NORTON ROSE FULBRIGHT

Blockchain Law

Crypto, terror, fraud and causation —a witch's brew

By Robert A. Schwinger, *New York Law Journal* — May 26, 2026

A year ago, this column explored a number of cases where plaintiffs who had suffered losses from fraud or terrorism brought suits seeking redress against certain digital asset platforms, or individuals involved in developing or running those platforms. See R. Schwinger, "No Virtual Causation for Virtual Assets?", N.Y.L.J., May 27, 2025.

These lawsuits were premised upon the theory that the actual wrongdoers had utilized these platforms to accomplish or support their illegal activities, and that the defendants who were being sued either knew or should have known enough about the wrongdoers' activities on and off the platform to make it appropriate to hold these defendants legally responsible under common law and/or statutory law for the injuries claimed by the plaintiffs.

In most but not all of the cases explored last year, the claims failed. The courts, largely applying traditional proximate cause principles, cited the attenuated causal link between the harms suffered and the conduct of the defendants with respect to the platforms, particularly given the decentralized nature of blockchain-based systems. Whether such judicial thinking might evolve to become more permissive in at least some such cases remained to be seen.

Over the past year, these issues have remained active and the caselaw continues to develop. While courts are not disagreeing much on basic principles, outcomes continue to be highly fact-specific.

The factual variations encountered across the range of lawsuits help illustrate where claims may be viable and where not. And some courts have shown a willingness to allow plaintiffs multiple opportunities to refine their claims in fraud- and terrorism-related crypto claims, to see if they ultimately might be able meet their burden of plausibly alleging causation in such cases against crypto platform defendants.

The attenuation hurdle in fraud causation

In fraud cases, plaintiffs have attempted to leapfrog over the causal gap that often exists between the conduct of the primary wrongdoers and the claimed failings of platforms whom they have sued. While in recent cases the courts largely continue to view proximate cause allegations as being too attenuated in such scenarios, the specifics of the defendants' alleged conduct may possibly furnish a path to relief in the right circumstances, as one of the recent decisions showed.

Among the more commonplace outcomes is the latest installment in the saga of the *Risley v. Universal Navigation Inc.* litigation. In that litigation's first two decisions, 690 F. Supp. 3d 195 (S.D.N.Y. 2023) (*Risley I*), aff'd in part, rev'd in part, 2025 WL 615185 (2d Cir. Feb. 26, 2025) (*Risley II*), as discussed in last year's article, the District Court and the Court of Appeals had rejected attempts to hold developers of the Uniswap Protocol responsible under federal securities laws for their losses from

ROBERT A. SCHWINGER is a partner in the commercial litigation group at Norton Rose Fulbright US.
LINDSAY BRACKEN, an associate in the Firm's litigation group, assisted in the preparation of this column.

Attorney advertising

Reprinted with permission from the May 26, 2026 edition of the *New York Law Journal* © 2020 ALM Media Properties, LLC. All rights reserved.
Further duplication without permission is prohibited. www.almreprints.com – 877-257-3382 – reprints@alm.com.

"scam token" rug pulls and pump-and-dump schemes perpetrated against them by other users of that platform.

In the most recent decision, 2026 WL 572065 (S.D.N.Y. Mar. 2, 2026) (*Risley III*), back in the District Court following remand from the Second Circuit, plaintiffs repled their remaining state-law claims against these defendants. Nevertheless, the court dismissed those claims as well, with prejudice. The court held that the plaintiffs failed to adequately allege that the defendants had actual knowledge of the wrongdoers' conduct or lent substantial assistance to it, so as to be subject to aiding and abetting liability.

Allegations that the defendants "should have known" about the alleged fraud were held insufficient, as New York law on aiding and abetting requires "actual knowledge" of the fraud.

Mere constructive knowledge is not enough, "nor is 'a lower standard such as recklessness or willful blindness.'" Even a "veritable forest of red flags," said the court, is insufficient to impute actual knowledge of ongoing fraud.

The plaintiffs also failed to adequately allege substantial assistance by the defendants in the fraud. The court stated, "merely creating an environment where fraud could exist is not the same as affirmatively assisting in its perpetration." Thus:

> "No matter how they try to dress up their allegations, plaintiffs are basically alleging that Defendants substantially assisted fraud by providing ordinary services that anyone could use for lawful purposes, but that some used for unlawful purposes."

