Consumer Finance Monitor (Season 8, Episode 11): The Patterns of Digital Deception

Speakers: Alan Kaplinsky and Greg Dickinson

Alan Kaplinsky:

Welcome to the award-winning Consumer Finance Monitor podcast, where we explore important new developments in the world of consumer financial services what they mean for your business, your customers, and the industry. This is a weekly show brought to you by the Consumer Financial Services Group at the Ballard Spahr Law Firm. And I'm your host, Alan Kaplinsky, the former practice group leader for 25 years and now a senior counsel of the Consumer Financial Services Group at Ballard Spahr. And I will be moderating today's program for those of you who want even more information, either about the topic that we're going to be talking about today or anything else in the world of consumer finance. Don't forget about our blog, consumerfinancemonitor.com. It goes by the same name as our podcast show. We posted our blog since 2011, when the CFPB became operational, so there's a lot of relevant industry content there. We also regularly host webinars on subjects of interests to those in the industry.

So, to subscribe to our blog or to get on the list for our webinars, please visit us at BallardSpahr.com. And if you like our podcast, please let us know about it. You can leave us a review on Apple Podcasts, YouTube, Spotify, or whatever other platform you may use to access your podcasts. Also, please let us know if you have any ideas for other topics that we should consider covering or speakers that we should consider as guests on our show. Today, I'm joined by a very special guest who has been on our podcast show before, specifically on August 3rd, 2023. And I am referring to Professor Gregory Dickinson, who is an assistant professor of law at the University in Nebraska, where he teaches contracts, business towards an unfair competition, the common law, and remedies.

He's also a fellow with Stanford Law School Program and Law, Science, and Technology. He holds a JD from Harvard Law School, and before he went into academia, Professor Dickinson practiced law privately at Ropes & Gray, a major firm based out of Boston, and he was also with two firms in Rochester, New York. So before we get into the nitty-gritty, Greg, very warm welcome to you. Terrific having you as a repeat guest on our show.

Greg Dickinson:

Yes, thank you, Alan. Such a pleasure to be back with you.

Alan Kaplinsky:

Now let me now tell our readers a little bit about the prior podcast that we did because today's podcast show really builds on the prior work that you've done and the prior podcast show that we did. We talked about so-called dark patterns, and during that show, we talked about the most common forms they could take. We considered whether and how dark patterns are used to influence consumers' online behavior and how that differs from traditional scams directed at consumers involving the use of deception. We then discussed the federal and state statutes and common law claims currently being used to challenge the use of dark patterns, as well as current legislative action to more directly target dark pattern and the challenges lawmakers face in crafting new legislation. We also assessed the effectiveness of using private lawsuits rather than government enforcement to police the use of dark pattern.

And we concluded, as I often like to do with the practical steps companies should consider taking to avoid the risk of enforcement or private actions arising from claims that dark patterns are present in their user interface designs. We decided to do that podcast show with you because of an article that you had written in Georgia Law Review, which was entitled "Privately Policing Dark Patterns". Now you've written another article, Greg, and this one, as I said, builds upon your prior work that's called "The Patterns of Digital Deception", and it's in volume 65 of the Boston College Law Review beginning at page 2457. This article, by the way, is available either on the Boston College Law Review website or on SSRN, and I strongly encourage our listeners to read the article for sure. So I have a lot of questions for you, Greg, and so let me launch into it right away.

Could you tell us a little bit about what you mean by digital deceptions and what led you to focus your attention on this particular area?

Greg Dickinson:

Yeah, so as you mentioned, I initially started by thinking about dark patterns. These tricky user interfaces or websites that pressure you. They don't necessarily grab you by the neck and make you, but they pressure you to do things that might be against your interest. And a classic example of that something like you check a box on a website, and in order to decline an offer you, have to say, "No thanks. I don't like saving money," or something silly like that, kind of some psychological pressure. That's dark patterns. But as you note, this paper builds on that. And really, by digital deception, I'm intending to bring into scope everything, everything from dark patterns that are comparatively mild right up to outright fraud where somebody tricks you into a Tinder romance and takes your money. The old-fashioned romance scam, I mean to cover everything, but what got me into it was really the surprise at how aggressive some websites were starting to be with tricking me, it felt like, out of my money.

