Client Alert

Akin Gump
STRAUSS HAUER & FELD LLP

When Airdrop? New Approach for Service of Anonymous Crypto Defendants

June 8, 2022

Blockchain – Crypto Theft – Alternative Service on Anonymous Defendants

Jurisdictions the world over are seeing a marked increase in civil cases relating to crypto theft, fraud and misrepresentation. However, a major stumbling block for claimants is how to serve anonymous defendants of unknown citizenship with court papers. A recent case in the United States has set an interesting precedent in dealing with this issue that is likely to be mirrored in other jurisdictions. The New York State Supreme Court ordered that documents be served on the anonymous person(s) controlling an Ethereum address by way of a 'service token' being airdropped into the address (the "Service Token"). The Service Token contained a hyperlink to a website on which the court papers were published.

Facts of the Case

The plaintiff, LCX AG ("Plaintiff"), a virtual currency exchange based in Liechtenstein, brought an action for theft of virtual assets against 25 anonymous 'John Doe' defendants ("Defendants"). The alleged theft resulted from a hack of one of the Plaintiff's digital wallets, with the Defendants transferring out approximately US $8 million worth of virtual assets (the "Stolen Assets").

The Defendants then took numerous measures to obscure the resulting transaction trail, including transferring the Stolen Assets to Tornado Cash, a mixing service that effectively 'washes' crypto assets by breaking the on-chain link between source and destination addresses.

Despite these measures, the Plaintiff was able to trace the Stolen Assets via expert tracing services. US $1.3 million of the Stolen Assets ended up being stored in the cryptocurrency stablecoin know as USD Coin ("USDC") at a single address on the Ethereum Blockchain (the "Address"). The controller of the address was unknown to the Plaintiff.

If you have any queries regarding the above, or crypto-related disputes more broadly, the experienced team at Akin Gump is on hand to assist:

Graham Lovett
Partner
glovett@akingump.com
Dubai
+ 971 4.317.3040

Wael Jabsheh
Partner
wjabsheh@akingump.com
Abu Dhabi
+ 971 2.406.8525

Michael Stewart
Associate
stewartm@akingump.com
Dubai
+ 971 4.317.3044

Centre Consortium LLC ("CCL") is the entity which governs the USDC protocol and has the power to block individual Ethereum addresses from sending and receiving USDC, a practice known as 'blacklisting'. CCL was added as an interested nonparty.

The Plaintiff, concerned that the Defendants could sell or transfer the remaining USDC at any time, sought a preliminary injunction and temporary restraining order (1) prohibiting the Defendants from disposing of the Stolen Assets, including those held at the Address, and (2) directing CCL to block the Address.

Court Order

On 2 June 2022, the Supreme Court ordered the Defendants to show cause why a preliminary injunction in the terms sought should not be issued (the "Show Cause Order"). Of most interest, the Plaintiff was ordered to serve a copy of the Show Cause Order, together with all related papers, on:

> *"...the person or persons controlling the Address via a special-purpose Ethereum-based token (the Service Token) delivered – airdropped – into the Address. The Service Token will contain a hyperlink (the Service Hyperlink) to a website created by [Plaintiff's attorneys], wherein Plaintiff's attorneys shall publish this Order to Show Cause and all papers upon which it is based. The Service Hyperlink will include a mechanism to track when a person clicks on the Service Hyperlink. Such service shall constitute good and sufficient service for the purposes of jurisdiction under NY law on the person or persons controlling the Address (the "Service Order)"."*

Discussion

Due to its virtual nature and its antiestablishment underpinnings, the crypto space is replete with entirely anonymous actors. Often in cases of theft or fraud involving asset transfer, the only identifier is the wallet address of the receiving entity. This creates significant problems in serving these anonymous defendants with court papers in a way that grounds a court's jurisdiction. The Service Order is a proactive and innovative solution to this problem.

'Airdropping' is a process by which a digital token is sent to a wallet address. The controller of the wallet address cannot block the airdrop. In this way, an anonymous defendant can receive notice of court proceedings, whether they like it or not.

In the Dubai International Financial Centre (DIFC) Courts (and other common law courts with similar rules), one potential hurdle is that, for a court to order service by alternative means, the court must be satisfied that the alterative means will bring the documents to the receiving party's attention. The Service Token here was a hyperlink to a website, and it is the website which stores the documents to be served. If the controller of the wallet never clicks the link, have the documents been brought to their attention? Is service effective in that scenario? This issue is particularly acute in the tech-savvy crypto space, where many avoid clicking on links whatsoever in fear of hacking and theft of their virtual assets.

In order to circumvent this problem, a plaintiff may consider converting digital scans of the court papers into non-fungible tokens ("NFTs") and airdropping the NFTs themselves.

Arguably, this method means that the court papers have been actually received at the address, and not merely linked. Evidence that the wallet is in frequent use would also be helpful.

Overall, the Supreme Court for the State of New York should be commended for tackling what is a difficult issue head-on and seeking to evolve means of service to match the technology. We expect to see similar applications for permission to serve via airdropped tokens in jurisdictions the world over.

akingump.com