Barclay Damon Live Presents *Cyber Sip™* Episode 46: "Toward a Trustworthy AI," with Justin Daniels

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Justin Daniels,** attorney, Baker Donelson, and cohost of *She Said Privacy/He Said Security*

[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]: Justin Daniels you are corporate M&A and technology transactions partner at the law firm Baker Daniels. You're based in Atlanta, right?

[Justin Daniels]: Baker Donelson. And I am in our Atlanta office. Yes.

[Kevin]: Okay. And there you are, counseling and helping companies solve complex cybersecurity and privacy challenges throughout their lifecycle. But for those that don't know, you are also cohost of the award-winning podcast, *She Said Privacy/He Said Security*, with your wife, Jodi Daniels, and you are the coauthor with Jodi of the bestselling book, *Data Reimagined: Building Trust One Byte at a Time*. And I'm going to read you some quotes when we get a little farther along in the in the episode. See if you still agree with them. But seriously, welcome, Justin. It's a great pleasure to have you on.

[Justin]: Thank you. I look forward to our "book club."

[Kevin]: Yes, absolutely. So today we're going to talk about AI and I think eventually are going to come on to the NIST framework for trustworthy and responsible AI. But before we get started, I just thought we'd just help our audience with the basic question, what is AI? Because... maybe you can just give us a brief, an overview as you like, because really artificial intelligence has been in our world personally and professionally for many years. And I think right now what we're focused on is a particular type of artificial intelligence, those including transformers and large language models. So could you maybe give us a little overview for some context?

[Justin]: Yes, I think the real transformation with ChatGPT last November is, as you said, with a transformer. And so what AI has evolved into is now you're seeing it being able to take large amounts of data and be able to analyze it and come up with very human-like responses. You could query it and say, hey, who is Kevin Szczepanski? And it'll give a whole seemingly well thought out paragraph or two about who you are and that is really what's been the game changer when it comes to AI and its ability to create thoughtful content that is like, that seems very human, like.

[Kevin]: Mm hmm.

[Justin]: And that's a level. That's what we have.

[Kevin]: Yeah. No, I appreciate that. And. And there are security risks associated with it. And I just on that point, I wanted to draw from James Dempsey's work, which is—and you had him as a guest— James Dempsey, who is by the way, for those of us that don't know, senior policy adviser for geopolitics, technology and governance at the Cyber Policy Center in Stanford, great interview that Jodi and Justin Daniels did with Jim Dempsey on the He Said/She Said podcast, which by the way, you can find where? Where's the best way to... best place to find your podcast?

[Justin]: Just we're on Apple and Spotify and all the typical places. So you can even go to the website for Red Clover Advisors dot com and all of our episodes are there. We've done now over a hundred of them.

[Kevin]: Which is amazing. Yes, I pick them up, sometimes on LinkedIn, but I am subscribed on Apple Podcasts and that's probably the easiest way for those of you that would like to access it. So I wanted to borrow from Jim Dempsey's piece on AI, and he says, and I'm quoting now, "it is also clear that ML, meaning machine learning, training methods and irresponsible deployments of AI systems can compromise the privacy of both users and the individuals whose data was collected for training purposes, running afoul of privacy laws and principles, and possibly requiring a disgorgement of that data." And yet he goes on to point out that OpenAI and Microsoft have seemingly ignored their own warnings and failed to implement appropriate control measures to address these privacy and security issues. In fact, OpenAI, according to Jim Dempsey, has expressly said that it is taking a quote, fix it later, unquote approach. So with that is our context, Justin, what are some of the privacy and security risks associated with these large language model AI tools and why? And I'll let you...this is a long and crazy question, address it however you think best. Why, given the risks, have the large data companies taken this wait and see or put it out and fix it later approach?

