NORTON ROSE FULBRIGHT

Blockchain Law

Personal jurisdiction in the age of blockchain

Robert A. Schwinger, *New York Law Journal – November 21, 2018*

As commercial activity increasingly intertwines with applications of blockchain technology with participants around the world, courts have had to grapple with the personal jurisdiction implications of such arrangements. Will participants in these blockchain applications based outside the United States find themselves subject to U.S. jurisdiction when disputes arise, based on how they have conducted their activities? Two recent New York federal court decisions examined such questions under traditional personal jurisdiction principles and upheld exercising personal jurisdiction over nonresident defendants.

'Alibaba Group Holding Ltd.'

Alibaba Group Holding Ltd. v. Alibabacoin Found., 18-CV-2897 (JPO), 2018 WL 5118638 (S.D.N.Y. Oct. 22, 2018), involved a suit by Alibaba Group Holding Limited, the parent corporation for a multinational web services conglomerate based abroad, against Alibabacoin Foundation and related parties to enjoin alleged trademark infringement, alleging they were using Alibaba's trademarked names and symbols to promote sales of their "AlibabaCoin" cryptocurrency. The defendants, all based in Dubai and Belarus, argued that the New York court could not properly exercise personal jurisdiction over them in this action by a nonresident plaintiff.

The court looked at whether the defendants had purposefully "transact[ed] any business with the state" of New York as required under New York's long-arm statute, N.Y. Civ. Prac. L. & R. §302(a)(1), and then further analyzed whether the exercise of personal jurisdiction comported with federal constitutional due process requirements. It held that the defendants' activity satisfied these tests.

The court found purposeful transaction of business in New York because "[d]uring discovery, Defendants produced a list of the email addresses associated with AlibabaCoin investors, and an investigation has revealed that at least one of these email addresses—connected to three transactions—belongs to an individual who overwhelmingly appears to be a New York resident." The defendants argued in response that "these sales did not occur in the United States because they consist of ledger entries made in Minsk, Belarus, following observation of changes in 'blockchain' data outside the United States," but the court deemed this argument "unpersuasive," explaining that, as with a debit card purchase, "it would strain common usage to say that the transaction occurs at the potentially remote location of the servers that process the buyer's ... activit[y] and not at the location where the buyer clicks the button that commits her to the terms of sale."

Robert A. Schwinger is a partner with Norton Rose Fulbright US LLP.

The court also rejected defendants' argument that their role in these transactions was not purposeful, based on their claim that "unbeknownst to [them], New York-based users of their website chose to effectuate cryptocurrency sales by initiating 'data exchanges' with Defendants' out-of-state electronic 'apparatus.'" The court held this argument "contrary to precedent" that had been developed in personal jurisdiction rulings involving website sales by out-of-state concerns to New York customers.

The court also held these transactions had a substantial relationship with Alibaba's trademark infringement claims. Noting that Alibaba had presented "evidence that over one thousand New York users had visited Defendants' website by mid-June 2018," the court held Alibaba had "established a reasonable probability that the transactions at issue here are not isolated instances, but rather a part of a larger business plan that involves the purposeful marketing and sale of AlibabaCoin to, among others, New York consumers."

"Ultimately, by adducing evidence that a New York resident has purchased AlibabaCoin through Defendants' website, Alibaba has demonstrated a reasonable probability that Defendants have transacted business in New York within the meaning of New York's long-arm statute."

Exercising personal jurisdiction over these defendants also met federal due process reasonableness requirements, said the court. It rejected defendants' suggestion that "subjecting them to litigation in New York would present so great an inconvenience as to constitute a deprivation of due process," given defendants' "obvious familiarity with internet communication" in "this modern age." It further noted that "New York has a clear interest in protecting in-state consumers from confusion resulting from the misappropriation of trademarks or trade dress," and that "Alibaba likewise has an interest in safeguarding its corporate reputation among potential New York customers or investors." Lastly, the court held that the fact that related proceedings might be pending in other counties did not suggest "that an exercise of personal jurisdiction here would be inefficient or would trench on the prerogatives of other states."

Accordingly, the court rejected defendants' personal jurisdiction challenge and issued preliminary injunctive relief against the alleged trademark infringement.

'PlexCorps'

SEC v. PlexCorps, No. 17-cv-7007 (CBA) (RML), 2018 WL 4299983 (E.D.N.Y. Aug. 9, 2018), was an SEC enforcement action charging the defendant promoters of the "PlexCoin" cryptocurrency with various counts of securities fraud, alleging they had participated in a fraudulent scheme to raise funds from thousands of investors. The individual defendants, based in Canada, moved to dismiss for lack of personal jurisdiction.

