Digital Planning Podcast (Season 4, Episode 5): NFT Scams

Speakers: Justin Brown, Ross Bruch, and Jennifer Zegel

Jen Zegel:

Welcome back to the Digital Planning Podcast. I'm your host, Jen, and I'm with my co-hosts Ross and Justin.

At the end of last year, we released an episode about NFTs and estate planning considerations. And today, we're going to continue that discussion, focusing on some of the most common scams in fraudulent activity used in connection with NFTs, and what attorneys need to know to alert and guide their clients who have or are contemplating creating, investing, or buying NFTs. Many issues with NFTs can stem from poorly structured terms or service agreements, but that's just the beginning. Given the relative infancy of this technology and the current lack of regulation surrounding it, some nefarious actors have emerged with scams impacting the sale, transfer, and ownership of NFTs. Recently, Ross wrote a great article for the ABA's Technology and Probate magazine titled NFT Scams Buyer Beware, which highlights a lot of the common scams in pitfalls.

Justin Brown:

Before we get into Ross's article, let's get everybody up to speed on what an NFT is. Jen, can you tell our listeners what exactly is an NFT?

Jen Zegel:

An NFT stands for non-fungible token, which is essentially a digital token embedded with a smart contract. NFTs can be digital art. Pictures, videos, a contract, a document, a tweet, a collector card for sports figures, to garbage pale kids. And more recently, are being used for concert tickets and for companies using them for promotional materials. Non-fungible means that there is only one of a kind. And so, the idea behind non-fungible tokens is that you're having something that's in a digital form that's one of a kind.

Justin Brown:

I'm going to ask the question that we frequently ask on the Digital Planning Podcast with regard to some of the new technologies that we're seeing. And that question is why would somebody want an NFT?

Ross Bruch:

Justin, I still don't know the answer to that question. There are certain examples where an NFT can be useful, an in-game purchase, like Jen mentioned, ticket sales, where it's more of a smart contract than it is a collectible. But we get to ask this question all the time of, why would you want an NFT? And sometimes my best response is, well, why would you want that original piece of artwork hanging on your walls? Why does it matter that you have the original Picasso and not a copy of the Picasso hanging on your walls? And the answer often goes back to economics of scarcity and the value in a particular object. And those lines get blurred a little bit more with NFTs because they're in the digital format. And digital assets are so easy to copy and look very, very similar, if not nearly identical to the original format. So that was a long winded way of saying, I still don't get it as much as I want to try. Jen, Justin, what are your thoughts around the NFT world?

Jen Zegel:

So I do want to stress that it's important to understand that the NFT is not, in many cases, the actual art or collectible or digital asset. It is only a smart contract and it is pointing to the location of the digital asset on the internet, which can be on a blockchain or may not be on a blockchain, and the smart contract itself can be programmed to collect royalties upon future sales. And so I think in the artistic community, having the ability for an artist to create an NFT that is based off of an original

physical piece of art or a digital piece of art that they have created, and to have control over future transfers and to receive royalties even in secondary sales, can be an attractive feature of the NFT and also providing different levels of income streams for the future.

Justin Brown:

So it's a right to access the original piece of art, or digital asset, or whatever it is. And I guess what you guys said is true. There is some exclusivity and value to being the only one who can access it or being one of a few people who can access specific pieces of digital assets.

Jen Zegel:

Exactly. And to add onto that, this is where the terms of service agreements really come into play, that you may or may not be getting some copyright or other intellectual property right in the underlying art. So that's where it's really important to look at terms of service agreements to see what exactly is being purchased and if there are provisions that would invalidate, or terminate, or no longer allow for copyrights to be given, if they're even ever granted, based on certain activities that could or could not happen with the use of the NFT.

Ross Bruch:

I think we're in agreement that the underlying smart contract feature of that is useful. It has numerous applications. But going back to the digital artwork, in the case of an NFT, I get asked, "Well, why would would you pay hundreds of thousands of dollars for a digital image? You can't display in your home the way you can, for example, a piece of actual physical artwork." And the answer is, well, there's other methods to display or to demonstrate that you own an NFT, and to show it to others. In September we did an episode on the Metaverse, and I think the Metaverse could be applicable to this type of ownership. But again, the line, to me, gets blurred when we're talking about a digital representation of something.

