MARCH 30, 2018

Legaltech news ONLINE

An ALM Publication

Litigating Cryptocurrency Fraud? Wait for the Right Time and Place

Kobre & Kim litigators found early success going after a cryptocurrency fraudster. But a lot depended on how and where the fraudster transferred the stolen goods.

BY RHYS DIPSHAN

While cryptocurrency trading has long evaded the purview of regulators and courts alike, its days as the Wild West of finance may be coming to an end. Still, in such a fast-evolving industry, scams can be rampant, and it's not always clear how to fight back against potentially anonymous traders using exchange platforms registered all around the world.

Cryptocurrency fraud litigation can result, but certain variables have to align just right. Just ask David McGill and Benjamin Sauter, litigators at Kobre & Kim who in February 2018 filed a complaint in the Superior Court of Delaware on behalf of their client Elizabeth White. White, who according to the complaint is the CEO of a Delaware-registered company which sells fine art, luxury goods and "is also actively involved in cryptocurrency mining, trading, and investing," was the victim of cryptocurrency fraud.

In late December 2017, an anonymous man referred to in the complaint as John Doe contacted White about a potential cryptocurrency transaction, where White would sell Doe 484,000 ripple—a type of cryptocurrency—in exchange for 46.5 bitcoin. The transaction would take place on a specific online escrow platform that would hold Doe's bitcoin until White sent her cryptocurrency to Doe's digital "wallet."

But when White went through with the transaction, Doe claimed he never received the funds.

The complaint alleges that though Doe specified the wallet address to White while communicating with her on the escrow platform's chat service, he was able to fraudulently alter the chat message "to show a different wallet address, thus giving the false impression that Plaintiff had made an error" and sent the money to the wrong wallet.

Shortly thereafter, Doe opened a "dispute" with the escrow platform, which canceled the transaction and returned the bitcoin to Doe. White never received her 484,000 ripple back.

But White was able to trace her ripple to the wallet that Doe initially told her to deposit in. From there, she traced it through

several exchanges Doe made to a digital wallet on the Delaware-registered cryptocurrency exchange platform Bittrex.

McGill and Sauter quickly filed a complaint in a Delaware court and asked Bittrex to freeze the account belonging to Doe. The exchange complied, but told the attorneys it would not disclose the identity of Doe without a subpoena, which McGill and Sauter are currently seeking in court. McGill noted his team's work in getting the exchange to freeze the account of the alleged fraudster could "potentially serve as a model for asset recovery."

"Obviously, we haven't gotten there yet, but at this point we have been successful in getting the account that is harboring stolen assets frozen," he explained.

A lot of variables had to align just right in order for the attorneys' strategy to get this far. For one, Bittrex was registered in Delaware, and not overseas. What's more, the ripple cryptocurrency operated on a public blockchain that "records the transactions and even discloses some information about where the asset goes" in real time, Sauter said.

If one can act fast, McGill added, it presents "a real opportunity to recover assets in this area, which is very difficult to do because of the speed at which people are able to convert digital currency in different forms and move them around the world."

Acting fast, of course, meant getting Bittrex on board. But here, the legal team was prepared as well. "We are fortunate to have contacts at a lot of the relevant cryptocurrency exchanges and future exchanges," McGill said, adding that his team had a "network of contacts" at Bittrex that they used to get John Doe's account frozen.

It also helped that Bittrex, as a financial exchange, followed its legal obligation to keep the "identities, addresses, phone numbers and contact information for the people who do business" on its platform, Sauter said, adding that for other cryptocurrency exchanges, this "hasn't always been done."

Of course, Bittrex's cooperation was also vital in allowing McGill and Sauter to go after the alleged fraudster.

"If exchanges do not want to help this process and are not willing to be cooperative, that would pose obstacles to defrauded individuals' ability to track their assets," Sauter said. But he added that exchanges that "want to be a mainstream part of the economy and financial infrastructure have incentives to help not only defrauded victims recover their funds, but to not facilitate that part of the economy that is not legitimate."

Of course, McGill and Sauter aren't the only ones finding some success in combating cryptocurrency fraud. The Federal Trade Commission announced this month that it had frozen the assets of four individuals involved in cryptocurrency schemes. The move comes as the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission have stepped up action against cryptocurrency businesses for fraud and illicit activity.

What's more, also this month, the U.S Department of Treasury's Office of Foreign Assets Control moved to address fraud in the cryptocurrency space, announcing it may sanction "specific digital currency addresses associated" with people already under sanctions.