Because substantial assistance was not pled, proximate cause likewise failed. The court held that "the proximate cause of plaintiffs' injuries was the issuers' fraudulent misrepresentations, which led plaintiffs to obtain the Tokens." The court also held that there were no sufficient allegations to support deceptive practices or unjust enrichment claims against the defendants.

In another recent fraud case, *Reca v. Flashdot Ltd.*, 2025 WL 3187079 (Nov. 13, 2025) (Cave, U.S.M.J.), report and recommendation adopted as modified, 2026 WL 82702 (S.D.N.Y. Jan. 12, 2026) (Woods, U.S.D.J.), putative class action plaintiffs whose crypto was stolen by unknown hackers brought RICO claims against a platform and its compliance software vendor, alleging that there were failures to implement adequate KYC/AML controls. These failures, they alleged, allowed money laundering to occur, and thus deprived plaintiffs of the ability to track and potentially recover stolen cryptocurrency.

The District Court upheld the magistrate judge's recommendation to reject this theory of injury, which it characterized as being based upon two separate phases, the first phase being the actual theft, and the second being the inability to track the proceeds of the theft thereafter.

Magistrate Judge Cave concluded that plaintiffs' theory of proximate cause was implausible because the "supposed Phase 2 inability-to-track injury would not exist without the theft injury in Phase 1." The theory involved "an indeterminate number of intervening events and circumstances," and the alleged injuries did not necessarily follow from defendants' claimed acts.

From the standpoint of "but-for" causation, Cave concluded that even accepting independent value in the ability to track stolen cryptocurrency, "absent the bad actors' theft, plaintiffs would not have been in the position of needing to [track and] recover their cryptocurrency" because plaintiffs would not have had any need to trace cryptocurrency already in their possession.

The district judge agreed, holding that "plaintiffs' theory of injury and proximate causation as alleged involved multiple intervening acts that plausibly could have contributed to plaintiffs' loss of the ability to track their cryptocurrency. In addition, the inferences that the plaintiffs urged the court to draw from their allegations "were implausible because they would require the court to go 'beyond the first step in the causal chain.'" Plaintiffs' RICO claims were thus dismissed with prejudice, with leave to amend those claims being denied as futile.

Another fraud case involving claimed KYC/AML deficiencies reached a similar outcome. The court in *Doe v. Stanford Fed. Credit Union*, 2026 WL 412476 (N.D. Cal. Feb. 13, 2026), was presented with a married couple who had been victimized by a crypto fraud scheme in which they wired approximately $600,000 to scammers. The couple then sued not the actual scammers but rather only various recipient and intermediary banks that had transferred and re-transferred the funds, on a theory of aiding and abetting fraud.

The court granted the defendants' motion to dismiss. It held that the plaintiffs' claim failed the knowledge element of aiding and abetting because the complaint focused on how defendants collectively chose "to abstain from KYC/AML procedures" rather than pleading with particularity that any specific defendant knew of the specific fraud Additionally, the complaint failed the substantial assistance element because pleading "[s]ubstantial assistance requires a significant and active, as well as a knowing participation in the wrong."

Plaintiffs' fallback attempt at a negligence claim faced an independent barrier, that "absent extraordinary and specific facts, a bank does not owe a duty of care to a noncustomer," and under California law "owes no duty to nondepositors to investigate or disclose suspicious activities on the part of an account holder."

Fraud allegations that survive the attenuation hurdle

Yet the door apparently is not entirely slammed shut in fraud cases, at least when more compelling facts are presented. This was seen in *Richter v. KRG Trading, Inc.*, 2026 WL 413399 (C.D. Cal. Jan. 7, 2026), another case involving claimed AML deficiencies, where the court denied a motion to dismiss in the face of allegations that presented an additional twist.

Richter was a case "concern[ing] a 'pig-butchering' cryptocurrency scam," in which the plaintiffs' earlier complaints had failed to survive motions to dismiss. Plaintiffs had alleged that certain registered money service business defendants would have detected certain "red flags" had they had "a compliant AML program," and that these failures thus "enabled the alleged fraudulent enterprise to function."

These defendants allegedly "provide cryptocurrency conversion and off-ramp services for shell entities" involved in the scam that were "... 'designed to assure scam victims that their funds would be safely converted into cryptocurrency, thereby lending false legitimacy' to the scheme."

However, "plaintiffs essentially only alleged that [these defendants] processed wires and benefitted incidentally, not that [they] agreed with the scammers to defraud plaintiffs or participated in the formation or operation of the fraud itself." Plaintiffs' prior complaints against these defendants thus had been dismissed, by analogy to the principle that a bank which merely receives criminal proceeds is insulated from liability because "the underlying criminal activity is an intervening and superseding cause that cuts off liability."

