
THE CRYPTO EXCHANGE: CRYPTO AS “FUNDS” UNDER THE EFTA – HOW A COURT’S RECENT RULING MAY IMPACT VIRTUAL CURRENCY PLATFORM OPERATORS

HOST: ETHAN OSTROFF

GUESTS: CARLIN MCCRORY AND ADDISON MORGAN

Ethan Ostroff:

Welcome to another episode of *The Crypto Exchange*, a Troutman Pepper podcast focusing on the world of digital assets. As longtime leaders in the intersecting worlds of law, business, and government regulations, our lawyers can go beyond the buzzwords and headlines to make sense of the emerging legal and regulatory frameworks for operating in the digital asset industry.

I'm Ethan Ostroff, one of the hosts of the podcast and a partner at Troutman Pepper. Before we jump into today's episode with my colleagues, Carlin McCrory and Addison Morgan, let me remind you to subscribe to our blogs, consumerfinancialserviceslawmonitor.com and troutmanpepperfinancialservices.com. And don't forget to check out our other podcasts on troutman.com/podcast. We have episodes that focus on trends that drive the payments industry, consumer financial services writ large, the Fair Credit Reporting Act, and more. Make sure you subscribe to the latest episodes.

Today, I'm joined by my colleagues Carlin McCrory and Addison Morgan to discuss a recent case in the Southern District of New York that has been in the news, *Rider v. Uphold HQ*, and, in particular, a ruling that signals virtual currency platform operators may be subject to the Electronic Fund Transfer Act and Regulation E.

Carlin and Addison, let's jump right in. Carlin, do you want to just give us a brief overview of the Rider case and what's really at issue?

Carlin McCrory:

Yeah, sure, Ethan, and thanks for having me on today. Looking forward to the discussion. The plaintiffs in this case brought a class action against Uphold HQ Inc. Uphold is a crypto exchange that enables users to transfer, purchase, trade, hold, sell crypto on its platform.

What happened here is when Uphold users create an account, they're required to set up two-factor authentication, which we see all the time these days. However, in this case, the plaintiffs allege that Uphold failed to implement the two-factor authentication correctly, which allowed unauthorized users to designate new devices using only the customer's email address and password.

So the mess-up here is that the two-factor authentication didn't require any access to the account holder's original device. So many times, we see this when we're logging into online banking or something like that, that you get a text message to your phone. It doesn't appear that was the case here. The complaint brings one claim under EFTA and then eight state law claims, such as breach of contract, negligence, gross negligence, and then unjust enrichment, amongst some other claims.

Ethan Ostroff:

This two-factor authentication and what's going on with these allegations sound kind of far-field from EFTA and Regulation E. How does that basic fact pattern and what's at issue end up

THE CRYPTO EXCHANGE: CRYPTO AS “FUNDS” UNDER THE EFTA – HOW A COURT’S RECENT RULING MAY IMPACT VIRTUAL CURRENCY PLATFORM OPERATORS

leading us to a decision that, you know, has potentially significant ramifications for virtual currency platform operators?

Carlin McCrory:

To get into this discussion, we kind of need to go into some of the nuances with Reg E. And I'll try not to bore the audience with the background on Reg E, but the Reg states in relevant part that there are required content of disclosures. So a financial institution, which we'll get to in a bit, must provide the following disclosures, the first being the liability of the consumer, which is a summary of the consumer's liability under Reg E or under state or other applicable law or agreement for unauthorized EFTs, electronic funds transfers.

The disclosures must also state the telephone number and address of the person or office to be notified when the consumer believes that an unauthorized EFT has been or may be made on their account. These regulations apply to any EFT that authorizes a financial institution to debit or credit a consumer's account.

So we'll get into the definition of some of these terms, and EFTA contains several definitions, first being that an EFT means any transfer of funds, other than a transaction originated by check, draft, or paper instrument, that's initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to instruct a financial institution to debit or credit an account.

And this kind of goes back to your original point about the case turning on, what's the definition of funds? But let's first address that financial institution point because I do think this is a sticking point here.

Technically, under Reg E, a financial institution is not only what you'd typically think it would be, you know, a state or a national bank, credit union, et cetera, savings or loan association, but it's also any other person who directly or indirectly holds an account belonging to a consumer.

The court stated that the statutory language here is pretty clear, right? Uphold is a financial institution under this definition because it holds an account belonging to a consumer.

Ethan Ostroff:

So, in this instance, these folks who are the plaintiffs in this case are saying that Uphold created these accounts that include cryptocurrency, savings, other personal and financial information, and that these failures in their security protocols and responsiveness allowed other people to be able to re-designate a user's device without additional identity verification and then drain the accounts? Is that right?

Carlin McCrory:

Yeah, that's right. There was unauthorized access to their accounts in this situation. And that would fall under EFTA because the court determined that cryptocurrency should be considered funds under EFTA. The term funds, interestingly, is not defined within the Reg, but the court stated that... You know, when a term is undefined in a statute, a court will give the term its ordinary meaning.

