disclaimer, I just wanted to say the information contained herein represents the opinions and views of the presenter and does not necessarily represent the views or opinions of Transalantic Reinsurance Company, Trans Re, or its affiliates. It has been made available for informational and educational purposes only and is not intended as legal advice. Neither the presenter nor Trans Re make representations or warranties respecting the accuracy, applicability, fitness, or completeness of the information presented, and Trans Re and the presenter hereby disclaim any and all liability to any party for damages arising from any use of or reliance on the presentation. No part of the presentation may be reproduced, published, or posted without written permission of Trans Re.

[Kevin]: All right, thanks very much, Bryan. And again, thank you for being here this morning.

[Bryan]: Thank you, Kevin.

[Kevin]: So the title of our episode is "What's Up with BIPA?"...BIPA being the "Biometric Information Privacy Act" in Illinois. But I think before we start talking about what's up with BIPA, we need to hit the basics. So BIPA deals with the protection of biometric information. Bryan, can you just give us a rundown? What kinds of information are we talking about here?

[Bryan]: Oh, sure. Biometric information, most commonly, we think of it as fingerprints, iris or retinal scans. There's also voice recognition, though, and a big-ticket item now is facial geometry and facial recognition.

[Kevin]: So I know you have a good story about how BIPA came to be, what is the Biometric Information Privacy Act? And share with us what you know about why it got enacted. I understand it was unanimously enacted by the Illinois legislature, by the way, which cannot possibly happen every day. Tell us about that.

[Bryan]: Well, yeah, Kevin, it's very interesting because in doing some research, right, the consensus is I think that BIPA is the most stringent of the biometric privacy laws enacted by any state. And sort of

interesting to think about the history of kind of what led to that. Right. No coincidence. You do some research on it. Essentially, BIPA was enacted in 2008, hard to believe because it's such a hot topic now in 2023. But it was actually enacted all the way back in 2008 and there was a company called Pay by Touch. And what they had done back in '07 and '08, they were linking consumer's credit cards to their fingerprints, and then those consumers were utilizing their service to pay for items at retailers within Chicago. Fast forward a little bit, the company went bankrupt, and wouldn't you know it, in the bankruptcy proceeding, one of the assets that was listed for sale was the biometric data of all the consumers.

[Kevin]: Ouch.

[Bryan]: I don't think anyone anticipated that ever would have been the case. There was a lot of upset. Right. And then lo and behold, shortly thereafter, we see that BIPA was passed.

[Kevin]: I think there was upset back in 2008 when it was passed. And I think it's only gotten worse since then. I think today we are at a low point in our country with consumer confidence in the willingness and ability of businesses to protect information. We don't have a high degree of confidence that that's happening.

[Bryan]: That's interesting to you, Kevin. I think it's definitely on the radar of consumers, more media than ever, and a lot of the settlements that we may talk about that are publicized. Right. And some of the facts behind those cases are probably getting into the public discourse as well. So folks are definitely aware of this now, perhaps more than ever.

[Kevin]: So tell us a little bit about what BIPA requires, Bryan. What is it that a business has to do to comply with the law and then we'll get into what businesses have to comply with it?

[Bryan]: Sure. Well, you know, it applies to private entities, right. So non-governmental entities. But essentially when you boil down the provisions, there's three main aspects of it. The first is obtaining consent from the Illinois resident and that's an important distinction too: Illinois residents. And not just consent but written consent to the collection, the next part of it is, is a written and published or publicly available plan for the retention and how the data will be used. And finally, a written and published plan for how the data will ultimately be destroyed. And the only other thing I would add in there is, I think based on the Pay By Touch issue, the data cannot be sold. So essentially, those are the ultimate protections that it offers.

[Kevin]: Right. And as part of that consent, it has to be a meaningful consent. Right. So the consent needs to inform the Illinois citizen that their biometric data is being collected, who is collecting it, and why it's being collected.

[Bryan]: Right.

[Kevin]: So critical statute and as we talked about before, Bryan, there are very easy ways that a business that is responsible for complying can get tripped up. So before we get to how they can get tripped up, let's talk about what businesses are subject to BIPA. Low-hanging fruit would be businesses that are headquartered in Illinois. Obviously, they have to comply. Is that it or are there more?

[Bryan]: No, and that's a key distinction. But yes, absolutely. Businesses headquartered in Illinois. But what I think some other companies were tripped up because they didn't necessarily realize you don't have to be headquartered in Illinois, you can do business in Illinois, or you can transact with Illinois residents and still be subject to the statute.