[Justin]: So let's start with the first part of your question about the privacy and security risks. So when you're evaluating an AI tool, ChatGPT, whatever you have... is in order for these tools to work well, they need to analyze lots and lots of data. So in order for something like ChatGPT to work, they need to go and find a lot of data. Well, where is the cheapest place to find data that you don't have to pay for it. Go on the internet and you scrape it. Are they the only company to do this? No, a lot of the other like facial recognition companies have done the same thing. What the challenge is, is you may go and scrape data of people that even though it's on the Internet, it still has personal information, even though, you know, your LinkedIn profile is out there, has some personal information, that's still PI. And so there are certain state laws, California being foremost among them, that have requirements on your collection, use, sharing of data. From a cybersecurity perspective, you have the potential vulnerabilities of the chat bot itself. But I think what's going to start to happen with cybersecurity is... most of the kind of data breaches we've seen fall under two places in what I call the CIA triad: C is confidentiality. Obviously, a data breach breaches confidentiality. Ransomware handles the A, which is Availability. Someone locked encryption network. It's not available, however, I believe where the mischief will lie with AI, will be injecting malware into the data set so the answers that AI gets are off base. And so it goes to the integrity of data. On top of the fact that it's well known that AI already hallucinates. The other issues are around. You've seen people been able to jailbreak AI and get around its control so you can ask it, how do I build a Molotov cocktail?

[Kevin]: Mm Hmm.

[Justin]: And things like that. And so it really brings to the forefront are what kinds of security risks are and how they are evolving with this new technology.

[Kevin]: Can I put you on the spot Justin? How does what they call "prompt injection" play into this? I think, you know, generally can let's talk through that a little bit. I think just in its most general basis, it's the ability of a bad actor to interfere with the prompt process and it can result in theft of misdirection of emails or other information. Can you talk us through that a little bit? Because that's an issue that I don't think everyone is thinking about. That's going to be a problem in the next 12 to 24 months.

[Justin]: Well, when we talk about prompt injection, you're talking about a threat actors' ability to go in and input information that can help create vulnerabilities or cybersecurity threats or, for example, what if a threat actor wants to say, hey, ChatGPT, I want you to review this code? But the code has malware. And now what you've done by asking ChatGPT to run the algorithm is you've put that malware into their... potentially their training set. And so and I know we're going to talk about this. To me, the challenge is, is how do you start to think about managing risks holistically from the outset? But the problem is, and this isn't unique to AI, is the businesspeople see a market opportunity and they want to be first to market. They want to get there fast. You've seen this with social media, you've seen it with search, you've seen it with Zoom. And so they want to push out ahead and they don't want to be bothered by the inconvenience and the time it takes to really think through this risk management, which is really what we're talking about when we talk about the security risks, the privacy risks. And so their view is, is we'll just get out there quick, get market share, become a big company, and if something bad happens, well, at that point, we'll have money and we can fix it then.

[Kevin]: Right.

[Justin]: That's a mentality that I see repeatedly when you talk to businesspeople, because for a lot of them, until they've experienced having their identity stolen or having a data breach, it just it's abstract to them.

[Kevin]: It's all hypothetical. And we are both we are both partners at large law firms. And so I think law firms tend to be careful and oftentimes market followers and not leaders when it comes to technology. So as careful as we are trying to make sure that none of our colleagues are misusing ChatGPT or, you know, looking up case law on AI and citing it in court, I mean, very... a quite a lot of the discussion is, well, how do we maximize this opportunity? And we want to be careful. We want to do the right thing. But too often we don't integrate those protections into the services we provide. Which kind of leads me to this boy here: Data reimagined. You and Jodi write a book bestseller on USA Today, Wall Street Journal. What am I missing? One more Amazon. And first, I've got to ask you, before we get to it, let's do a little pivot here. Why did you write this book?

[Justin]: Why did we write this book? We wrote the book for a couple of reasons. Number one, Jodi and I decided that we wanted to build off of our podcast and the brand that we had built. Each of us do speaking individually. People have us come speak together and we decided that, hey, you know, we felt we had a message to bring to the marketplace and there's never a good time to write a book. You just have to roll up your sleeves and do it. And that's what we decided to do. And the main message behind the book is businesses tend to think privacy and security are an afterthought. But the reality is privacy and security can be used to build trust with your customer because how you treat their data is by extension, how you treat them. And we go through various things. But if you ask me, that is the real thesis of the book and what we felt we could contribute to the idea is that we're out there around privacy and security and it's been very well received and we could have a whole podcast of what it's like to write a book, let alone write one with your spouse.

