NORTON ROSE FULBRIGHT

Blockchain Law

Redressing cryptocurrency losses through negligence claims

Robert A. Schwinger, *New York Law Journal – November 19, 2019*

In his Blockchain Law column, Robert Schwinger discusses two recent California federal court rulings—'*Terpin v. AT&T*' and '*Fabian v. LeMahieu*'—which indicate that the ability of negligence claims involving cryptocurrency thefts to survive dismissal at the pleading stage will turn on the plaintiff's ability to adequately plead the elements of a negligence claim: duty, breach, causation and damages.

As the popularity of cryptocurrencies continues to mount, hacking and theft directed at individual cryptocurrency accounts and cryptocurrency exchanges has proliferated as well. See, e.g., CipherTrace, Cryptocurrency Anti-Money Laundering Report, 2019-Q2 (July 2019) (estimating approximately $4.26 billion in losses from cryptocurrency thefts, hacking, exit scams and other misappropriations in 2019). Surging cybercriminal activity in the cryptocurrency space has, not surprisingly, spurred a rise in litigation brought by cryptocurrency investors seeking redress for their lost funds and lost cryptocurrency tokens, including through claims that the negligence of others led to their losses.

While cryptocurrency technologies are still relatively new, the relevant legal principles for negligence claims are not. Two recent California federal court rulings indicate that the ability of negligence claims directed at cryptocurrency thefts to survive dismissal at the pleading stage will turn on the plaintiff's ability to adequately plead the traditional elements of a negligence claim—duty, breach, causation and damages.

$24 Million SIM Card Swap

The consequences of failing to adequately allege causation in a negligence claim arising from a cryptocurrency hack are illustrated by a case decided this past summer, *Terpin v. AT&T Mobility*, 2019 WL 3254218 (C.D. Cal. July 19, 2019). *Terpin* was brought by prominent cryptocurrency investor Michael Terpin, who alleged that he fell victim to two hacks of his personal phone in the course of 11 months, allegedly as a result of his cellphone provider's failure to properly protect his account, thus supposedly allowing hackers to gain access to his phone and ultimately steal $24 million worth of his cryptocurrency. Terpin sued his cellphone service provider for negligence and a number of other contract and tort-based claims.

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US LLP.
Jacob Laksin, an associate in the commercial litigation group, assisted in the preparation of this article.

Terpin alleged that in June 2017 his "phone suddenly became inoperable because his cell phone number had been hacked." The hackers ultimately succeeded in remotely changing Terpin's password, gaining access to Terpin's phone number and those of his accounts that used his phone number for authentication, including his cryptocurrency and Skype accounts. Impersonating Terpin, the hackers then convinced a client of Terpin's to send them Terpin's cryptocurrency, which they then stole.

The cellphone provider was able to cut off the hackers' access to Terpin's phone later on the same day, but not before "the hackers had stolen substantial funds" from Terpin. Terpin later met with representatives of the provider to discuss the hack and was allegedly assured that his account would be placed "on a higher security level with special protection," including a six-digit passcode (known only to Terpin and his wife) that would be required for any change to Terpin's cellphone account or the transfer of his phone number to another phone.

Despite the added security, just seven months later in January 2018 Terpin's phone "again became inoperable." Terpin alleged that he eventually learned that an employee at one of the cellphone provider's stores in Connecticut had been tricked into assisting an unnamed imposter with a so-called "SIM card swap," in which the employee allegedly transferred Terpin's phone number to a SIM card (the small removable chip that stores the phone user's identification information) controlled by the criminal imposter. Terpin alleged that he then contacted his cellphone provider to cancel his phone number but the provider failed to act quickly enough, thereby allowing hackers to access Terpin's personal information, including phone calls and text messages, and to gain access to his cryptocurrency accounts. Terpin alleged that as a result of the SIM card swap the hackers stole nearly $24 million worth of his cryptocurrency.