Alan Kaplinsky:

Yeah. So tell us, Greg, some examples of the things that you have in mind. I mean, you mentioned already romance scams and things of that sort, but what would be some other examples?

Greg Dickinson:

So the more common one, actually, one of or the most common one, would be something as simple as you pay for a product, and it's never delivered. It's a company that you've maybe not worked with before or a third-party seller on a platform that you are familiar with. You send them your money, and you never get your product. You don't think of that as much as fraud because, usually, fraud involves something a little more tricky than just not giving you what you paid for. But that's fraud, too, and that's a very common example. Some trickier examples, commonly you'll see, for instance, fake sale offers on websites that will say, "Here's this offer, but it's only available for a limited time," when in fact it's available always, or fake inventory listings that will say there's only a couple of these left in stock. But really, it always says that. There is no actual live database stock number.

Things like fake product reviews are another common one where people pay people to submit positive product reviews and distort with the appearance of objectivity. And then one that I'm particularly worried about is targeted scams that might target folks that, for instance, don't speak English as a native language, and so might be more susceptible to trickery, or the paper talks about some scams that target members of the military or prospective military members as well. And so you can actually get pretty targeted with these things, too.

Alan Kaplinsky:

Right. Right. So, how is modern online deception any different than old-fashioned in-person fraud?

Greg Dickinson:

Yeah, this is a question that I had a lot of fun wrestling with in the paper because, in some ways, there's nothing really different at all. Humans have been tricking each other and taking their stuff for about as long as there have been humans. You think about the Trojan horse story or the guy in the early 20th century who sold the Brooklyn Bridge; I think three or four times he sold the Brooklyn Bridge. And so that's not new. Humans have always been doing that. And from that, I reason in the paper that we may not need any new substantive law. The law has had quite a long time to develop to deal with trickery, but to get back to your question, what's really different is that you can have a combination of scams that are targeted and also quite cheap to run.

It's always been the case you could run cheap scams, send out a bunch of flyers for a deal that doesn't exist, or that you could have targeted sophisticated scams like the Brooklyn Bridge, but those take a lot of work. If you're going to find somebody gullible enough and interested in buying a bridge, you've got to do some groundwork to figure that out. But what modern

fraud or modern online fraud allows is fairly targeted scams that are also cheap to run because they're done by algorithm rather than an actual person watching the public and looking for just the right guy. And so it's that combination of targeted and inexpensive that really makes the difference with online fraud.

Alan Kaplinsky:

Right, right. So what have lawmakers been doing to address this issue, and have they succeeded, and what sort of restrictions do you see on the horizon?

Greg Dickinson:

Well, fortunately, not much yet. And I say fortunately not because I don't believe fraud's a problem, but because the solutions have been scary. And so I'm worried more than hopeful about what has been proposed so far. But what has come along are proposals that look a lot like lawmakers often make. It says there's a bad thing here, let's get it, partly because it's new and partly because, well, the public that I'm relying on for votes is concerned about this, and so I better do something. And so you get laws, for instance, targeting technology that drives these scams. And so a couple examples of that. There's the DETOUR Act that has been proposed maybe in the last three congresses, and that does a whole lot of things, many of them bad, but a couple of the things it does is bar or prohibit behavioral testing, which sounds scarier than it is.

I'll get to what that is and also bars, what it calls addictive designs. And both of those sound bad. Nobody wants to be subject to some sort of experiment or subject to addictive designs. But when you think about what that means, addictive designs could be just about anything. It could be Candy Crush, the app that's really fun to play. It could be an addictive design or maybe even Duolingo, which I use every morning as I'm trying to learn Arabic. And so that could be addictive. And behavioral testing is a really important tool for software companies as they try to develop user interfaces that people can use intuitively that are actually easy to use.