[Kevin]: We should do that. You guys should do that. No, I... it's very well received here and I think it's... there was a market for it. It's that it's been written and that it's been written so well and that those of us who may not be IT or information security experts, those of you out there who are running your organizations, this is a less than 200-page book that reads very easily. And it underscores what I... it's the trust; it's the business competitive aspect to cybersecurity and privacy. And I wanted to pivot then to a couple of points in your conclusion that I think lead in nicely to what we're going to talk about next with respect to AI. So you say on page 190, in your conclusion, "data reimagined" "in reimagining data, we've argued that the gold rush mentality of collecting as much customer data as you can grab doesn't translate into having a relationship with customers any more than stalking leads to love. But data collection that is respectful and consensual can build trust, which is an even more valuable and increasingly rare commodity." Later on page 191, this is your "command," if you will. "Build privacy and security into your business processes, from design to products to culture, and articulate and document this new mindset in policies and procedures that stipulate collection of only data for which you have a business use, which account for its privacy and security, and which comply with the wide range of laws that govern customers' rights, breach notification and purchasing of data." I think that's a great segue into our discussion of AI. And I guess my question is, I think we're going to talk about the NIST modules for AI, but how do you put those commands, those recommendations into practice when it comes to AI, Justin?

[Justin]: Well, it really starts from the top. This... the C-suite and the leadership; that they're saying, you know what part of our mantra is, we really care about building trust with our customers, be it business customers, or employees, what have you. So it has to start there because that will inform how the organization is going to go about dealing with AI. So that can be from creating your own AI or purchasing it from a vendor, the kind of process that you put them through, understanding where they're collecting their data, how are they being compliant? But and to your earlier question, that's where companies I think really struggle is there's such a pressure on the... from the C-suite, to get out there, do it fast, get market share that privacy and security are the afterthought and we want to flip that idea on its head. But in order to get there, you have to have companies that say, you know what, if it takes us another month or two or whatever to do this, we really want to make privacy and security a selling point of our product. Candidly, the challenge with that is if you're a startup and you want to get venture funding, they care about product market fit, getting the product to market and they don't want it to slow down. And so you run into "that's just how people think."

[Kevin]: Right?

[Justin]: And they don't appreciate the risks they have with privacy and security until they have a problem that blows up. I see this repeatedly when I speak on panels with either venture capitals or private equity firms and until they've had a breach or problem, they just don't see it that way. No matter what you say. I... the best analogy I can give you is this education is important, but it's not something that will happen overnight. I love using the example of seatbelts. Like, did you wear a seatbelt when you were young? Probably not. Your parents didn't really do it. And now we do it without thinking because we had education about it. We have laws around the use of seatbelts, so now, seatbelts went from an afterthought to something that you do without thinking. And that's why your show and things that we're all doing are important from the educational standpoint to make cybersecurity and privacy the digital seatbelt of the 21st century.

[Kevin]: Yeah, no, that's a great point. Just because I didn't wear a seatbelt and I didn't get into an accident doesn't mean I was safe. I think a lot of companies today, especially the smaller, the startups, they're moving 100 miles an hour and they think because they haven't had a breach that they must be doing everything right. And they're not, as you say, until you've suffered a breach. You don't realize what your shortcomings are. I want to put a pin in what you said about vendors, too. We could do a whole episode on that. But I think one critical point that that many are missing at this point and hopefully will be able to send the message is: if you're using ChatGPT or any one of a number of these, what is it, are we up to 19 now, different models, different products? You as an organization, especially if you're regulated, you have an obligation to do your due diligence and make sure that those models, that product, comports with your own duty to provide privacy and security safeguards. So if something goes wrong, you can point to ChatGPT and say, well, that was that's on you. But as between you and the people whose data you have, it's your responsibility.

[Justin]: And I think what will amplify that point will be the new SEC cyber regulations that came out earlier this summer because to me, that's a backdoor way to regulate AI, because if you're a publicly traded company and you're using AI and you have a data breach that comes from use of the AI, well, what were your disclosures about how you were managing that risk from a cybersecurity perspective? And if you don't have them, there appear there will be consequences for that. So I'll be interested to see as we get to December and beyond when these laws go into effect, how that plays out, because I don't know how you're going to get a lot of companies to care more about AI without regulation. And there's been a lot of talk in Congress about doing it, But I'm willing to bet you that California will pass an AI law before the US Congress does right?

[Kevin]: Right.

