DREW & NAPIER

DREWTECH SERIES

CHAPTER 10

Service by airdrop – no parachutes required

7 July 2022

LEGAL UPDATE

In this Update

In *LCX AG v John Does Nos. 1 – 25* (***LCX AG***), the Supreme Court of New York (***NY Court***) ordered service of court documents on unknown defendants via the "airdrop" of a "special-purpose Ethereum-based token" containing a hyperlink to court documents. In this article, we examine the facts and reasoning in *LCX AG* in closer detail, and discuss whether such a method of service would be allowed by a Singapore Court.

INTRODUCTION

On 8 January 2022, hackers broke into the primary digital asset wallet address held by LCX AG, a digital asset service provider incorporated in Liechtenstein. The hackers transferred approximately US$7.94 million worth of various digital assets into a mixing service via numerous transactions, before withdrawing and converting most of the stolen assets to the form of the cryptocurrency known as USD Coin (***USDC***). Mixing services disguise blockchain transactions by making it more difficult to ascertain the source of digital asset transfers. The USDC, which is based on the Ethereum blockchain, was eventually stored at a digital asset wallet address allegedly associated with the hackers.

The software rules on which USDC operates is governed by an entity named Centre Consortium, LLC (***CCL***) which has a presence in New York. As the protocol operator of USDC, CCL was able to prevent the hackers' digital asset wallet from sending and receiving USDC, and therefore freeze the stolen assets which were converted into USDC.

LCX AG filed a complaint in the NY Court against the unidentified hackers – as unknown defendants – to recover the stolen assets and obtained an order requiring the defendants to show cause as to why the NY Court should not issue a preliminary injunction directing CCL to block the hackers' wallet from sending and receiving USDC (***Order***), thereby preventing them from disposing the stolen assets therein.

In what appears to be the first case of its kind in any jurisdiction, LCX AG was permitted to serve the Order by "air-dropping" (i.e. the transfer of digital assets) into the hackers' digital asset wallet a special purpose Ethereum-based token (***Service Token***) containing a hyperlink to a website containing the court documents – this was understood to be the only viable way to transmit the relevant documents to the unknown defendants. The hyperlink contained in the Service Token had functionality which enabled LCX AG to see if the hyperlink was clicked (***Access Record***). This novel method of service effectively tokenized court documents into an NFT insofar as the Service Token was a token which was not replicable and provided access to the court documents.

WOULD THIS WORK IN SINGAPORE

The Singapore Courts have not been one to shy away from ensuring that Singapore law and procedural rules keep up with the times. Service of court documents has been allowed through email, Skype, Facebook, an internet message board, and WhatsApp. Would the Courts similarly permit service by NFT?

A. Service within Jurisdiction

The starting point when serving originating papers has always been personal service. Typically, where a natural person is concerned, this means providing said person a physical copy of the originating papers. While the Singapore Rules of Court have recently been transformed, this remains the case in the recent Rules of Court 2021 (***ROC 2021***) – see Order 6 rule 4 of *ROC 2021* read with Order 7 rule 2(1) of *ROC 2021.*

Of course, there may be times where it is impractical to effect personal service, for instance if the counterparty actively tries to evade personal service, or if the physical location of the counterparty is unknown (which would likely be the case where the identity of the counterparty is unknown, as was the case in *LCX AG*). In such circumstances, the law provides a party with the ability to apply for permission from the Court to effect service by other means that is effective in bringing the document to the notice of the person to be served. This is known as substituted service. To this end, Order 7 rule 7(2) of *ROC 2021* provides that the Court may order any method of substituted service, including *"the use of electronic means"*, which on its face is wide enough to encompass service by blockchain. However, the Court's practice directions provide that a party should attempt personal service twice before applying for substituted service.

On its face, it does appear the new Rules of Court read with the practice directions empower the Court to order service by NFT. However, while the Court can order service by NFT, would the Court do so? The *ROC 2021* and previous case law generally require that the Court must be satisfied that service by blockchain would *"in all reasonable probability"* be effective in bringing knowledge of the document to the counterparty. The Court has held that the applicant may thus be required to prove that the electronic platform that the applicant proposed to use for service is (1) used by the counterparty or (2) was recently used by the counterparty.

In a recent case involving the freezing of certain cryptocurrency assets which also involved substituted service on unknown persons (*CLM v CLN* [2022] SGHC 46), the Court allowed substituted service of the relevant originating papers by email. The claimant in *CLM v CLN* did not know where the respondents were located and only had their email addresses. However, there was evidence that the respondents' email addresses had been recently used, and throughout the dealings between the claimant and the respondents, the respondents had always used their email addresses. The Court was thus satisfied that serving the papers at the relevant email addresses would be effective in bringing notice to the respondents.

Let us consider the facts in *LCX AG*: (a) the claimant did not know how else to contact the respondents, (b) there was sufficient evidence that the respondents were associated with the relevant digital asset wallet address, and (c) there was evidence that the relevant wallet address had been recently used. Following the reasoning adopted by the Court in *CLM v CLN*, it is arguable that the Court would have, in similar circumstances, ordered substituted service by blockchain since:

(a) it would be impracticable for the claimant to effect personal service (since the claimant did not even know who the respondents were); and

(b) serving the documents at the relevant wallet address would arguably bring notice of the documents to the respondents insofar as there was evidence that the respondents were associated with the relevant wallet address.