They'll track how long it takes you to find what you're looking for under one version of the interface versus another. And so this sort of thing can be dangerous to target the technology because it's multi-purpose. Another one I mentioned is the No Section 230 for Generative AI Act targeting Generative AI, broadly removing some traditional protections for that sort of technology, partly out of fear of fraud, things like deepfake videos, and whatnot that might support a product. And so those are the sorts of proposals that have been highest profile. And as I mentioned, I'm kind of worried about them.

Alan Kaplinsky:

So I could put it in crude terms. Unfortunately, legislators tend to use a meat cleaver rather than a scalpel. They tend to, in their zeal to get rid of the fraud, they use what you would call in your article a technological approach, they end up throwing out the baby with the bathwater to put it in another way.

Greg Dickinson:

Yeah, that's the real danger. And so I can sympathize. I've never been a part of a legislature, but if I have people telling me this is a big problem, an obvious or apparent solution, at least, is to say, "Well, you aren't allowed to use those tools if you're going to misuse them like that," without realizing all of the good stuff that those tools do that we'd also lose if we restrict it.

Alan Kaplinsky:

Right. Right. Right. So, you mentioned in your paper the challenges to lawmaking in the area. Could you talk a bit more about that?

Greg Dickinson:

Yeah, so as I mentioned, one problem is that these are general-purpose technologies. You think about what's driving scams under the hood; it's not anything weird. It's large databases full of information about consumers. It's cookies and other tracking technologies that help entities follow people around the internet so they can collect data about them. It's things like machine learning algorithms, basically statistics tools to analyze that data, and well, that's the same stuff that powers everything

else that we like. That's the same stuff that makes Amazon have such great product recommendations for me. I bought three books today, and often, it's books I've never heard of except that Amazon found them and told me about them. That's what I buy. But you can find anything on there, and every app you use it remembers where you've been. It can offer suggestions, and the sort of things that we love about our electronic products, apps, and services is all possible because of the very same tools that power deceptive ads.

I guess what that means is we should be worried about bright-line rules that bar technologies. And then another point that I make in the paper is usually if you're going to make the sacrifice to just use the meat cleaver, as you said, and really outlaw a particular technology, you're hoping to get the benefit of, well, at least everybody will know what the law is. It'll be super clear: don't use this stuff. But another point that I make in the paper is in this area, you still have the common law of fraud. You still have state unfair and deceptive acts and practices statutes. And so even if you were to have a federal law that says, "Don't use these tools, you're still not going to know which tools you can use because there's always the possibility of a common law fraud action or an FTC unfair and deceptive acts and practices investigation." And so you're not going to get any certainty despite the fact that you sacrifice a lot of flexibility with the bright-line rule.

Alan Kaplinsky:

Yeah. Now, I take it you mentioned the Federal Trade Commission. They've done a lot of work in the area of dark patterns, and I assume they've done a lot of enforcement work in the broader area of eliminating digital deceptions. I assume that they use principally their tool is Section Five of the Federal Trade Commission Act, that proscribes unfair and deceptive acts and practices. Am I right?

Greg Dickinson:

Yes. So that that's right. That's the FTC's traditional tool, and that's the tool I would encourage them to use. I think that's the better approach here. They have contemplated passing some regulations, not just guidance documents, but actual notice and comment regulations in this space. I think that would be unwise for the reasons I've mentioned, but I just wanted to get that out there. There has been talk of it, but primarily enforcement actions for unfair, deceptive practices.

Alan Kaplinsky:

You don't mention in your article, at least if, you mentioned it, I missed it, which is possible. I don't generally get too involved with the footnotes, and there are a lot of footnotes. So, CFPB, you would talk a lot about the work of the FTC in the area, but I don't think anything about the Consumer Financial Protection Bureau. Now, things have very recently changed with the change in administrations, but under the Biden administration, that was a very, very active, some would say overreactive consumer protection agency, have they not really done much work in that area, in the area of digital deception and dark patterns?