[Justin]: You know, the EU will likely pass their law early next year. It won't go into effect until 2025, but it gives you a good roadmap about how they're thinking about AI. But boy, what happens this next three years where people are out there in kind of the wild, wild West, right? I suspect some company will engage with AI in some way that looking back on it, you're just scratching your head is what were they thinking? Because

I think they're playing with something they don't truly understand. Because AI is learning, it is evolving, and the people who develop it don't always appreciate how that is taking place. And like I said, we're all learning. I mean, every day I'm working on it. We're learning something new. Things are coming out. I think, Kevin, in my view, I'll be the culmination of consequences likely bad that have occurred because Congress abdicated their role to put regulation in place to govern the 21st century economy. I mean, it's crazy to me that I have an Apple Watch that has really, health data on it. But HIPPA doesn't regulate that. HIPAA is from 1996... on Section 230 that people argue about. It was an afterthought in the Telecom Act 1996. We are in desperate need of an upgrade of our laws around our digital economy and Congress has just not done their job.

[Kevin]: Yeah, and it reminds me back at least to the historical analog to me are the 1930s era enactments of the Securities Act and the Securities Exchange Act that if you talk to anyone on either side of the political spectrum today, even those who favor as little regulation as possible, anyone, anyone intelligent on either side will tell you we needed some guardrails for the modern marketplace. And those rules have... they've stood the test of time. They've evolved. They're not perfect. But the FCC has been at the forefront, of this corporate maze that we have in the modern economy. Nothing on the cyber side. We're literally still waiting for the first meaningful attempt by Congress to provide to give us some certainty and predictability. I'm sure you've had... you've got you've got a maze right now of federal and state regulators. And I think I don't know what your take is. I think that, truth be told, the state regulators, when they're writing their rules, they've got the SEC and FTC regs on one side of the desk and they're borrowing, but it's very difficult to counsel clients these days because we say, well, we see what's in California, we see what's in this act. And they say, well, am I subject to that regulation? And then we have to... we have to try ...We have to counsel people correctly. You're either subject to a law or you're not. And if you're not, it is hard to convince a business to do. I don't want to say the right thing because it implies that they're doing something wrong. But it's hard to say to a business you really should have some policies and procedures in place, if at the end of the day they're not subject to the laws from what you're drawing, those policies and procedures, how do you manage that in your world when you're dealing with a client who may not be a regulated entity, but that still needs some guardrails?

[Justin]: I think it's difficult. You know, we wrote the book for the reasons that I stated, and that would be a goal. But I think by and large, companies that aren't legally required to do something, they don't want to be bothered. Now, there are a few who say, you know what, this is something about the culture of who we are, but they're more of the exception than the rule. Because if you think about it, as you and I talked today, there are now 12 states that have privacy laws that have passed their legislature here. Then, you know, on the federal level, FCC has some privacy laws, FTC has rules. HIPAA, Gramm-Leach-Bliley. And so if I'm a business and I want to do the right thing or I'm in a gray area, I mean, think about the cost you have to incur now to think about all these different laws that potentially could apply to what you are doing. And if it's in a gray area or it doesn't apply, companies look at it as, "Well. That's a the cost savings."

[Kevin]: Right.

[Justin]: And so, you know, and then I think the other thing to talk about is while we do have privacy laws, they've been watered down to an extent only California has a private right of action. But I'm not even sure that's the right remedy to get people's attention, because the only people who make money off of that are the class action lawyers who bring the case. I'm sure you're cashing your variety of the settlements for $7.62.

[Kevin]: And the lawyers, $20 million or $200,000. Right. Right.

[Justin]: But that's the one thing that gets companies' attention. But I don't know that it really helps the consumer who is the party really affected by it. So that's why I think you see some of these other things where there could be laws out there that says, hey, software developer, by default, you're the one who has to be in charge of the design of your software. Logically, that makes some sense, but the business community is going to pull all "That's going to cost us a lot of money." Well, now you're really talking about who should be responsible for the cybersecurity of a product. Is that any different than an autonomous vehicle? I think if you don't have good cyber, an autonomous vehicle, that's a product defect and there's a liability with that. So it's really bringing to the forefront, you know, what does it mean to have a safe product? Well, in this digital age, it should be one that makes you feel secure. You know, is privacy enhancing. And when we start talking about the RMF, the risk management framework, you're going to see these concepts are built right into it. And that's why I think it's, in my view, the best holistic approach to AI risk management that I see out there today.