In their latest pleading, however, the *Richter* plaintiffs added new allegations that the money service business defendants "not only derived a material financial benefit from processing the fraudulent transactions," but actually "diverted hundreds of thousands of plaintiffs' funds directly into their own shell entities." The court held that these new allegations changed the causation analysis.

Such allegations, held the court, were sufficient to plausibly allege a "direct and proximate causal relationship" to plaintiffs' injury. Coupled with the allegation that these defendants "had already entered in agreements to provide banking infrastructure to other defendants before plaintiffs' first transfer", the latest pleading permitted "a plausible inference" that the money service business defendants were "more than a passive downstream [sic] and that a fraudulent conspiracy existed." The court thus sustained plaintiffs' civil conspiracy and RICO claims against these defendants and denied the motion to dismiss.

Terrorism cases now facing stronger causation challenges

In terrorism cases, plaintiffs claiming injuries from terrorist acts have brought claims against cryptocurrency platforms where transactions connected to the perpetrators took place. Such claims have been brought under the Antiterrorism Act (ATA), 18 U.S.C. §2333(a), and its additional "aiding and abetting" provision known as the Justice Against Sponsors of Terrorism Act (JASTA), 18 U.S.C. §2333(d). New such cases over the past year have shown a change in the causation burdens that plaintiffs bringing such claims will be required to meet.

Last year's column discussed the nuanced outcome in *Raanan v. Binance Holdings Ltd.,* 2025 WL 605594 (S.D.N.Y. Feb. 25, 2025), which arose out of the Oct. 7, 2023 terrorist attacks. In that case, the plaintiffs' ATA claims failed for lack of proximate cause between the injuries claimed and the defendants' alleged AML/KYC failures, but the court held that the claim based on JASTA's aiding-and-abetting provision (which extends to persons who "knowingly provide substantial assistance" to an act of international terrorism) could move forward.

The *Raanan* court held that because there were sufficient allegations in that case "that the defendants were generally aware that they were playing a role in international terrorism," that they "failed to comply with—indeed, intentionally evaded—[various] regulatory requirements," and that they did so "intentionally... in order to retain illicit actors [like the terrorist organizations responsible for the attacks] on the platform" as customers. The court held this sufficient to support a JASTA claim despite the lack of a "close nexus" between the defendants' activities on the platform and the attacks.

More recently, though, another Southern District judge concluded in *Troell v. Binance Holdings Ltd.*, 2026 WL 636849 (S.D.N.Y. Mar. 6, 2026), that JASTA claims against platforms in terrorism cases did indeed require a closer nexus to be pled between the defendants' activities on the platform and the attacks causing the plaintiffs' injuries, based on a recent intervening Second Circuit decision.

Troell explained that JASTA claims such as these were governed by a trio of higher-court decisions:

> "First, JASTA itself explicitly references the D.C. Circuit's decision in *Halberstam v. Welch*, 705 F.2d 472, 227 U.S. App. D.C. 167 (D.C. Cir. 1983), as providing the 'proper legal framework' for assessing the scope of aiding-and-abetting liability. 130 Stat. at 852.
>
> Second, the Supreme Court provided clarification as to the proper application of this framework to institutional entities that provide generalized services to the public in *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 143 S. Ct. 1206, 215 L. Ed. 2d 444 (2023). And finally, the Second Circuit recently addressed the viability of aiding-and-abetting claims brought against institutions that provide financial services to terrorists in *Ashley v. Deutsche Bank Aktiengesellschaft,* 144 F.4th 420 (2d Cir. 2025)."

The *Troell* court found that the plaintiffs plausibly had alleged that the defendant platform was generally aware that it was playing a role in terrorist financing, thus taking the case beyond the mere provision of ordinary services discussed in *Twitter.* The court also noted plaintiffs' allegation that the defendants had advised users to use Virtual Private Networks (VPNs) to mask their true IP addresses and thus their physical locations, in order to allow them to evade international sanctions. Nevertheless, plaintiffs' claims still failed.