Greg Dickinson:

Because of their more limited jurisdiction, I didn't collect numbers on their enforcement actions, but looking over their guidance documents and their reports and things, they seem to be operating roughly in parallel with the FTC, meaning they're primarily pursuing things through enforcement actions and guidance documents. And may also, I don't recall for sure, be considering regulation, but same basic trend where they're seeing the rise in online scams just like the FTC is.

Alan Kaplinsky:

Right. So, in your article, as I said, you mentioned you talk a lot about the FTC, and they have done, I know, a lot of work in the area. We've done a couple of podcast shows with Malini Mithal, who is a senior lawyer at the Federal Trade Commission, and a lot of the cases that she talks about involve digital deception or dark patterns, but you also talk about private litigation and how that could play a more important role. And then, you talk about some of the drawbacks of private litigation, but let's start with the private litigation itself. You think that could be... Private litigation could play a more prominent role.

Greg Dickinson:

I think it could. And so you and I had the chance to talk about this a bit before, but just to remind everybody, I think there's a role for private litigation here because you think about who has the most information about a scam, who has the most incentive, the guy who got tricked, he could bring a claim. And that's, in fact, until the early 20th century, that's exactly how it worked. If you got defrauded, maybe there would be some criminal charges, but probably the only way you were going to address it was through a fraud action. Not through any sort of governmental enforcement effort. And as I mentioned, that has some advantages. You have lots and lots of enforcers. So basically, everybody who could get scammed is an enforcer.

And in a certain sense, in a limited sense, you also have essentially unlimited enforcement resources that you have the entire private sector that could fund these things, but you have problems. There are limitations. You aren't going to bring a lawsuit over a hundred dollars or even a thousand dollars, probably that you get scammed out of. And so, there are limited contexts where the incentives align, even though private enforcement can be a very powerful tool. And so in the paper I wrote called "Privately Policing Dark Patterns", I suggested that maybe statutory damages being available would help with something like this or maybe punitive damages or treble damages, all sorts of different ways that you could incentivize it.

Alan Kaplinsky:

And how about attorney fee shifting language, language that says that the consumer prevails his or her attorney's fees can also be recovered from the dependent?

Greg Dickinson:

Yes, this could do it too. You see this with the ADA, and you do have to be careful because you can accidentally get a lot more enforcement than you meant to. And so if you're passing an aspirational law that you don't really want enforced, well, that's not something that you want to give attorneys' fees or treble damages for, but if you really mean it, if you really want this stuff to go away, that can certainly get it done. But it's not as if I'm the king, and so I don't get to make the law. And so, for now, the law is the way it is, and there are not typically attorney fee shifting or treble damages provisions. Some states have that, but most don't. And so, this paper tries to think about what the FTC could do, how the FTC might be able to prioritize its enforcement decisions given the limited scope, powerful but limited scope of private enforcement.

Alan Kaplinsky:

Yeah. And in your article, well, in terms of private enforcement, it identifies certain kinds of cases that are suitable for private enforcement. You talk about fly-by-nighters, a lot of companies like that, you don't even know where they're located. Very, very difficult for a private litigant to even serve papers on that kind of a company. And in most cases, they're gone or operating under a different name by the time you think you've caught them. So why don't you tell us about, you mentioned a few things. I remember arbitration; it's another thing you've mentioned that's not particularly suited for private litigation if there is an arbitration provision and they are included in online agreements with consumers. So tell us a little bit about that and then how you see public enforcement as an overlay in terms of prioritizing what the government ought to be going after or who they should be going after.

Greg Dickinson:

Sure. So I gave them silly names just so they'd be more memorable, but you got the basic point here. You even remembered the names. So the fly-by-nighters, if you have somebody operating out of jurisdiction, it may be if it's enough money, there are ways to make the lawsuit happen, but it's not generally going to be worth it. Nickel and dimers was another one I mentioned. This is somebody, an entity who's taking small sums of money, maybe from a large group of people, so maybe it's economically significant, but if you lose a hundred dollars, you're not going to run out and file a lawsuit about that. You'll just say, "Well, I'm not going to work with that guy again because he took my money." Other ones, as you mentioned, arbitrators. And the arbitration itself isn't what has the effect so much as, generally, when you have an arbitration provision, you're also waiving the right to aggregate resolution of the dispute.