[Kevin]: So let's go there now. Let's suppose, you know, I think what concerns the average person, the average American out there is, how can I trust that these large companies are being responsible and how can I trust the security of my data, my children's data, our financial information? And that leads us, I think, nicely to the NIST risk management framework for AI. So in our remaining time, Justin, let's talk about that. What do you make of it and give us an overview of how it works. And I know I started with what do you make of it? In giving us an overview, give us your take on whether you think this is going to be a real game changer for the marketplace.

[Justin]: Well, why don't we start with what is the challenge? So when I've spoken to companies who are trying to grapple with it, a lot of times for many companies it comes up in the context of my employees want to use it, so I need some kind of AI policy for employees using it, because if you think you're going to ban it, I downloaded ChatGPT on to my mobile phone last night... It's going to be impossible to stop.

[Kevin]: Right.

[Justin]: So I see that come up in that context. But the challenge is, is okay, maybe I understand what AI is, but what is trust and trustworthy and responsible AI look like. And so what does that look like? And so how do you come up with a comprehensive approach? Because a lot of people say, oh, we need trustworthy AI, it needs to be responsible. But they're pretty scant on, well, what exactly does that mean? So for those in our audience who don't know, NIST is the National Institute on Standards and Technology. It is a part of the Department of Commerce under the federal government that comes up with various frameworks for things like cybersecurity and privacy. And in the cybersecurity industry, NIST is highly regarded because it's nonpartisan. It's just looking to come up with standards that companies can use to really think about various things, in this case, AI risk management in a very comprehensive and holistic manner. So let's talk about well, what does that look like? Well, one of the things I like about NIST is they have what they call "attributes" of what does trustworthy and responsible AI look like. So here some of the attributes, it's reliable, validity. Another one is it's safe, secure, resilient, interpretability, transparent, privacy promoting. And then the other one was, you know, focus on limiting or taking limiting or eliminating bias. So what I like about this is, these are attributes. Now, does that mean you have to weigh all attributes the same? No. Does it mean some attributes could be at odds with others? Absolutely. You can have great privacy and transparent AI, but if it's often wrong but never in doubt, maybe that's not the best AI. And so what I like about it is, is if I'm a company and I'm trying to get my head around AI, it gives you a pretty broad-based approach of thinking about all these different variables and then saying, okay, here's what use cases look like to us. This is the context of the industry that we operate in what we're going to do. So what do these variables look like to us? And then it has four concepts. So one is govern, then model, measure, and manage. And so between those there, those four core ideas, there's like 72 sub steps. So really what it does is it gives you a really good comprehensive approach and it helps you start to think about and ask the right questions. The older I get, Kevin, the more I realize as a lawyer, what sets us apart if you really want to be good at your field, is, it's not knowing the answer. It's asking.

[Kevin]: The right.

[Justin]: Questions. We're paid thinkers. And what I like about this framework is it helps you think broadly about asking the right questions. The answers may vary from organization to organization, but when I've introduced this to clients, they see how they might have been thinking about things narrowly and not being able to connect the dots, and I feel like in my mind what's out there now, the risk management framework from this does a really good job of helping connect dots and help people to think holistically and comprehensively of, well, what is trustworthy AI look like, How do I want to manage the risk? How do I prioritize, assess the risk to my organization? Because it's very different from an e-commerce company to a health care company. I just published an article this morning on that topic with Bloomberg Law, but that's where I think it can benefit companies because—think about it, you're a pretty large company. You've got, you know, your privacy team, your security team, risk management team, and they're all very busy. Now you're going to load AI on to that. And then where does it sit? You know, privacy role can sit with the CIO. They could create its own role. It could be in marketing. Is its own thing or where does it sit? And what happens most times as companies try to do this on the fly, they make an expedient decision, which may not be a good long-term decision, but they're only looking at the 50 yards in front of them.

[Kevin]: Right.

[Justin]: And I feel like the NIST framework helps you think longer term so that you don't end up going in front of a board because you've had a data breach and have to explain to them, oh, well, we just trusted the vendor. We didn't do much diligence as opposed to here's a framework that you can use to start to figure out, what does our risk profile look like? How do we go about due diligence, that kind of thing.