Jen Zegel:

In the world of rewards programs and customer loyalty points, I think NFTs could be and are beginning to be a little bit of a game changer there. Recently, in the news, Starbucks just announced that they are going to be onboarding a new standalone rewards program using NFTs and Web3 to really help increase their customer usage of rewards programs and also expand the types of rewards offered. So it'll be exciting to see what they do as this new rewards program expands and what other companies will do as a result.

Ross Bruch:

All right. So let me push on that a little bit. Can you convince me that a blockchain-based rewards system is any better than just giving my phone number or using an app on my phone other than it's new and novel and unique? To me, that sounds exactly the same thing. We're just applying the blockchain to it.

Jen Zegel:

So I think specifically with Starbucks's program, they're also going to have some type of ability to trade or sell what they're calling journey stamps, which will be part of this NFT rewards program, and then can be redeemed for real rewards. So I think the ability... In their current system, I don't believe you can sell loyalty reward points at Starbucks to other people. So having this feature, I think adds some additional benefits and opportunities for users of the system.

Ross Bruch:

The Starbucks reward black market, what a world we live in. So with my skepticism in mind, for a year or two, we've heard a lot about NFTs and the possibilities, and I think those on the more skeptical side have also had their antenna up about, okay, what can go wrong? And that's where we're going to talk about a little bit today of examples of how individuals with greater knowledge than the people they're selling to are trying to take advantage of other people with less information, with less data

and knowledge. And people are also, and this is my personal opinion, that they're trying to take advantage of some of this fear of missing out mentality, that for a year, we heard about how interesting and great NFTs are. And regardless of the outcome of that equation, there's still some lingering feeling of, "Hey, this could be the next big thing and values only seem to go up."

And for a period of time, they certainly did. From when they first gained momentum in popular culture and in mainstream media, the value of NFTs, the stories that were being reported were of the increase and remarkable sums that some NFTs were being sold for. So of course, some investors who see a world where prices only go up, think it's a no brainer to go invest in an NFT, regardless of whether you think it's a collectible item, regardless of whether you find value in that particular object or digital asset, and just see it as this is easy money. So when that occurs, it's very easy for other people, for scammers, for grifters to come in and manipulate the system.

And so, let's talk about a few of those examples and then we're going to talk about how to advise clients to protect themselves, protect yourselves from examples of NFT scans. This isn't an exhaustive list, but let's go down and name a few.

The first one I want to talk about is called a rug pull scam. And an example of a rug pull scam would be, I want to create a new coin, a new NFT, let's call them Ross coins and I am going to announce on the web that Ross coins are what you want to own. There's collectible shots of me and there's going to be 100 released, and boy, do you want to invest in this. I need initial investors. And I'll guarantee you, for the first 50 of you, you are going to get a Ross coin at a discount price. And I collect your money and I say I'm building it. And then all of a sudden, I shut down either the coin itself or the market. And that was always my intention. Sometimes projects fail and that's not necessarily a scam, but when my intention was to pull your money, I was never actually building something out there, but I took your money and then shut it down, that's a rug pull scam.

Justin Brown:

So how do you avoid this? How do we protect ourselves and how do we protect our clients from somebody pulling the rug out from under us?

Ross Bruch:

In the purest sense of a rug pool scam, which you're most worried about, is somebody who has either a history of doing this or has no track record whatsoever of creating something new and asking for investors before you're able to get any meaningful value out of what you've just paid for. So the world, first of all, of NFTs is very new. So it sounds a little ridiculous to say this, but find somebody who has a history of building successful projects in the NFT world, finding somebody who has a history and a is a known individual or entity of creating successful marketplaces that you can trust. Again, if NFTs in the pop culture have only been around for a few years, no one's going to reach that level for me or for advising other people to invest in that, but some might be more comfortable with seeing somebody who has even just a short track record of success here.

Jen Zegel:

Exactly. I think doing due diligence on who the seller of the NFTs are, trying to find out as much about the project, and whether there are other investors or other third parties that you can do further due diligence in investigation on to help determine whether the project is bonafide or if there are risks that should be accounted for in determining whether or not to continue the purchase.

Justin Brown:

Ross, what are pump and dump scams?

Ross Bruch:

Similar to rug pull scams, it involves somebody promoting an idea and then not following through on what they had said or just completely manipulating the market intentionally. So pump and dump scams have existed in the stock market for decades, if not centuries. And there's no difference between that and what's going on. In the digital world, it's just a new market. And again, going back to that idea that you have some people who have more information than others and are taking advantage of perceived greed or fear of more missing out or misperceptions about the marketplace itself. So a pump and dump scam

commonly might involve an individual who's a well-known commodity, who is a well-known promoter of different crypto or NFTs or other digital assets, and is able to influence other investors and tell them, "This particular asset, this particular investment is worthwhile making. It's going to go up in value. You can trust me. You should follow through and make an investment in this."