A Proximate Cause Problem

Based on these events, in August 2018 Terpin sued the cellphone service provider for negligence and a variety of other causes of action. The defendant cellphone provider moved to dismiss the negligence claim (and indeed all the claims in Terpin's complaint) for failure to adequately allege proximate cause for his alleged injuries. The defendant raised two principal arguments. First, it argued that the criminal acts of the hackers and imposter were an intervening cause that severed any negligence on the part of the provider as an alleged proximate cause of Terpin's harm. Second, the defendant argued that Terpin failed to adequately allege how the purported SIM card swap, in which Terpin's phone number was allegedly transferred to the imposter, resulted in his losing $24 million worth of cryptocurrency.

The court rejected the first argument for dismissal based on intervening causation. Relying on precedent holding that the criminal acts of a third party do not constitute an intervening or superseding cause if they are reasonably foreseeable, see *Ileto v. Glock Inc.*, 349 F.3d 1191, 1208 (9th Cir. 2003); *Kane v. Hartford Accident & Indem. Co.*, 98 Cal. App. 3d 350, 359, 159 Cal. Rptr. 446 (1979), the court noted that Terpin had informed his provider in June 2017 that he was the victim of a SIM card swap, and was advised by the provider that his account had been placed on higher security with special protection. The court thus concluded that the provider "was put on actual notice that Mr. Terpin's account was at risk," and that "[d]espite this knowledge, Mr. Terpin was again the victim of a SIM card swap in January 2018, allegedly as a result of [the provider's] assistance." Accordingly, the court held that Terpin's allegation that the criminal act of the hackers/imposter was reasonably foreseeable was sufficient, such that Terpin's negligence claim should not be dismissed on an intervening cause basis.

Nevertheless, Terpin's claim faltered on proximate cause grounds, the court accepting the provider's second argument that Terpin had not sufficiently pleaded how the SIM card swap was the proximate cause of his loss of $24 million worth of cryptocurrency. While Terpin alleged that the SIM card swap provided hackers with access to his phone number, the court took issue with Terpin's failure to further "explain how the hackers accessed Mr. Terpin's cryptocurrency account(s), whether they sold Mr. Terpin's cryptocurrency then transferred the money, or whether they transferred the cryptocurrency to a cold wallet. At this stage, the court is left to speculate how having access to Mr. Terpin's phone number resulted in the theft of cryptocurrency." On this basis, the court dismissed Terpin's claims to the extent they were based on the alleged $24 million in damages, although allowing him leave to replead.

$170 Million Theft From Cryptocurrency Exchange

A negligence claim proved more successful before a different California federal court in *Fabian v. LeMahieu*, 2019 WL 4918431 (N.D. Cal. Oct. 4, 2019), another cryptocurrency

theft case involving negligence claims brought on a class action basis by a victimized cryptocurrency investor. Although *Fabian* involved issues similar to *Terpin*—the theft of a substantial volume of cryptocurrency, in this case from an online cryptocurrency exchange—the plaintiff's negligence claim against the cryptocurrency's primary development team was held sufficient to survive a motion to dismiss, by setting forth the requisite tort elements of duty, breach, causation and damages.

In *Fabian*, the plaintiff cryptocurrency investor filed a purported class action on behalf of a proposed class of U.S. investors against the cryptocurrency platform Nano and key members of its development and marketing team, as well as against the Italy-based cryptocurrency exchange where Nano was traded, BitGrail, and its principal. According to the amended complaint, "Nano purports to have created a faster, cheaper, and more easily scalable blockchain and cryptocurrency that improves upon earlier blockchains and cryptocurrencies such as the widely-popular bitcoin." Plaintiff alleged, though, that $170 million worth of the Nano cryptocurrency had been stolen from the BitGrail exchange as a result of the negligence of the Nano defendants. Plaintiff's 11-count amended complaint asserted not just federal securities violations, but also contract and tort claims, including a negligence claim.

The amended complaint alleged that the Nano defendants developed a Bitcoin-like cryptocurrency, traded as digital coins called "Nano Coins" or "XRB." Plaintiff further alleged that beginning in April 2017 the Nano defendants used social media like Reddit and Twitter to promote XRB and to encourage the investing public to purchase, trade and store their XRB through BitGrail, an online exchange dedicated to creating a market for XRB, assuring investors "that their funds were safe on the BitGrail Exchange."

