# 'NFT-y' service: service of process via NFT

**Kayla Joyce**
*Holland and Knight*

**Andrew Balthazor**
*Holland and Knight*

**Jose Casal**
*Holland and Knight*

This article considers a recent decision by the New York Supreme Court to permit the use of an NFT to anonymous defendants on notice of suit. It argues this will be a key mechanism for serving anonymous and evasive defendants in the blockchain space in future.

## Introduction

Many industries have been exploring blockchain technology-based solutions for streamlining business processes and developing trust between parties with little or no knowledge of each other.

Recently, the Supreme Court of the State of New York permitted Liechtenstein-based cryptocurrency exchange LCX to use a non-fungible token (NFT) on the Ethereum blockchain to put the anonymous defendants on notice of the suit.

Given the marked increase in cryptocurrency theft since 2020,[1] the order is a noteworthy example of a court embracing new technology to overcome a key legal barrier in the blockchain space due to its anonymous nature.

## The LCX hack

On 8 January 2022, an anonymous defendant or defendants hacked into the primary LCX Exchange wallet and transferred $7.94m worth of various crypto assets to an Ethereum blockchain address under the defendants' control.

LXC contracted with blockchain-tracing investigators to trace the stolen assets and identify the hackers. The investigators' tracing reports showed the defendants moved quickly to convert the stolen assets into ether (ETH). Virtually all of the ETH was then deposited into Tornado Cash, a popular mixing service often used to obfuscate stolen assets on the Ethereum blockchain.

While mixing services are designed to hide the digital trail of blockchain transactions and are often used for money laundering,[2] by using algorithmic forensic analysis the tracing specialists were able to identify the address receiving the proceeds of the LCX hack.

LCX has managed to track down and freeze about 60 per cent of the stolen funds, with investigations underway in Liechtenstein, Ireland, Spain and the United States.[3] Although the hackers' identities are unknown, pinpointing the address allowed LCX and law enforcement to trace the hackers' activities.

In March and May, whoever controlled the address swapped the ETH to US Dollar Coin (USDC), a stablecoin issued by Circle Internet Financial, with a registered office in New York. The hackers then sold 2.82m USDC in two large transactions. In June 2022, 1.3m USDC was sitting in the address.

USDC has a noteworthy feature: access denial. Specifically, Centre Consortium, the entity that governs the underlying technology for USDC, may deny access to addresses by blocking individual Ethereum addresses from sending and receiving USDC.

Holland & Knight appeared for LCX, led by Asset Recovery Chair Warren Gluck, associate Elliot Magruder, Virtual Asset and Blockchain associate Andrew Balthazor, and co-counsel Zach Bluestone of Bluestone Law.

LCX requested a preliminary injunction in New York, directing Centre Consortium to invoke its access denial policy to prevent the address from transacting in USDC. However, how to serve the anonymous defendants was not resolved until immediately prior to the hearing on LCX's motion.

## Notice by service token

Thirty minutes prior to the 2 June 2022 court hearing regarding LCX's argument on the motion for injunctive relief, the Holland & Knight team had an epiphany: the defendant relied on blockchain transactions to create a shield of anonymity—so why not use that same technology to pierce that shield?

At argument, LCX's counsel argued that service by token to the anonymous defendants' address would be appropriate in this context. After hearing the arguments, New York Supreme Court Justice Andrea Masley issued the requested temporary restraining order and ordered the unknown hackers to show cause why the court should not issue a preliminary injunction directing Centre Consortium to deny USDC access to the thieves' address.

Most significantly, the court approved of LCX's proposed service – airdropping a 'service token' that contained a hyperlink to a webpage with all the pertinent court documents:

> ORDERED that Holland & Knight LLP, Plaintiff's attorneys, shall serve a copy of this Order to Show Cause, together with a copy of the papers upon which it is based, on or before June 8, 2022, upon 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 Holland & Knight LLP, 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[.][4]

On 6 June, Joe Dewey, Chair of Holland & Knight's Virtual Asset and Blockchain team, created a smart contract to mint the service token, embedding in the token a hyperlink to the website hosting the service documents, and then airdropped the token to the wallet address controlled by the defendants.[5]

Airdropping is a process by which a digital token is sent to a blockchain address. The owner of an address cannot block the airdrop; the anonymous defendants would receive notice of the court proceedings whether they liked it or not. This method of service effectively tokenised court documents into an NFT, circumventing the problem of serving defendants where the identity and residence of the party controlling the address are unknown.