So then the court went into this interesting analysis as to the definition of funds and whether cryptocurrency is funds. The court used the dictionary definition of funds to state that it is "a sum of money or other liquid assets established for a specific purpose."

And then the definition of cryptocurrency that they used is "a digital or virtual currency that is not issued by any central authority, is designed to function as a medium of exchange, and uses encryption technology to regulate the generation of units of currency to verify fund transfers and to prevent counterfeiting."

So under its ordinary meaning, the court decided that the term cryptocurrency means a digital form of money and, therefore, funds under the EFTA, but the defense had an argument here that cryptocurrency is not funds.

Ethan Ostroff:

Carlin, that's right. You know, as I read the case and the opinion, the defendants in this case, which included the CEO of this company, right, an individual executive defendant, were trying to latch on to the CFPB's 2016 prepaid accounts under the Electronic Fund Transfer Act and the Truth in Lending Act rule and were trying to argue that somehow, that statement in that rule by the CFPB led to the conclusion that somehow, cryptocurrency falls out of a plain meaning definition of funds, which, interestingly enough, is undefined in the statute and undefined in Reg E.

But as the court correctly noted, what the CFPB stated in that rule was that it actually takes no position with respect to the application of existing statutes like EFTA to virtual currencies and services. And the CFPB advised in that rule that as part of the broader administration enforcement of its enumerated consumer financial protection statutes, it's simply going to continue to analyze the nature of products or services tied to virtual currencies.

The court also acknowledged that regardless, legislative history should only be used to resolve ambiguity or rulemaking statements, which the court didn't see as a problem here because it determined that funds is an unambiguous term that can be defined by Black's Law Dictionary.

One of the other things I thought was interesting about the decision in this context was that it relied upon two other circuit court cases, one from the Sixth Circuit and one from the Fourth Circuit, and, in particular, the Sixth Circuit case from 2022 that dealt with a criminal prosecution under a federal money laundering statute that actually determined that the term funds encompasses any currency that can be used to pay for things and concluded in that case that Bitcoin qualifies as funds under the money laundering statute issue there.

So while this decision in *Uphold* is novel in definitively stating in this court's opinion that cryptocurrency qualifies as funds under EFTA and Regulation E, it's kind of a natural outgrowth from prior decisions that have made decisions about the ordinary meaning of funds to refer to assets of monetary value that are susceptible to ready financial use.

So, in some respects, this is an unsurprising result, although interesting to note the result in the context of the other entities in the ecosystem, as you mentioned, who directly or indirectly hold an account belonging to a consumer.

I think one of the interesting things for us to monitor as the case law develops is whether or not we see any decisions that actually address the issue of who qualifies as a financial institution by indirectly holding an account belonging to a consumer.

This issue of first impression about interpreting funds to include cryptocurrencies under EFTA and Reg E is not the only issue in this case. And there are a couple other interesting points I think we can take away from this case as well.

One claim, as we mentioned, involved two-factor authentication, as you discussed, Carlin, a prevalent account security scheme used very widely by a lot of different entities. Addison, do

you have any thoughts about the rest of this decision and other aspects of it that we should be aware of and tracking?

Addison Morgan:

Let's start out by discussing the issue with Uphold's two-factor authentication system, as described by the plaintiffs. When Uphold creates an account, they're required to set up two-factor authentication. When a user logs in, an authentication server sends a code to a device designated by the user, and this is generally a cell phone. To access his or her Uphold account, the user must input the authentication code that the authentication server sends to the user's designated device.

Ethan Ostroff:

Seems pretty straightforward. That's how two-factor authentication generally works. So what problem did the plaintiffs have with Uphold's two-factor authentication system in this matter?

Addison Morgan:

Apparently, the device that an Uphold user designates to receive his two-factor authentication codes could be deleted, and this could allow an unauthorized third-party privy to the user's username and password to re-designate the two-factor authentication device, which the original user uses to receive the codes from Uphold servers.

So, according to the plaintiffs, Uphold failed to implement two-factor authentication properly because unauthorized third parties should not have been able to access or redirect two-factor authentication codes to an unauthorized device without having access to the user's designated two-factor authentication device itself.

Ethan Ostroff:

So if I'm understanding this correctly, right, they're saying an authorized third party had the user's username and password in order to re-designate a new device, and the plaintiffs are saying they shouldn't be able to redirect to an unauthorized device without having access to the original device itself. Is that right?

Addison Morgan:

Exactly. The two-factor authentication device itself is separate and distinct from the user's username and password, but these things were obviously linked because we're assessing this claim now.

Ethan Ostroff:

It seems interesting to me because I may use my cell phone today for this, right, and then lose my cell phone. It may get stolen tomorrow. I make get a new cell phone. I wouldn't even myself have access to that prior device anymore, right?

Addison Morgan:

Right.

Ethan Ostroff:

So if you followed these allegations to their logical conclusion, you'd say, "Look, that means if someone loses their own original device used for two-factor authentication, that they should no longer have access," right?