[Kevin]: Right? So where the rubber meets the road, what we're talking about, Justin, is an organization you decide that you're going to use AI. You settle on the product or products that you're going to use and ideally before. But if the horse has left the stable after, you're going to map this particular AI product to this NIST framework that we're talking about, you're going to evaluate it. And to me, I always tell clients there's a dual purpose. First, if you do this, if you follow the NIST framework, you know that you're going to hit all these targets. You're most likely to have a reliable, safe, secure, transparent, fair system. But also, if you do this the right way, as we're... as you're outlining and something goes wrong, then when you have to talk to the board or you have to talk to a regulator, or when you have to answer a lawsuit, you're in a position to say, in effect, yes, this thing happened and we're not happy that it occurred. But here's what we did to try to mitigate the risk. And that's going to put your clients and mine in a much stronger position to defend themselves when the inevitable incident happens.

[Justin]: And you know what, Kevin, you bring up a great point, because if you look at how the EU AI Act is structured, basically what they want you to do is to be able to show your work.

[Kevin]: Right.

[Justin]: To your point, Kevin, show me your framework, show me the types of inquiries that you did and things that you asked. How did you document the, you know, the origin of their data? How did you document how they claimed that their AI worked because to your point, with the inevitable bad happens and the regulator comes in, you can show them your work. We did all of this and still something happened. Well, if I'm a regulator, I'm going to say, okay, this bad happened. But, you know, all these people really made the effort as opposed to some other company that says nothing.

[Kevin]: Right? We trusted the vendor.

[Justin]: Or we didn't have a process in place. And I think that's going to be a pretty tough sell because I think, Kevin, I think the one regulator now who already has the law to do what they need to do is going to be the FTC,

[Kevin]: FTC

[Justin]: Section 5 with their own deceptive trade practices, squarely fits within the broad expanse. And the FTC, as you know, has been having hearings. So it'll be interesting to see how that develops, because they don't need legislation to enforce what they already have on the books. But if I got brought in front of the FTC and I was able to say, look, here's the framework we used, it was this. We went through all of these things. This is the... this is the new, you know, the tailored version that we developed. They may not like the outcome, but it's hard to argue that you just did it without having any thought around it because you went through that whole analysis. I mean, I think, Kevin, that's why the FCC cyber rules are based off of the NIST framework from what we're seeing and that's why I think by analogy, I'm telling people there's certain NIST frameworks out there that help you get at, well, what's a material? What's material when it comes to a cyber breach? Right. I think it's hard to go wrong with the federal government to say we were using NIST as a standard because it's right from the Department of Commerce. And it's highly regarded.

[Kevin]: Yes. And the regulators are looking to NIST as well. And we can see that when you look at the regulations of the various state and federal regulators, there's a lot of overlap. And that's because in many ways they're all funneling back to a single source. So I think that's right. I want to have you back to talk about the FCC, the rules. But I'm going to let you go now because the next time I call, I want don't you be thinking, oh, there's that Kevin again, he kept me on for so long and I just can't do it. But I... in all seriousness, I think I love your line "show your work." I'm going to do some micro content on that phrase. I think that that contains the essence of what we ask all of our clients to do. Plan ahead, map it to a framework, be able to explain even when you decided not to undertake a certain safeguard. Be able to explain why, even if it's for financial reasons. You know, we had an option. We had five issues on the table. We had went with three of them. We tabled two of them. Why? Well, we just felt like we need to wait a little longer to make that financial commitment. You're in a much better stead with the regulators than if you can't answer the first question, which is how did you go about trying to make this safe and reliable for your employees and your customers?

[Justin]: I agree with that.

[Kevin]: Yeah. Well, we will leave it there. Justin, thank you so much for joining us. I encourage everyone watching and listening to check out "She Said Privacy/He Said Security." It is an awesome and by the way, award-winning podcast, nice 30-minute bites with industry leaders and game changers out there. Check that out and as well, check out this best-selling book, "Data Reimagined: Building Trust One Byte...." See what they did there "One Byte at a Time." Justin, thank you so much.

[Justin]: Thank you.

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

[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.

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.

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.*

Thanks for listening.