And while those statements are being made and while the value of that asset is increasing, at least in the eyes of the scammer, hopefully, they are selling out, they're exiting that position and only will let the general public or their followers know about their sale long after they have already exited. And when they do or when other market conditions change that they know are going to change, they are long gone from that investment, leaving other investors to hold the bag, having bought in at a high valuation and now having a far, far, far less valuable asset in their hands.

Jen Zegel:

Now, pump and dump scams aren't particular to NFTs. They can be used in a lot of other areas. The problem here is the SEC has a lot of regulations with respect to stocks and pump and dump scams that currently doesn't apply yet fully to the NFT market.

Ross Bruch:

That's absolutely right. And since the last time we talked about NFTs, the SEC has stepped in certain ways with regards to digital assets in general. I won't specifically say NFTs, but they're trying to apply existing laws and previous laws to the current digital asset world. This summer, we saw individuals charged with insider trading at one of the major exchanges. And that's an example of there's not new regulation that applies to crypto or to digital assets or to NFTs, but the agencies who are looking into this are trying to use what they have available to them for the time being. I think that regulation is, one, a good thing overall for the market in the long run. And two, somewhere in our future, but whether that's next year or the next five years or the next 10 years, who knows. So, in the meantime, they're doing what they can with what they have.

Jen Zegel:

What's another common type of NFT scam, Ross?

Ross Bruch:

The next one I want to cover is called a bidding scam. And this is pure manipulation of how payment is made and what is exchanged for an asset with regards to a contract, with regards to a sale. And a bidding scam is really as simple as, Jen, let's say that you create an auction for a certain NFT that you have created or that you just own and you have invested it and now you want to sell it. And I am the winning bidder and I said I was going to pay 10 Bitcoin, whatever the price is of that 10 Bitcoin at completion, that's my bid, and I'm the winner, and you've selected me. And then, just before I actually make payment, I switch from Bitcoin to some other type of cryptocurrency. And if you're not vigilant and if you're not watching what's going on, and if the parameters of the exact sale are done loosely and you're just not being a vigilant seller... Maybe you didn't notice. Maybe you didn't notice that you got 10 Dogecoins instead of 10 Bitcoins, and there's just a tremendous difference in the value of those two coins. And I've walked away with the NFT that I've purchased and paid far, far less.

That might be an extreme example because I think that most individuals who are selling at auction or... And any other means, even if it's just a third party contract, are going to hopefully be watching exactly what they're getting in exchange for what they're giving. But in a world where these happen fast, and in a world where after I've received my NFT, if we're doing this with some level of anonymity, you won't be able to find me if you then realize, by the way, you didn't pay the right amount. You scammed me because you paid with a different type of coin. It's the equivalent of buying something in a store and pretending like I gave you a $50 bill when I really only gave you a five. Well, hopefully, in that situation, you're going to be able to find me in the parking lot before I drive away and stop me and say, "This wasn't right." But in the digital world, much, much harder to do that.

Justin Brown:

And I think one of the problems is there's no third party overseeing the transaction who can stop the transaction. There's nobody who's holding things in an escrow, for example. When the digital payment is exchanged, the NFT is exchanged instantaneously and you run the risk that the person runs out of the store and you can't get them.

Ross Bruch:

Isn't that the whole point? Isn't that what we've heard so many people who are in favor of this digital market say, yes, but these are valuable because we don't need the middle man? The middle man is an extra cost, it's an extra layer of cost and delay and we don't want that. We want a world where we can transact with one another and trust one another based on the blockchain technology that we're going to use for this contract. Well, until that's refined, until we have a system where I can sell you that NFT and the system knows only to release it once it receives 10 actual Bitcoin... And I'm sure that technology exists. And so, hopefully in time this type of bidding skim goes away. But until it does, it's evidence of why that middleman exists in the first place because you cannot always trust the person on the other end of that transaction. And you sometimes need that, unless you have the technology really verifying for itself that you are protected.

Justin Brown:

So how do you avoid that? If you're engaging in this type of transaction with somebody, what steps can you take to avoid putting yourself in the position where somebody pays with a alternate currency?