Addison Morgan:

Right. They shouldn't. And technically, I think that is what the security of two-factor authentication is based on. And I'm sure there are some back doors where you may still be able to access your account, but I think the issue here was that you should not be able to re-designate an account while I do still have access to my device, right? I still have access to my cell phone, but now somebody is changing the device itself, although I have not lost my cell phone, and I did not approve of that re-designation.

Ethan Ostroff:

I'll be honest with you, I'm not sure how Uphold or any other company would ever know whether or not you do or do not still have access to that original device. It's kind of amazing, the theory behind this, right?

Addison Morgan:

Yeah.

Ethan Ostroff:

So did they just allege that Uphold's two-factor authentication scheme should have been stronger, or is this really about alleging Uphold misrepresented the efficacy of its two-factor authentication scheme?

Addison Morgan:

So it was actually the latter. The plaintiffs filed this claim under New York General Business Law Section 349, and this statute governs deceptive acts and practices. The plaintiffs allege that Uphold violated this law by misrepresenting, both by affirmative representation and by omission, the safety of its systems and services, by failing to give timely warnings and notices, and by failing to implement reasonable and appropriate security measures.

What plaintiffs are really alleging is that they lost their crypto and their personal financial information due to the two-factor authentication flaw, right? Because if you can access my account because you were able to re-designate the two-factor authentication device, that's an issue. And they're alleging that Uphold is the reason that these issues occurred.

Ethan Ostroff:

And then Uphold turns around and argues that the plaintiffs failed to plausibly allege that Uphold engaged in any type of materially deceptive or misleading conduct, and the court agreed with them. How did the court get to that conclusion? What was its rationale?

Addison Morgan:

The court concluded that the plaintiffs could not specify any affirmative misrepresentations that Uphold made with respect to the two-factor authentication issue. And so, like we discussed

earlier, the plaintiffs allege that Uphold misrepresented by omission, not by affirmative misrepresentation, but by omission, that its two-factor identification system and related warnings were safe. But the court held that these allegations were too conclusory and that plaintiffs needed to point to affirmative misrepresentations made by Uphold.

Ethan Ostroff:

So it seems to me... If we go back to section 349 and talk about deceptive acts or practices, they're defined as acts "likely to mislead a reasonable consumer acting reasonably under the circumstances." In order for there to be claims that are actionable under 349, there's got to be something directed at consumers, the acts must be leading in material way, and there's got to be injury, right?

The court's rationale seems to be premised on the lack of an act that Uphold specifically directed at consumers. And all of the plaintiffs alleged that Uphold misrepresented the safety of its two-factor authentication system. There was actually no support, really, factual support, for that claim. Is that right?

Addison Morgan:

That's correct. The plaintiff cited several promises that Uphold made. And most companies make promises. "We have security protocols," et cetera, et cetera. For example, Uphold's general representation is regarding the strength of its security protocols. However, none of Uphold statements actually related to the two-factor authentication issue that we've been discussing, which was basically the foundation of their 349 claim.

Ethan Ostroff:

Gotcha. And then the plaintiffs also argued that there were some other types of violations of New York law, is that right?

Addison Morgan:

Yep. They also argued that Uphold's actions allegedly violated New York's BitLicense regulation, which governs, among other things, licensure disclosure and capital requirements of entities that engage in any virtual currency business activity.

The plaintiffs also argued that Uphold violated Part 5 of the New York Department of Financial Services Regulations, which governs cybersecurity requirements for financial services companies. And then, lastly, the plaintiffs argued that Uphold violated Section 5 of the Federal Tort Claims Act.

Ethan Ostroff:

And the court dismissed each of these arguments, right? The plaintiffs were alleging that Uphold's violations of these statute served essentially as additional deceptive acts under Section 349 and really tried to leverage these alleged statutory violations as predicates for 349 claims. Is that right?

Addison Morgan:

Exactly. The court dismissed all of these claims, right? As you stated, they tried to use them as predicates, but none of those statutes have private rights of actions. And so the court's rationale

is that, "We're not going to let you guys end around the GBL or end around the lack of a private action under these statutes by trying to integrate them into a GBL argument that we've already dismissed on its face."

Ethan Ostroff:

Gotcha. Well, thank you, Carlin and Addison, for joining us today. Thank you to our audience for listening to today's episode. Don't forget to visit our blog, consumerfinancialserviceslawmonitor.com, and subscribe so you can get the latest updates. Please make sure to also subscribe to this podcast via Apple Podcasts, Google Play, Stitcher, or whatever platform you use, and we look forward to talking with you next time.

Copyright, Troutman Pepper Hamilton Sanders LLP. These recorded materials are designed for educational purposes only. This podcast is not legal advice and does not create an attorney-client relationship. The views and opinions expressed in this podcast are solely those of the individual participants. Troutman Pepper does not make any representations or warranties, express or implied, regarding the contents of this podcast. Information on previous case results does not guarantee a similar future result. Users of this podcast may save and use the podcast only for personal or other non-commercial, educational purposes. No other use, including, without limitation, reproduction, retransmission or editing of this podcast may be made without the prior written permission of Troutman Pepper. If you have any questions, please contact us at troutman.com.