On 15 June, attorneys representing the 'Doe' defendant(s) filed a notice of appearance with the court.[6] They subsequently filed opposition papers, asserting that LCX failed to properly serve the order and refused to disclose the names or any identifying information about the defendants. According to the defendants, the court wrongly authorised alternative service because LCX did not make a showing of impracticability under the New York Civil Practice Law and Rules and did not demonstrate that the method was reasonably calculated to provide the anonymous defendants with notice.

## 'Good and sufficient' service

The primary objective of service of process is to notify defendants of a claim being made against them so that the parties may appear and be heard to defend themselves in court. The service NFT was apparently successful in providing this requisite notice, given that the attorneys filed appearances on behalf of the anonymous defendant(s).

Typically, service of process requires personally serving the other side with physical copies of the court papers. Of course, the law acknowledges that sometimes personal service may be impractical. In New York, a court has broad discretion to formulate an alternative method of service to be used in lieu of other methods when personal service is impracticable. For example, courts have approved service by email for a difficult-to-locate defendant,[7] service by Amazon's Message Center on a defendant whose address was unknown,[8] service by Facebook messenger to an account known to be used by the defendant,[9] and even service via Twitter and WhatsApp.[10] Service under other methods is often impracticable when the defendant cannot be found or the defendant's address cannot be ascertained. While the term 'impracticable' is not easily defined, courts will evaluate the circumstances of the particular case to determine the meaning of 'impracticable'.[11]

In fashioning a method of service, the court is constrained by due process, which requires that the method of service be 'reasonably calculated' under all the circumstances to apprise the defendant of the pending lawsuit. At the same time, due process does not require that the method of service guarantee actual notice to the defendant. Courts will also consider which alternative method will most likely give the defendant notice under the particular circumstances.

In an oral hearing on 22 July, the court affirmed that service by NFT was appropriate in this case. A written order is currently pending, but Judge Masley's bench order was clear on this point. Conventional methods of service of process require a name and physical address. LCX had no identifiable information that could be used to serve the defendants. The only known fact about these unknown hackers is that they transferred a portion of the LCX hack proceeds into the identified address.

Moreover, the hackers employed deliberate countermeasures to further obfuscate their identity, such as using the Tornado Cash mixing service. It was therefore impracticable to serve the defendants using conventional means. Notably, while the service token included the functionality to see if the embedded hyperlink was clicked, the court's order did not require actual proof that the defendant had accessed the court documents.

It was also clear that the service NFT delivered to the blockchain address would be the most effective way to reach the defendant. The anonymous defendants were in control of that blockchain address, which contained highly valuable assets, making it likely that the defendants would be returning to and using the address regularly. Indeed, 24 hours before LXC filed the complaint in New York, the blockchain address showed the defendants were still conducting transactions.

The court accepted LCX's arguments that the service token was a proper method reasonably calculated to effect service because: (i) the token would be delivered to the very address holding the stolen assets; (ii) the address contained valuable quantities of digital assets, making it likely the defendant would return to the address; and (iii) the token contained a hyperlink to a website wherein the process and court's order would be published.

This targeted method of serving notice to an anonymous defendant was akin to service via email, Facebook messenger, or Twitter, which courts have increasingly permitted in the appropriate context. The service token is simply the most recent type of alternative service in the line of expanding electronic service.

## Asset freeze by smart contract

The 2 July order enjoined the anonymous defendants from transferring, selling, removing or conveying its assets, including USDC held in the address. The court also directed Centre Consortium – the entity that controls the underlying USDC smart contract – to deny the address access to transacting USDC.

The smart contract governing USDC on the Ethereum blockchain includes this access denial feature to better comply with sanctions, regulations, enforcement actions and court orders. Centre Consortium's invocation of the access denial policy effectively froze the USDC in the address *without needing control of the private key unlocking the address itself.*

This too was a novel approach. Asset recovery in the digital context faces unique obstacles when enforcing orders against anonymous defendants. Crypto thieves generally have exclusive control over assets in their custody via their private key. Accordingly, while courts have issued freeze orders with respect to stolen virtual assets, the ability to give practical effect to these orders is generally limited to enforcement via third parties.[12] Specifically, the only available avenue for relief would be to locate an entity with custody of the assets and serve an asset freeze order on that entity, like a cryptocurrency exchange.