Ross Bruch:

Well, what would you do if you were advising a client who's selling a piece of property? Let's go back to law school and call it white acre. Selling white acre from A to B, and you were advising B on the purchase of it or A on the sale of it. You would read that contract. You would go through with a fine tooth comb. You would make sure you would read the title. You would get the title report. You would make sure everybody is abiding by the contract that they say it is. It is, quite simply, and maybe this is just too easy of an answer, but it's the due diligence on making sure what is agreed upon is actually what's happening.

Justin Brown:

I think a difference, though, with whiteacre is that you have potentially a title company or an attorney who can hold a deed or who can hold funds in escrow until both sides have fulfilled their promises and the transaction can go through. So you can do all of your due diligence in a real estate transaction, but you still have the protections of that independent third party who's monitoring everything to make sure it works. I can do my due diligence on a cryptocurrency transaction or an NFT transaction and I can look up the person who's doing it and if I can even find information if at all on the person on the other side. But there's still an element of trust that has to go into it that the person is going to pay with what they say they're going to pay with after you have given up your NFT.

Ross Bruch:

I think that's absolutely right. I think that it's just an element of be skeptical of every transaction. And I realize I'm starting to sound very, very negative on a lot of these transactions by saying I just don't get it. And really you have to be careful cause you can't trust anybody and you can't even sometimes trust the technology, but we're just not there yet. I see where it's headed, but there's incidents like this that get in the way of what is intended to be a middlemanless contract situation.

Jen Zegel:

I think one way, in this particular type of scam, to help ensure that you're not a victim of it is to check, check, recheck before any crypto is actually transferred because the way this works is they're changing the type of crypto right before the commencement of the transaction. And if somebody's watching closely, they're going to catch that. And it's when people are doing things too quickly or are having too much trust and aren't taking that extra time and extra step to make sure they're paying in the correct cryptocurrency that was in the original agreement and that it's not switched at the last minute.

Ross Bruch:

Yeah, I'd absolutely agree with that.

Jen Zegel:

So moving on. I think one of the other big issues with scams and fraudulent activity is just with plagiarism. Do you have any thoughts on that, Ross?

Ross Bruch:

Going back to where we started the conversation on, well, can't you just copy that digital image? And you have the equivalent of, if I have an NFT and an associated ownership of a digital image, the original piece, but I put it up on the web so that anybody can see it so I can display it and say, "Look what I own," and then each of you download a copy of that, well, that's not plagiarism, but that's still giving you the equivalent of what I've bought and what I see value in. But plagiarism is a little bit different in that it's actually going out to the marketplace, taking your copy of what I've displayed, or maybe I haven't displayed it, but you found a way to get a similar replica of it, or maybe you've created a replica of it and going out on the marketplace and saying, "This isn't original. This is as valuable as what Ross has. Go ahead and buy it."

And the answer to this is a combination of a few different scams that we've heard before. It's due diligence. Luckily, the benefit of part of digital assets is that you can see the code. Now, I don't know how to read the code, but perceivably, somebody who can do the due diligence on the blockchain, who can see who created it, when it was created, the transactions that have occurred with regards to this token, and can verify if the story that you are buying into aligns with what you're seeing in the actual coding and the actual blockchain information.

Now, that's a little bit different and perhaps easier than fighting some forms of plagiarism in the real world because if you show up on my doorstep with what looks to be a Picasso, yes, there is a way to do an analysis of, does that seem to line up with what we know about what a real Picasso would look like and can we make an educated guess? But not a lot of people are doing that type of due diligence on everything that they're buying. And so, there's an opportunity for scammers to take advantage of the marketplace, the recurring theme here, and sell to people what looks to be an original thing, perhaps at a discount, and maybe you do a little bit less investigation when you think you're getting such a steal of an asset. And you walk away with something that is basically just a copy, and the scammer walks away with your funds.

Justin Brown:

So speaking of inflating potentially the value of NFTs, are there any strategies that scammers have used where they work together to try to artificially inflate the value of NFTs?

Ross Bruch:

What a great pivot, Justin. Artificial inflation scams, let's give an example of what that would look like. Let's say that Jen and I are in cahoots, you don't get to use that word that often so we'll go, in cahoots with one another and we are going to scam the public and make some money off of whether it's a plagiarized NFT or something that we just created that perceivably has no real value. But, I'm going to create a market and I'm going to sell it to Jen and she's going to pay some outrageous price. As proof to the world who doesn't know that we're working together, that somebody out there is willing to pay this price for this asset, therefore, it must be worth that, or something near that.