The court held that the plaintiffs were unable to satisfy the "knowing and substantial assistance" prong under JASTA because of the lack of a "definable nexus" between the platform conduct and the specific attacks. Indeed, said the court, plaintiffs' broad allegations of the platform facilitating illicit activity "writ large" actually undermined an inference of intent to aid a particular terrorist organization's attacks, as required under the Second Circuit decision in *Ashley.*

For some of the terrorist organizations involved in the attacks at issue, the court held that the plaintiffs' wallet-transaction allegations were too conclusory, as not identifying wallet owners, relationships, timing relative to attacks, or transaction nature.

For some other terrorist groups, described as "a closer call", the court held that broad allegations of facilitating illicit actors generally undercut the required inference of specific intent under *Ashley*. The court noted that *Ashley* rejected arguments based "on money's fungibility" to get past having to show a direct nexus between actions on the platform and particular attacks.

The court acknowledged that the *Raanan* decision had come out differently on the causal nexus analysis, but it distinguished *Raanan* as having been decided before the Second Circuit's decision in *Ashley.* The court concluded that *Ashley* required dismissal on *Troell's* allegations.

However, the court did grant leave to amend, recognizing plaintiffs still might be able to plead transaction-level detail to establish the required nexus.

Just a few days later, a federal court outside New York likewise found a terrorism case against a platform deficiently pled for lack of transaction-level facts linking the defendants' actions with the plaintiffs' terrorism-related injuries. *Newman v. BAM Trading Servs., Inc.,* No. 2:24-cv-134-ECM-CWB, slip op. (M.D. Ala. Mar. 11, 2026), was another case arising from the Oct. 7, 2023 attacks. The complaint there asserted claims under the JASTA provisions of the ATA, as well under the Alien Tort Statute, 28 U.S.C. §1350, and common-law negligence theories.

The court dismissed the complaint, holding it to be deficient "shotgun pleading" that made only conclusory allegations about "substantial financial assistance" having been provided by the defendants to the terrorists. Similar to *Troell*, the court in *Newman* cited the lack of any detail on critical points such as:

> "what such assistance relates to Hamas and what such assistance relates to PIJ, what assistance allegedly was provided by any one or more of the defendants, or how the assistance 'aided and abetted... in committing, planning, or authorizing acts of international terrorism.'"

The court thus ordered repleading and required, among other things, allegations connecting each defendant's conduct to specific injuries, identifying particular transactions relating to particular groups and the Oct. 7 attacks, and identifying special treatment or affirmative acts by the defendants directed toward the relevant terror groups, rather than just general allegations of facilitating terrorist group attacks through activity on a cryptocurrency platform.

Conclusion: The brew is still bubbling

The cases from this year and last show that there is no simple or single factor that determines whether cases against platforms that are brought by plaintiffs who suffered injuries from fraud or terrorism will survive an early motion to dismiss or not. The cases all require a complex, fact-specific analysis of what exactly the defendants are alleged to have done, what they knew, what they intended, and how that connects to the actions of third parties who were the primary wrongdoers against the plaintiffs.

In this witch's brew of factors, certain common threads do appear, though. Merely alleging general failings on the part of the platform, or the platform's general awareness of illicit activity by its users, without more specifically connecting it to a specific harm caused by a specific third party, tends to encounter judicial resistance as not bridging the gaps in causation between the platform defendants and the primary wrongdoers.

By contrast, cases that allege direct participation by the defendant in the primary wrongdoers' activities, as opposed to mere enabling or AML/KYC regulatory noncompliance, or where there are detailed allegations of transaction-specific facts directly connecting the defendant's conduct to particular injuries, may be able to move past the threshold of plausibly alleging actionable causation.

Thus, a mere "but-for" chain tracing through multiple independent actors seems unlikely to be enough. The possibility raised by *Raanan* last year that plaintiffs bringing terrorism-related claims under JASTA might face a lighter burden in terms of pleading causation seems to have been set back by the refinement in JASTA caselaw seen in the Second Circuit's *Ashley* decision, as *Troell* illustrated.

But all is not lost for such plaintiffs. Even where the allegations as originally pled in fraud-and terrorism-related cases brought against crypto platforms may prove deficient, courts seem willing to be liberal in granting leave to amend where there is some reason to think that upon repleading the absent necessary detail could be provided.

Whether plaintiffs in particular cases can assemble the right ingredients—such as transaction-level linkage, direct participation, and a definable nexus with specific wrongful acts by terrorists and fraudsters—for the witch's brew of factors in the causation analysis seems likely to be the question that will dictate outcomes in future rounds of such lawsuits.

Norton Rose Fulbright © 2026. All Rights Reserved
US_71470 - 05/26