[Kevin]: So—and I was talking with a friend of mine before we got on this morning who is in New York. We were talking about hockey and MSG. And MSG is known to collect biometric data from time to time. So if I'm

in a New York City hockey game and the Chicago Blackhawks are in town and there are Blackhawks fans in attendance and their biometric data is collected without notice or consent, that could be a problem.

[Bryan]: I agree. Yep, absolutely. Because ultimately it was enacted to protect the residents of Illinois.

[Kevin]: So what's the remedy for an Illinois resident whose biometric data is used, taken, stored without this written consent? What can happen?

[Bryan]: So this is, I think, where BIPA differs from almost any other statute. Each resident has a private right of action under the statute for a violation, not necessarily for actual harm suffered. So, for example, actual harm suffered could be there was a BIPA violation and it resulted in identity theft. Right. You may have suffered some actual damages. That's not the case here. Each Illinois resident has a private right of action for a violation. And then we get into sort of the calculus of how much each violation is worth under the statute.

[Kevin]: There are...and as far as determining how much each violation is worth, Bryan, there's a statutory range of damages, isn't there? I think it's $1,000 to $5,000 per violation, isn't it?

[Bryan]: That's right, Kevin. $1,000, I believe is the negligence standard. And then a... $5,000 is for reckless or intentional.

[Kevin]: So if you've got 500 or 1,000 or more individuals whose data is collected without their knowledge or written consent, you multiply that by even $1,000, you can start to see how this is a potentially significant exposure for businesses that are dealing with Illinois residents.

[Bryan]: Absolutely. And, you know, I'll add in the statute itself allows for the recovery of attorney's fees if violations are proven. And it goes actually as far as to specify attorney's fees plus litigation costs and expert fees, it actually delineates those specifically. So that alone can be pretty costly regardless of...

[Kevin]: Right.

[Bryan]: ...the actual violation calculation.

[Kevin]: Right, as you and I know from our past lives, the attorney's fees can be expensive and expert witnesses can be expensive. So the fees add up. And your point about attorney's fees is a good one, and leads to my next question. So with the actual harm being essentially irrelevant to the ability to bring a claim and these statutory damages, $1,000 to $5,000 plus attorney's fees, sounds to me like there is a lot of incentive out there for lawyers to find clients and to sue businesses under BIPA. What are you seeing in terms of lawsuit trends?

[Bryan]: Yeah, I mean, so again, I keep coming back to the fact that it's so interesting that we're talking about a 2008 statute now in 2023 that's causing a lot of concern. Right. But there was a case in 2019, I believe it was the Rosenbach case, where the Illinois Supreme Court confirmed that a private right of action was available to residents. And I think the ultimate definition is if you're aggrieved. Right. So you don't need actual harm. You just need to be aggrieved. And you have this private right of action. I think from 2015 to 2019, there were a number of class actions out there. From 2019 forward after the Rosenbach decision. Just after that, there's over a thousand class actions filed just from 2019 on.

[Kevin]: Are they mostly in Illinois or have they expanded to other states as well?

[Bryan]: Well, under the statute, they're mostly in Illinois. You know, one of the interesting issues is, you know, it's not like... we're talking about it's not just Illinois companies that are being sued. But, you know, there were some larger companies that settled within the last year or so, Facebook, TikTok, Google. They weren't

necessarily certainly... not exclusively doing business in Illinois, but they learned they were subject to the statute as well.

[Kevin]: So, again, you can be a business that is located in New York, for example. And if you collect data on Illinois residents and you don't comply with the statute, you can be sued in Illinois or maybe elsewhere for violating BIPA.

[Bryan]: Yeah, and I think that's news a lot of folks that may have been aware of that, especially, you know, if you have an insurer that's writing a policy to a company that's not headquartered in Illinois, you know, the insurer and the insured company, I think, both need to be aware that this statute is out there and may apply.

[Kevin]: And there was a recent case, wasn't there, Bryan, the Rogers case, which just went to trial this year, I believe. So. Can you talk a little a little bit about that case? Because I think our viewers and listeners would be interested to know that these lawsuits can get very expensive, not only from a legal defense standpoint, but from the potential verdict and settlement that you could be suffering as a result of violating the act.

[Bryan]: No, thanks, Kevin. That's right. I think it was Rogers versus BNSF. And essentially the facts as I understand them was, you know, BNSF had rail yards and rail cars in Illinois and they were requiring truckers to use fingerprints to get access to the yards, to get, you know, to get the cargo. It was alleged, and they were sued, essentially saying that BIPA was violated in terms of the consent provision and the notice provision. This was just back in October, I think, Kevin. So only a few months ago...

[Kevin]: Right? The verdict...