And then she goes to Justin and she says, "Justin, and I got this great NFT. I need to sell it. I'll give it to you at a discount. I paid $8,000 for it. I'll sell it to you for seven." Or she goes the other way and says, "I paid $8,000 for it a year ago and it's appreciated in value and I want you to pay 8,100." And then Jen and I just split that 8,100. We've created something out of thin air, both benefited from it. Justin walks away thinking he has something of value. When he tries to resell that on the market, unless he's able to do the same thing that was done to him, he may find a lack of viable buyers, and therefore, his asset will be worth a lot less or possibly nothing on the open market. So that's how an artificial inflation scam works.

Jen Zegel:

Yes. And we will have successfully bamboozled him.

Ross Bruch:

Wow. This is quite some vocabulary in this episode. And then there's one more that I want to touch upon, which is an airdrops scam. And this one is really fascinating to me because, again, it's taking advantage of individuals, fear of missing out of potential greed. Well, greed's probably a bad word, but upside potential and thinking about the long-term investment and that NFTs are going to increase in value. And it's as simple as the scammer placing something into your wallet. So we talked about wallets on previous episodes, but you're going to hold your NFTs, you're going to hold your tokens in an online, a hot wallet or in some external drive, a cold wallet. Regardless of how you hold it, I'm going to, as the scammer, place an item into your wallet.

And I recently learned that you don't even need to accept that. If a scammer knows the location, the address of your wallet, especially if it's... I do believe in this case it needs to be connected to the internet in some way. But if I know the address of your online hot wallet, I can place a token inside of it. You don't have to approve that. You don't have to acknowledge receipt of it. I'm just going to put it there. Alternatively, and we'll talk about what happens that's going to be a little nefarious after that. But alternatively, I can use this as a giveaway opportunity. I'm going to post it to my website. The first 100 people to email me are going to get a free Ross coin and I'll send it to you and you can put it wherever you want, whether it's your hot wallet or cold wallet.

Now, when you do that, that item, that token living in your wallet might have a click here or it might have a link that I'm going to ask you to acknowledge receipt. I'm going to ask you to do some additional step. When you do that, it's going to give me access to your wallet and I'm going to be able to enter your wallet and remove any assets that are in there. Where it gets really nefarious is that it doesn't necessarily have to be a link that's obvious. We all know not to click on links of random emails that we get. Do we know that for NFTs that were given away for free? Maybe, maybe not. But even if you try to... I can embed that link. I can embed that, my secret way into your wallet just by anything you do to this token, including trying to delete it.

When you say, "You know what? I don't know what this is. I just want this out of here. I'm going to hit delete and I'm going to remove it," that action could be the key for me to getting into your wallet. So the first bit of advice here is do not accept free tokens. Maybe I give the caveat, unless you absolutely trust the source, unless you know where they're coming from, but even then, I'd be a little bit leery.

But secondly, regardless if you get a free token and you about this, or two, one was just airdropped into your wallets and suddenly appears, don't touch it. Don't touch it for all of time. That is a permanent part of your wallet. Let that sit there because doing anything, manipulating anything to that may give access. Maybe if that's the only thing in your wallet, then you can try to remove it. But I don't necessarily think I would trust the wallet after doing that ever again. So just let it sit there and don't touch it.

Justin Brown:

I mean, this sounds like a digital pick pocket, so to speak, or planning something in that can pick your pocket digitally. But other than not accepting it or not clicking on it or not trying to delete it or anything, are there any things that you can do to protect your wallet itself? Can you compartmentalize your wallet or can you have, I don't know, a staging wallet where before things go into your real wallet, they go into this staging area where you can clean them or see what it is?

Ross Bruch:

Well, I think one of the solutions might be to have multiple wallets so that, just like you're going to have multiple LLCs to protect an individual investment in one of them, if there's a liability in one LLC, it doesn't impact the others, the same rules might apply to a wallet. Separating them, having multiple ones so that you're not jeopardizing other items in there is a potential solution.

Justin Brown:

So from a planning perspective, that makes me nervous because now we've got more wallets that are out there. Now we have more private keys that we need to locate and keep track of. So I prefer more consolidation and less keeping everything all over the place. If you have one of these unknown tokens in your wallet, can you remove everything else from your wallet? Or is it possible that the removal of everything else could be a trigger based upon this token?