PlexCoin had been sold through an Initial Coin Offering (ICO) which had been publicized through a "white paper" and through webpages and Facebook accounts. Early purchasers had been promised a return on investment of 1,354 percent within 29 days.

In assessing purposeful contacts with the United States, the court noted that both individual defendants had traveled to the United States at the start of the ICO pre-sale. Although the defendants claimed the trip was for "leisure" purposes, the court said the evidence suggested it "related to the PlexCoin venture," noting that one of the individual defendants "registered two PlexCoin-related websites with [a] United States registration company ... during the trip, and logged onto PlexCoin's PayPal account about 20 times."

The court also cited "[t]he Individual Defendants' repeated use of United States-based payment servicers" such as PayPal, Square, Stripe and Kraken as being "significant" contacts, particularly where U.S. dollar transactions were involved. The court analogized this to cases holding that "[t]he use of a forum's banking system as part of an allegedly wrongful course of conduct may provide sufficient jurisdictional contacts when that use is an integral part of the wrongful conduct."

Similar to the defendants in *Alibaba*, the Individual Defendants argued that jurisdiction was not proper "because the actual sale takes place outside the United States," arguing that "[b]ecause PlexCoin sales are not finalized until the cryptocurrency transfer occurs, and because the transfer does not complete until the PlexCoin owner publicly logs a record of the transfer on the online, network-wide ledger," the PlexCoin sales "necessarily occur[] at the location of the servers of the PlexCoin owner publicly logging the transfer." The court rejected this argument,

stating "even if the final step of those sales (the public transfer of PlexCoin on the ledger) occurred outside the United States, the initial steps (the payment through the accounts) involved in-forum contacts."

The court lastly pointed to "the purposeful distribution of web content to United States investors," focusing on Facebook accounts and websites through which the defendants advertised and marketed to persons in and outside the United States, and websites that were used "to market and ultimately process sales to persons both within and without the United States." The court held that defendants' Facebook activity, while not necessarily dispositive, was a "notable contact." The court cited the "interactive" nature of some of these Facebook accounts, noting that they conveyed information and responded to questions about the ICO, and provided links to the plexcorps.com website. It found that "[t]he Facebook accounts were integral to finding investors and directing statements at them to encourage them to participate in the alleged fraudulent scheme," and moreover that the defendants "directed Facebook advertisements and messages containing fraudulent misrepresentations to potential purchasers who were United States residents."

The defendants claimed they excluded the United States from their Facebook marketing campaign and never directly communicated with potential United States purchasers. However, the court noted that PlexCoin's "marketing strategy" as stated in its white paper was to "focus[] ... efforts on Facebook," and that Facebook was their "main ally" in making PlexCoin known to the "highest number of people possible," with at least one advertising campaign specifically targeting "North America." In fact, "two United States purchasers declared that they learned about the sale from Facebook ads."

The court also pointed to the www.plexcoin.com website, which "is interactive, is accessible to United States buyers, and facilitates sales by those buyers," including taking credit card information and sending emails to users. "Four United States buyers declared that they created accounts to purchase PlexCoin." Declarants attested that "[e]veryone involved with the PlexCoin project" knew of purchases from the United States buyers and even the defendants admitted that PlexCoin employees "suspected from the outset that some individuals from the United States would attempt to access the website and purchase PlexCoin." While at one time the website required purchasers to certify they were not United States citizens or residents, the evidence showed the defendants "knew the checkbox and Exclusion clause were at least somewhat ineffective," as they "learn[ed] about purchases from United States-based IP addresses." Moreover, the checkbox statement was later removed from the website to try to gain more United States-based purchasers.

Finally, as in *Alibaba*, the court upheld exercising personal jurisdiction over the nonresidents under constitutional reasonableness requirements. Like the *Alibaba* court, the *PlexCorps* court cited how "the conveniences of modern communication and transportation ease what would have been a serious burden only a few decades ago." The court also noted the United States' "strong federal interests in pursuing securities cases and protecting domestic investors," and rejected the notion that exercising jurisdiction here could interfere with related proceedings ongoing in Canada.

Conclusion

In both *Alibaba* and *PlexCorps*, the courts were not persuaded by personal jurisdiction defenses based on arguments about how and where blockchain transactions were effectuated and recorded. Instead, the courts upheld jurisdiction by focusing on traditional jurisdictional indicators such as marketing and sales activity directed toward the United States, use of interactive websites, website purchases, and use of U.S. financial systems in receiving payment. Such holdings may help provide comfort to persons affected by such activity that they will not lose access to U.S. courts for relief against nonresidents merely because blockchain activity is involved that takes place overseas. As more such cases arise, the courts will make clearer whether they will follow the personal jurisdiction approach taken by these courts when faced with blockchain fact patterns.

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.