[Bryan]: The verdict came out and I believe it's the first case of its kind to go to verdict. Right. I think what we see is most of them settle. So the numbers were pretty staggering, right? $228 million. The plaintiff class, I believe, was somewhere between 44,000 to 50,000 truckers.

[Kevin]: Right. 45,000.

[Bryan]: 45,000. And I think if you...if you kind of do that quick math, the numbers at the high end of the $5,000 threshold per violation. So the jury came down pretty hard. And again, I think that was a little shocking to folks to see those numbers out there.

[Kevin]: No, that's very significant, because if they had been hit with just the thousand-dollar penalty or damage under the statute, it would have been only $45 million. So you're absolutely right. The jury was was definitely not happy with the defendant in that case. But as you say, having just. Oh, go ahead. Yeah.

[Bryan]: Now, I was going to I just find it funny that we do say "only" $45 million. Right. So that can show us just how impactful this statute....

[Kevin]: A big number.

[Bryan]: I don't have it, right.

[Kevin]: No. And it's funny, but it proves the point too. So if you're an organization out there and you are dealing with more than a thousand potentially affected Illinois residents, and this statute permits damages in the range of $1 to $5 million... Right there you're looking at an exposure in the $1 to $5 million range, plus attorney's fees and the time and the aggravation factor that you will incur defending that case over what will almost certainly be many years. Right, because you're dealing with a class action.
[Bryan]: I agree, Kevin. And we've seen these cases take a long time to cycle through. I think one case

was filed in 2017, just settled recently. I think it was the Hyatt case. Also, there's a lot of challenges in defending these cases, which I don't know that folks may particularly like.

[Kevin]: No, I was going to ask you about that. We talked a couple of weeks ago about this very thing: you get lawyers like me coming in and saying, hey, we've got a great strategy. We're going to be able to defend this. We're going to be able to get this case dismissed. And I imagine you hear that a lot because lawyers are representing these businesses that are being sued and they're trying to achieve the best possible resolution for their client. But as I think you and I have talked, it's not as easy as some might think to defend these cases. What are some of the challenges that make it difficult?

[Bryan]: No, sure. I mean, for starters, it's hard to believe just based on when this was enacted. But there are still some key elements of the statute that have not been defined by the Illinois Supreme Court. So let's start at the basics of trying to narrow down the class size. There's an open issue as to what the relevant statute of limitations is for a BIPA claim. I think I see it's split between the the last decision I read, I believe, from the appellate court was one provision, may be one year. Another provision may have a five-year statute. And the Illinois Supreme Court, as I understand it, is going to... has taken that issue up. But at this point, there's no... there's not necessarily any law of the land in terms of even how you can definitively narrow your class size based on statute of limitations. So you start right there.

[Kevin]: So let's tease that out a little bit for our viewers and listeners. You're in a situation where you're sued and something as fundamental as the statute of limitations, in other words, how much time do you have to bring this suit? If it's only one year, then in effect, you've only got a one-year lookback period for potential victims. Right. But if it's a five-year statute of limitations, then anyone whose data was improperly collected without written consent over the prior five-year period...

[Bryan]: Yeah.

[Kevin]: ...is potentially part of that class. So I'm just making up numbers for the sake of, of example. But if you assume a thousand Illinois residents per year, if it's a one-year statute, you're dealing with a thousand residents times $1,000 in damages. But if it's a five-year statute of limitations, you could be looking at a risk that's five times greater. So that little issue of the statute of limitation is actually very important.

[Bryan]: Agreed, and almost like a threshold issue of trying to define, you know, what the scope of the damages could be because you don't even know how many how many plaintiffs have viable claims. And then another key issue, Kevin, which I found interesting when I was researching it, you know, the statute talks about a violation. Well, I also believe the Illinois Supreme Court will be defining...is a violation, you know, per individual rate or per incident. So, for example, a lot of these cases and I think a lot of the earlier ones, too, and we can talk more about how it's expanding. But a lot of these cases were, you know, when you clock into work, right, you give your fingerprint. When you clock in and you clock out, it helps the employer track time, payroll, etc. So, you know, what was what was essentially happening is, you know, if you have a violation because of either notice or storage or consent, you know, okay, is that a violation for each individual that has a viable claim as a plaintiff? Or is it every time every individual clocked in and clocked out during the relevant period? Right. And you start doing that multiplication and that becomes a little, you know, that becomes a little... a lot more expensive. So those are great key issues, I think, that still have to be worked out. Sorry, Kevin.