And so if you have waived your right to aggregate litigation or resolution, you can't turn those hundred-dollar claims into a hundred-thousand-dollar claim by combining them with a bunch of other folks who had the same thing happen, and so that's another problem area.

Alan Kaplinsky:

Pause on that for a second. Assuming that there wasn't an arbitration provision, and so there was no class action waiver, would these be easy kinds of cases to bring as a class action? Would they satisfy all the requirements of Federal Rule 23 or state law analogs to Rule 23?

Greg Dickinson:

So some of them could be you have a bunch of people tricked out of a small amount of money, but the problem is the FTC doesn't give you a private cause of action. And so your cause of action is probably going to be, you could use common law fraud that's pretty stringent or the state Unfair and Deceptive Act and Practices analogs. The problem with those is even though there is a Uniform Deceptive Trade Practices Act, it's not been adopted uniformly. It's been adopted by 50 states in about 50 different ways. And so you could have problems getting a class certified. The other problem that I mentioned in the paper is sometimes this stuff changes really quickly.

We were talking earlier about customized scams. If they're customized right down to the user level or nearly so, and if it's a fly-by-night company, for instance, that moves quickly or changes things quickly to come up with new scams, you might have trouble getting class certification because people have been harmed in different ways. And so you have this risk, both of the law being different in important ways between jurisdictions because it's a state statute, and maybe not everybody saw the same tricky interface. Maybe they saw slightly different ones that would create fact questions that would be a problem. So yes, it could be a perfect case, but you can also run into some problems.

Alan Kaplinsky:

Okay. So you talked about the fly-by-nighters, the nickel and dimers, those that are subject to arbitration. I think there was a fourth thing you mentioned, too. Am I right?

Greg Dickinson:

The interface shape-shifters kind of a Star Wars-inspired thing.

Alan Kaplinsky:

Right. Got it, got it, got it. So what you suggest is that those are the kinds of companies that the FTC ought to be focusing on since they're the hardest for private litigants to go after. Have I got that right?

Greg Dickinson:

So that's exactly right. Given that I don't foresee, at least in the near future, things like attorney's fees or treble damages becoming the law in this area, one thing we can do kind of a second best thing we could do is at least target federal and state governmental enforcement resources at those areas where private folks are least able to protect themselves. And so the FTC going after companies in China that are running repeated scams is more effective than me certainly, I don't want to do that, I can't do that. And they even have certain advantages. They have arrangements with foreign law enforcement agencies. They, of course also, they aren't worried about turning a profit. They're funded by the government, and so they're not looking to make money like a plaintiff's class action lawyer or something, and also, they didn't sign any contracts. And so the FTC isn't bound by your arbitration provision. They can investigate whatever they want and, so there are real advantages to having the FTC look into these specific types of cases and maybe leave off to let consumers protect themselves in big cases where that's actually possible.

Alan Kaplinsky:

Right. I wanted to get your reaction to one other thing, and that is that your area of focus is on an area that I think there would be wide bipartisan support for. So, the Federal Trade Commission, you've got a commission of five individuals. Right now, I don't think every position has been filled, but it's essentially supposed to end up with three Republicans and two Democrats. And there's been a lot of issues raised with the CFPB's work in this area because the focus of their work has not been just on scams and deception. It's dealt with areas where people have felt that they'd been pushing the envelope and have broadened their own jurisdiction. But I think when it comes to your area, I don't think there's any difference between a Republican and the Democrat. I don't think anybody likes to be scammed. Am I right? I mean, I don't think that enforcement ought to slow down at all to any perceptible extent under the new FTC created by President Trump.