But in early February 2018, BitGrail announced that it had "lost" $170 million worth of XRB—totaling approximately 80 percent of the XRB held in BitGrail customers' accounts and 15 percent of all the XRB in existence—due to "unauthorized transactions." Plaintiff asserted that as a result of the massive XRB theft, he lost all of the XRB in his BitGrail wallet, and that Nano holders in the purported class suffered similar injuries.

The Nano defendants moved to dismiss the various counts in the amended complaint on a number of grounds. With respect to plaintiff's negligence claim, the Nano defendants argued that the claim failed because plaintiff did not adequately allege the essential tort elements of duty, breach, causation and damages. Unlike the result in *Terpin*, however, the court in *Fabian* concluded that plaintiff had adequately pleaded each of these elements, including causation.

Duty and Causation Established

In evaluating the defendants' challenge to the negligence claim, the court examined whether the Nano defendants owed a duty of care to the plaintiff by applying a six-factor test set forth by the Supreme Court of California in *Rowland v. Christian*, 69 Cal. 2d 108, 113, 443 P.2d 561, 70 Cal. Rptr. 97, 101 (1968). Under that test, the court considers

> (i) the foreseeability of the harm to the plaintiff;
>
> (ii) the degree of certainty that the plaintiff suffered injury;
>
> (iii) the closeness of the connection between the defendant's conduct and the injury suffered;
>
> (iv) the moral blame attached to the defendant's conduct;
>
> (v) the policy of preventing future harm; and
>
> (vi) the extent of the burden to the defendant and consequences to the community of imposing a duty of care.

The court determined that these factors weighed in favor of a finding a duty owed by the defendants to the plaintiff.

As the court explained:

> It was foreseeable that a lack of security on the primary exchange for [XRB] would cause harm to individuals who, like plaintiff, deposited their [XRB] on that exchange and that any security failure on that exchange would result in harm to plaintiff and other similarly situated individuals. Further, it is plausible that Nano defendants' alleged conduct, if true, could be viewed as morally reprehensible and this type of action could further the goal of preventing future harm. Imposing a duty to exercise care in this instance will not result in an undue burden on the Nano defendants or the industry at large. Moreover, Nano defendants' conduct was proximately connected to plaintiff's injury, even if through the actions of the BitGrail defendants.

Because these factors weighed in favor of finding a duty owed by Nano defendants to plaintiff, the court held that the plaintiff had sufficiently alleged that the Nano defendants had "a duty to exercise reasonable care with respect to their management of XRB," and that they had also made "sufficient allegations that Nano defendants breached that duty."

While the court was less impressed with what it termed plaintiff's "generic allegation" of causation, it nonetheless held that plaintiff had adequately pleaded causation by incorporating by reference statements of an Italian bankruptcy court that was overseeing the bankruptcies of BitGrail and its principal. The Italian court had found that the alleged theft of the XRB had been made possible through exploitation of a fault in the code developed by the Nano defendants, which caused certain transactions to be entered two or more times. The court concluded that these "allegations of causation based on 'double withdrawals'" satisfied plaintiff's burden to plead causation and precluded dismissal of the negligence claim.

Conclusion

Although the facts of *Terpin* and *Fabian* are not parallel, they show that the viability of negligence claims for lost or stolen cryptocurrency will hinge on plaintiffs' ability to sufficiently allege the standard tort elements like duty and causation. In *Terpin*, plaintiff's negligence claim was doomed by his inability to plead a clear causal connection between the hackers' gaining access to his phone and the subsequent loss of $24 million. In *Fabian*, on the other hand, a direct link between the blockchain code developed by defendants and the resulting cryptocurrency theft permitted the plaintiff's negligence claim to survive dismissal. These cases highlight the importance for counsel seeking to prosecute such negligence claims of getting down into the weeds of the systems at issue so that counsel can show in a complaint's allegations how they function. In this way, counsel can connect the dots of causation for the courts who must evaluate such claims, despite their lack of prior familiarity with the cryptocurrency/blockchain world and its technology.