[Kevin]: We're... no thank you. So you're talking then about each Illinois resident has either one incident or maybe hundreds of incidents if they're clocking in and out. And then you multiply that by the statutory damages, and you can easily get to that that "small" number of $45 million. What are some of the other issues that you're seeing, Bryan, in addition to the statute of limitations and the definition of violation?
[Bryan]: Well, I think the challenge also is, you know, a technical violation is sufficient to prevail from the

plaintiff's side. Right. So, you know, I ...and from what I had read, too, early on, I think a lot of the defense strategies involved around sort of pointing out the equity of the fact that there were no actual damages here. The case should be dismissed. Well, now we know that that's irrelevant. So, you know, can you prove that you were in strict, perfect compliance with every element of the statute? And perhaps you have experts saying you were, and you have depositions and you have discovery and you review the written policies to make sure. But again, right, on the defense side, I think the deck is stacked against the defense because any technical violation, it doesn't have to...As we said, it can be just basic negligence. That's enough for the plaintiffs to prevail.

[Kevin]: Before we close, I ask you one final question, Bryan, I just want to underscore for our audience that this is not a problem that's limited to companies that are headquartered in Illinois. We've seen in our end, in fact, we're defending right now an insurance coverage case arising out of the settlement of a BIPA class action lawsuit. And while, as you said, the lawsuits commonly take place in Illinois, the defendants in that lawsuit were New York businesses. They had provided the point-of-sale machines to restaurants that were using those machines to collect biometric data from their employees as they logged in and logged out every day.

[Bryan]: Okay.

[Kevin]: And so if you're out there thinking, well, I'm not headquartered in Illinois, so I don't have a problem, you need to expand your look and think about whether you're doing any business in Illinois. And even if you're not doing business in Illinois, are you collecting biometric data for any Illinois residents? Oftentimes that can be the case. Even if you're not actually doing business in Illinois or headquartered in Illinois, right, Bryan?

[Bryan]: I agree, Kevin. And I think that's what we saw with the Google settlement, right? I think it was essentially photographs that were tagged with personal biometric information and that was an issue.

[Kevin]: So it's something that we all need to look carefully about. We need to do an inventory, you know, where are we doing business? Whose data are we collecting? Where do those individuals reside? Let me close with a question, maybe a hard question, Bryan, but I know our audience will want to hear from you: As a reinsurance adjuster, what are you focused on when it comes to BIPA claims? What keeps you up at night when you think about these risks?

[Bryan]: Well, you know, it's interesting, right, Kevin, because, you know, on the reinsurance insurance side, we have a little bit more of a bird's eye view in terms of trends and things like that. It's a tough question, but I think the answer is relatively basic, right, in terms of: it all starts with a conversation. In my opinion, the insured, the carrier, perhaps the broker and the insured carrier and the broker should have a conversation early on to determine if BIPA compliance is at issue, meaning if the insured is subject to the statute. Beyond that, the underwriter perhaps and the insured can discuss the insurance policies and procedures and that sort of thing. But also to have a conversation to say, hey, this is at issue and here's the intent for where the coverage should fall if it is intended to be covered at all. And having that conversation early, number one, making everyone aware that the statute may apply. Then also talking about policies and procedures and compliance and then talking about coverage. Because at the end of the day, the worst thing I think that can happen is a surprise. Right. Someone didn't think it was applicable. And then they are sued. And then there's a coverage question and the dispute. And I don't think anyone wants to be there. Right.

[Kevin]: Right. No, that's a great point, Bryan. So what I'm hearing you say is when you're thinking about your potential exposure to BIPA claims, got to first determine whether you are exposed. If you're not headquartered in Illinois, are you doing business there? Are you collecting data from Illinois residents? And then have the conversation about risk management. So what security controls do you have in place? Are you disclosing, as you should, to the Illinois residents whose data you're collecting, what you're taking, why

you're doing it, and are you getting written consent? And then on the other hand, do you have security controls in place, physical, electronic safeguards to protect that biometric data while you have it? And then finally—and I know we're out of time, but I want to talk maybe on another episode—about the potential insurance coverage. Because that's another critical form of risk transfer that can potentially save the day if you have the right coverage in place.

[Bryan]: Absolutely. And Kevin, you know, I like to talk coverage. And we both we both enjoy talking.

[Kevin]: We both do. Yes, we both do. Well, that sounds like a good place to leave it. Bryan, thank you so much for coming on. I really appreciate it. And I want to have you back on another episode to talk about insurance coverage for BIPA claims, if that's okay.

[Bryan]: That would be great, Kevin, and thanks again for the opportunity. Really appreciate it. Thank you.

[Kevin]: No, thank you. And thanks to all of you for joining us on this episode of Cyber Sip. We'll be back soon with another episode. Take care.

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

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.