Ross Bruch:

Yeah, I think you're safe to move assets out of the wallet that you trust and relocate them to a new wallet, and thus leaving behind the assets that you find questionable or potentially corrupted, and therefore, plan around it using that. Maybe that's a way to consolidate over time your wallet. I hear you on the planning aspect of it. This is all about balance as we're trying to figure this out of how to protect versus how to have access to things, how to keep track of assets. I don't have a great answer for you yet.

Jen Zegel:

I had a friend be a victim of one of these airdrop scams, and 20,000 worth of Ethereum was pulled from her hot wallet as a result of the scam. And she's been talking with the FBI and other investigative authorities right now to no avail. But the way that scam worked on her hot wallet was there was some tracking device within the link and the drop of the cryptocurrency into her wallet. So the perpetrator, once it was clicked on, had full access to see everything that was in her wallet, every action that she took. So I think as scammers get more advanced with these types of technologies, it could be even more dangerous that they could get access to other assets that are within the wallet before they can be removed. So it can be pretty tricky to get the assets out before a scammer could potentially get them as this evolves and they're able to really overtake somebody's wallet and directly control it. So it's scary.

Ross Bruch:

If you recall, when we spoke with Joel Revill from Two Oceans Trust, he described the protocol that Anchorage Custodian uses to store digital assets and access them. And when you talked about that there was an arm that came down and accessed an individual wallet and removed it from the internet and removed its access to the internet. Maybe we have to have Joel back on to ask why, but my suspicion is it's something worth related to this type of nefarious activity that access to the online world could corrupt certain files within a wallet, and thus give access to the entire wallet. And when it's offline, maybe you have that element of protection.

Jen Zegel:

Absolutely.

Ross Bruch:

So I think that solutions to this are there, maybe they're expensive and not commonplace, but in the future, maybe we'll see protocol of that nature become more common. But again, Justin, to your point, of all the steps that we can possibly take to make this safer, also come at a cost of making them more cumbersome to initiate, or to find or to administer, or to do everything that we're thinking about as planning attorneys, trying to make things simpler for individuals.

Justin Brown:

I think that is a fundamental problem that fiduciaries run into and are going to go running into when they are serving as executors or trustees or multiple trustees of multiple trusts that are holding these digital assets. And if one of those wallets gets, I'm going to say infected, so to speak, can that potentially impact all the other wallets that a corporate fiduciary or an individual fiduciary is holding in other trusts or estates? I mean, the liability there, you can see how that can just get out of control. And explains why a lot of these maybe corporate fiduciaries don't want to get into holding cryptocurrencies or NFTs as part of their fiduciary duty and they're outsourcing it to sub-custodians so that they don't have that liability.

Ross Bruch:

Yeah. I think that's absolutely right. And as we close out, I want to circle back to two very brief ideas that we've covered so far in this show. Number one is going back to just that level of due diligence. I think that's so important. When we've talked before about when using electronic documents of electronic wills, you lose some of that ceremony in signing the document because it becomes so easy to just click my signature on a document and you lose some of the perspective that what you're signing is really, really important. Well, the same rules might apply to the digital world when buying or selling NFTs or other digital assets, that it has become so easy to do and so commonplace. And that action of just clicking through and saying, "Yes, I buy, or yes, I sell," resembles so many other activities that we do on a day-to-day basis on the internet. And that's why it's important to just slow down, slow your clients down, do that due diligence, take the extra time. If it's really that valuable and important of investment, spending extra time with it is necessary, but also, just wise in general.

The other item I want to leave with is we briefly talked about the SEC and regulations. And we've used the phrase before, and some of our guests have used the phrase before the Wild West when it comes to digital assets and planning. And I'm a little bit optimistic. Despite this episode being all about things that can go wrong, I'm optimistic about the future of digital assets because, to overuse that analogy, it feels like the sheriff is coming to town, or at least on their way, because different agencies are interested in protecting the general public. There's just so much to do. There's so much to absorb and learn about.

And even though a lot of these scams we talked about today have had their place in other marketplaces throughout time, the application of those same ideas of grift and scam now being applied to the digital world require a new set of tools and a new outlook on how to try to stop them. And as this unfolds and as new things pop up and new ways to scam people pop up, those regulators are finding new ways to try to stop it. And it's an interesting battle that will continue to go on.

Justin Brown:

Well, Ross, thank you so much for sharing all the information and the research that you've done in order to write this article. For those of you who want to see the article, it's in the November, December 2022 edition of Probate and Property from the ABA, the American Bar Association. It's a great article. You should definitely check it out. For Jen and for Ross, I want to thank everyone for listening to this episode of the Digital Planning Podcast. And we'll see you next time.