Greg Dickinson:

So I think that's right. You'll see a reduction, I think, in interest in regulations because of the possibility of inadvertently impeding innovation. But I don't think you'll see any less interest in enforcing the sorts of scams or in enforcement actions against sort of scams that I'm talking about. And so I think that's exactly right. It seems sensible enough, and as I think about why isn't this happening, and I don't mean to claim it's not happening at all, I'm sure there is some attention paid to these sorts of things.

But you also think about the incentives at the FTC, if you're fresh there and trying to make a name for yourself, maybe you don't feel like picking the tiny little company that's tricking people out of a hundred dollars at a time in the middle of nowhere. If you want to make a name for yourself, you go after Amazon or something like that. And so there are some competing incentives against a pure, efficient use of resources at the FTC that may be part of the reason that you don't see a focus like this. Everybody likes to go get the big player, even if maybe private actors could have handled that, too.

Alan Kaplinsky:

Right. Right. So we're drawing toward the end of our program for today, but wondering if you could share with us your vision for this area of law and then I'd love to know if you're willing to disclose it, what's your next area of focus going to be? I'm sure it's going to be in this intersection between technology and the law, but I wonder if you could comment on that.

Greg Dickinson:

Yeah. So if I got to be in charge for a day, which is the fun position your question puts me in, I want some incentive for private lawsuits here, something like treble damages or something like that, because I think there really is a lot of power in the private sector here to enforce. If you want to get rid of something, the ADA and employment discrimination laws have showed us how, not that we don't have discrimination still in those areas, but boy, you can do a lot of work with plaintiff's lawyers if you're sure about what you're pointing that at. And so I think there should be some careful thought about what we want to incentivize because that's a powerful tool.

And the other thing, maybe some processes for how the FTC selects cases is worth pursuing, something along the lines of what I outline in the paper, things like companies that are hard to pursue. There does need to be some allowance, though for, of course, the FTC has to get its budget from Congress, and if you've got a bunch of targets that nobody's heard of, maybe Congress doesn't want to give you your money for next year. And so I think there does have to be some allowance for that sort of thing, but careful use of public resources and pulling the private sector in a bit, that's my particular vision.

Alan Kaplinsky:

So, are you already working on a new article, or are you taking a little time off right now?

Greg Dickinson:

Well, I'm always thinking about this stuff, and so I hesitate to claim an article because right now, I've got ideas rather than an article. But I've been thinking about maybe developing a taxonomy of the sorts of dark patterns and the sorts of online scams

that warrant investigation that maybe warrant both private lawsuits and public enforcement rather than those that resist private enforcement. The tricky tools that online folks are using that are most despicable. It'd be a fun project.

Alan Kaplinsky:

Right. Right. I take it probably, given we're in the very early stages of the use of artificial intelligence; you probably can't even imagine what kinds of scams are going to be coming down the pike because it seems like the scamsters are staying at least one step ahead of everybody else.

Greg Dickinson:

It's hard to imagine. So my fear and not a fear, the market can handle it, but you're going to get videos of celebrities endorsing who knows what, and it's going to be hard to tell the difference between the real deal and not. So that's something I definitely foresee on the horizon.

Alan Kaplinsky:

Right, right. Okay. Well, Greg, want to thank you very much for taking the time today to share with me and our listeners this very interesting follow-up law review article that you've written for Boston College Law Review. And to also let you know that we love tracking the work that you're doing in this area, and keep us in mind whenever you publish something new. So again, thank you, Greg.

Greg Dickinson:

Such a pleasure chatting with you. Really, really, truly a pleasure, and I'll definitely keep you in the loop if I have any new ideas.

Alan Kaplinsky:

Great. And to make sure that you don't miss our listeners, don't miss any of our future episodes, please subscribe to our show on your favorite podcast platform, be it Apple, YouTube, Spotify, or wherever you listen. Don't forget to check out our blog also to call Consumer Finance Monitor for daily insights of the consumer finance industry. If you have any questions or suggestions for our show, please email us at podcast@ballardspahr.com. Stay tuned each Thursday for a new episode of our show. Thank you very much for listening, and have a good day.