Would the Court require proof that the hyperlink sent via the blockchain was actually accessed by the defendant? It is arguable that the Court would not require this before allowing substituted service by blockchain. The Court has accepted that the method of substituted service only needs *"in all reasonable probability"* to bring notice of the papers to the defendant. It has also accepted that, barring actual personal service through physical means, all forms of substituted service carry the risk of a document not actually being brought to the notice of the person being served. Thus, like in *CLM v CLN* where the Court allowed service by email and did not require, for instance, a read receipt of the said email, a link which records when the documents attached thereto had been accessed would arguably not be necessary. Notably, while the NY Court in *LCX AG* ordered that the Service Token shall include the Access Record functionality, the Order did not require that actual proof of access by the defendants be shown to constitute effective service of the Complaint documents.

B. Service out of Jurisdiction

What if the relevant documents are required to be served out of jurisdiction? This is an open question under the new Rules of Court that will require guidance from the Court in the future.

At the threshold level, there is no equivalent provision for substituted service which governs service out of jurisdiction in *ROC 2021* (there is no equivalent of Order 7 rule 7 in Order 8 of *ROC 2021*). This on its face is a departure from the previous edition of the Rules of Court 2014 (***ROC 2014***), which expressly provided that the provisions for substituted service therein would apply to service out of jurisdiction (Order 11 rule 3 of *ROC 2014*). Thus, insofar as there appears to be an express departure from the *ROC 2014*, it is arguable that this was deliberate drafting to remove the ability to effect substituted service out

of jurisdiction, and substituted service out of jurisdiction by blockchain is not permitted.

On the other hand, it could be argued that the ability to order substituted service out of jurisdiction has been subsumed into Order 8 rule 2(1)(f) of *ROC 2021*, which provides that service out of Singapore may be effected *"according to the manner provided by the law of that foreign country"*. Thus, insofar as the law of *"that foreign country"* permitted substituted service, then a claimant would be able to serve documents out of jurisdiction using substituted service by blockchain.

There may be other issues if, for instance, the claimant does not know where the respondents are located, but knows that the respondents are not in Singapore (so service out of jurisdiction will be required). Pursuant to Order 8 rule 2(6) of *ROC 2021*, *"[n]othing is to be done under this Rule that is contrary to the laws of the foreign country"*. A similar requirement was present in the previous Rules of Court (Order 11 rule 3(2) of *ROC 2014*).

Accordingly, if a particular country does not permit service by a particular method, then the claimant may not be allowed to use that method to serve the papers on the respondent, notwithstanding that such a method could have been permissible under Singapore law. If service was effected by a method contrary to the law of the jurisdiction in question, then the respondent would have grounds to challenge the validity of the service and argue that no valid service has been effected. If a respondent succeeded, then this may lead to delay as the claimant would then have to re-serve the papers. The risk for potential claimants hoping to serve originating papers out of jurisdiction on unknown respondents by blockchain would then be that the jurisdiction in which the respondents are located prohibits service by blockchain, and that such service would be liable to be set aside by the Court.

It may be that this issue may be more of an inconvenience rather than fatal in the grand scheme of the action (since, in challenging service, the respondent would have to disclose where it actually is located), but it could still result in the expenditure of additional time and costs in prosecuting the action insofar as service out of jurisdiction would have to be effected again. Notably, this appears to have not been relevant to the analysis in *LCX AG* insofar as pursuant to the New York Civil Practice Law and Rules (***CPLR***), the laws of the foreign jurisdiction do not appear to matter as long as the service is made pursuant to the relevant provision of the *CPLR* unless a treaty signed between the US and the foreign jurisdiction mandates some other service requirements.

CONCLUSION

LCX AG represents a novel use of digital assets in the court process. On its face, the *ROC 2021* would appear to empower the Court to permit service of process by NFT, but the exercise of the Court's discretion to make such an order remains an open question.

UPDATES IN DREWTECH SERIES

1. Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>
2. Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>
3. Chapter 3: I host, you post, I get sued? <24 September 2019>
4. Chapter 4: Diabolus ex machina <18 February 2020>
5. Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>
6. Chapter 6: Signing without signing – contactless contracts <16 July 2020>
7. Chapter 7: My Kingdom for a Horse – When your Systems are Held to Ransom <22 January 2021>
8. Chapter 8: New risks in new skins – Updates to the Guidelines on Risk Management Practices – Technology Risk <3 March 2021>
9. Chapter 9: Of blockchains and stumbling blocks <21 July 2021>
10. Chapter 10: Service by airdrop – no parachutes required <7 July 2022>

If you have any questions or comments on this article, please contact:

Rakesh Kirpalani
Director, Dispute Resolution & Information Technology
Chief Technology Officer
T: +65 6531 2521
E: rakesh.kirpalani@drewnapier.com

Chua Tju Liang
Director
Head, Blockchain & Digital Assets
T: +65 6531 4101
E: tjuliang.chua@drewnapier.com

DREW & NAPIER

Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906