Here, however, LCX was able to identify specific assets held in the address which had built-in software features that would provide a third-party – Centre Consortium – some measure of control over a portion of the proceeds of the theft.

## Conclusion

Soon after the New York court's novel service-by-token order, a judge in London approved the use of a service NFT to put an anonymous defendant on notice of the lawsuit. In an interim relief hearing on 24 June, High Court Judge William Trower ruled that the plaintiff could airdrop the summons and complaints to the digital wallets controlled by the defendant who allegedly defrauded him.

Judge Trower reasoned that this alternative method to effect service was appropriate under the circumstances because '[t]he difficulties that would otherwise arise and the complexities in relation to service on the first defendant mean that good reason has been shown'.[13]

These cases are exciting developments for the legal profession. The service token will be a key mechanism for serving anonymous and evasive defendants in the blockchain space – a space replete with bad actors who have been able to shield their ill-gotten gains by utilising the blockchain's cloak of anonymity. Blockchain technology has the potential for broader application in the legal industry: creditor lien by token, perhaps?

**Note**

[1] Cryptocurrency theft increased by 516 per cent from 2020. See MacKenzie Sigalos, 'Crypto Scammers Took A Record $14 Billion in 2021' (CNBC, 6 January 2022) www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html.

[2] LCX Hack Update, 7 June 2022, www.lcx.com/lcx-hack-update.

[3] *Ibid.*

[4] *LCX AG v John Doe Nos 1–25*, Order to Show Cause and Temporary Restraining Order (Index No 154644/2022, Supreme Court of the State of New York, 2 June 2022).

[5] See *Affidavit of Josias N Dewey* (Index No 154644/2022, Supreme Court of the State of New York, 27 June 2022).

[6] *See Notice of Appearance* (Index No 154644/2022, Supreme Court of the State of New York, 15 June 2022).

[7] See, eg, *Snyder v Alternate Energy Inc*, 857 NYS2d 442, 448-449 (Civ Ct NY Cnty 2008).

[8] See, eg, *Noco Co, Inc v Zhejiang Quingyou Elec*, 338 FRD 100, 105-106 (ND Ohio 2021).

[9] See, eg, *ELVH Inc v Bennett*, No 18-cv-00710, US Dist LEXIS 236021, at *8, 2018 WL 6131947, at *3 (CD Cal, 2 May 2018).

[10] See, eg, *Rule of Law Soc'y v Dinggang*, Index No 156963/2022, 2022 WL 1104004, at *1 (Sup Ct NY Cnty, 8 April 2022).

[11] See *Safadjou v Mohammadi*, 105 AD3d 1423, 1424 (4th Dep't 2013) ('The meaning of "impracticable" will depend upon the facts and circumstances of the particular case').

[12] See, eg, *Astrove v Doe*, No 22-CV-80614, 2020 US Dist LEXIS 129286 (SD Fla, 22 April 2022) (ordering third-parties to freeze anonymous defendant's crypto assets); *Williams v Doe*, No 21-CV-03074-RK (WD Mo 23 April 2021), ECF No 47 (preliminary injunction entered

against John Doe defendant, ordering freeze of defendant's cryptocurrency assets); *SEC v Blockvest*, No 18-cv-2287, 2018 US Dist LEXIS 179424 (SD Cal, 5 October 2018) (ex parte ruling in SEC enforcement action freezing defendants' digital assets at financial institutions and coin exchanges and ordering third-parties to hold and not transfer those assets).

[13] Sarah Martinson, 'London Court OKs NFT To Serve Anonymous Defendant' (Law360, 12 July 2022) www.law360.com/articles/1510718/london-court-oks-nft-to-serve-anonymous-defendant.

**About the authors**

**Kayla Joyce** is a student at Fordham University School of Law in New York and was a summer associate at Holland & Knight New York City office. She can be contacted at **kjoyce14@fordham.edu**.

**Andrew Balthazor** is a Virtual Asset and Blockchain litigation associate at Holland & Knight's Miami office, with experience in virtual asset recovery and commercial litigation. He can be contacted at **andrew.balthazor@hklaw.com**.

**Jose Casal** is a Miami-based partner at Holland & Knight with a focus on international litigation, bankruptcy, creditors' rights, and blockchain-related matters. He can be contacted at **jose.casal@hklaw.com**.