IN THE EASTERN CARIBBEAN SUPREME COURT
IN THE HIGH COURT OF JUSTICE
BRITISH VIRGIN ISLANDS
(COMMERCIAL DIVISION)

Claim No: BVIHC (COM) 2022/0031

BETWEEN:

CHAINSWAP LIMITED

CLAIMANT

AND

(1) THE OWNER OF DIGITAL WALLET 0X941A9E3B91E1CC015702B897C512D265FAE88A9
(2) THE OWNER OF DIGITAL WALLET 0XEDA5066780DE29D00DFB54581A707EF6F52D8113
(3) THE OWNER OF DIGITAL WALLET 0XB63F0D8B9AA0C4E68D5630F54BFEFC6CF2C2AD19
(4) THE OWNER OF DIGITAL WALLET 0X196593ADE7CC7EDF18981C7A7DBC2E96000004FB
(5) THE OWNER OF EMAIL ADDRESS: TRUMANBROUGHTON@GMAIL.COM
(6) OTHER PERSONS UNKNOWN

DEFENDANTS

Appearances:

Mr. Christopher Pease and Ms. Megan Elms of Harneys for the Claimant
The Defendants did not appear nor were they represented

2022 March 15
May 4

JUDGMENT

[1] **JACK J [Ag]:** I heard this matter on 15th March 2022, when I continued a freezing injunction, which I originally granted *ex parte* on 17th February 2022. At the end of

the hearing, Mr. Pease appearing for the applicant ("ChainSwap") asked whether I would give a written judgment in light of the novel aspects raised on the application. Harneys have helpfully prepared a note, which I am happy to use as the basis for this judgment.

[2] The background is that by an application dated 14th February 2022 ChainSwap sought, inter alia: (i) a worldwide freezing order against persons unknown, being those allegedly responsible for cybercrime consisting of the theft of digital assets; (ii) permission to serve its claim on the persons unknown out of the jurisdiction and by alternative means; and (iii) a letter of request to be issued by this court to the Croatian authorities seeking the provision of evidence from a cryptocurrency exchange located in Croatia, including information that will identify the unknown defendant or defendants.

[3] Following an *ex parte* hearing on 17th February 2022, I granted the relief sought by ChainSwap. Originally ChainSwap sought to sue "persons unknown" identified merely by their involvement in the theft of the cryptocurrency. This did not seem to me to be appropriate: **Cameron v Liverpool Victoria Insurance Co Ltd**.[1] I directed that the defendants be identified by reference to their ownership of the "wallets" that are alleged to have been used by the defendants to receive and dissipate stolen tokens.[2]

[4] An application to continue the worldwide freezing order came back before me on 15th March 2022. Notice of that application was given to the respondents in accordance with the alternative service which I permitted outside the jurisdiction. However, the respondents did not appear at that hearing. I continued the injunction on the following grounds.

[1] [2019] UKSC 6, [2019] 1 WLR 1471 at [13].
[2] Since making my decision, Jackson J sitting in the Queen's Bench Division in England has permitted a claim to be brought against "persons unknown" simpliciter, but his judgment is sealed, so his reasoning is unclear: Ward Hadaway LLP v Persons Unknown (unreported 26th April 2022), no neutral citation number, WestLaw citation [2022] 4 WLUK 217. In that case, hackers were holding the files of the claimant solicitors to ransom.

[5] ChainSwap is a company incorporated in the British Virgin Islands. ChainSwap provides a service that allows cryptocurrency tokens to be transferred between different blockchains, known as a cross-chain bridge. ChainSwap facilitates the transfer of tokens between blockchains via a smart contract, which is essentially a computer programme that operates on a blockchain according to a set of pre-determined rules. ChainSwap's bridges redirect tokens that are sent to its contract addresses into a specific wallet that acts as a vault ("the vault wallet"). Once the smart contract registers the receipt of assets into the vault wallet it automatically instructs new tokens of the equivalent type and value to be "minted" or created on the second blockchain to which the user has requested their tokens be transferred. Whilst it appears as though the bridge transfers tokens between two blockchains, in reality the original token is locked away and disabled in the vault wallet and a new token (that represents the old token) is created for use on the new blockchain. The smart contract keeps a tally of disabled tokens and newly minted tokens to ensure each correspond.

[6] In July 2021, unknown hackers were able, without authorisation, to exploit vulnerabilities in ChainSwap's computer programmes and amended the open-source code on which ChainSwap's bridge operates. This happened on two separate occasions, approximately one week apart. On the first occasion, hackers altered the code to the bridge smart contract so that all tokens transferred to the bridge were re-directed to a private digital wallet owned by the hackers rather than going to the vault wallet. In addition, the hackers were able to exploit the fact that numerous users of the bridge had pre-authorised their digital wallets to transfer unlimited tokens to the bridge, which allowed the hackers to "request" that tokens held in those wallets be transferred to the bridge smart contract, whereupon they would be redirected to the hackers' private digital wallet.

[7] On the second occasion, hackers altered the code to the bridge smart contract that regulated the number of tokens that could be minted on the new blockchain, which would normally be restricted to the number of tokens received into the vault wallet. The quota code was removed, which meant that unlimited new tokens could be

issued without the need for any tokens at all to be received into the vault wallet. The newly minted tokens were directed into private digital wallets belonging to the hackers.

[8] The consequence of the hacks carried out against ChainSwap's cross-chain bridge was that hackers were able to misappropriate assets from: (i) private users that had authorised their wallets to interact with the bridge (pursuant to the first hack); and (ii) projects issuing digital tokens that had used the bridge to offer cross-chain operability on their tokens (pursuant to the second hack).

[9] Tokens taken during the attacks were received into two separate digital wallets. Some of the misappropriated assets were then traded and exchanged for different cryptocurrency tokens, including tokens that are pegged to mainstream fiat currencies, such as the US dollar (known as "stablecoins"). Quantities of tokens with substantial value were subsequently transferred from these two wallets, some routed via a third wallet, to Tornado Cash, which describes itself as a fully decentralised protocol for private transactions.

[10] Tornado Cash uses smart contracts to receive tokens which it will hold for a period of time and then, at the discretion of the user, transfer out to a different wallet than that from which the transfer was originally made. Where numerous users transfer tokens into Tornado Cash at the same time, it can have the effect of mixing those tokens so that when paid out into different wallets, it will obfuscate their origin.

[11] ChainSwap engaged the BVI firm, Kalo Advisors, to identify whether the transfers of tokens from the three wallets used by the hackers could be matched to any assets transferred out of the Tornado Cash smart contract. Kalo identified that:

(a) In total, there were twenty-four transfers each of 100,000 DAI from the three wallets to Tornado Cash between 16:45 and 22:35 (GMT) on 5th September 2021. (A DAI is a stablecoin worth US$1.00 per DAI.);

(b) Less than 24 hours later, between 14:46 and 15:42 (GMT) on 6th September 2021 Tornado Cash made twenty-four transfers of just under 100,000 DAI to a different (fourth) wallet; and

(c) Tornado Cash directed a small amount of the tokens being transferred to a relay wallet, which essentially takes a small commission as payment for the service. This would account for why the payments out were slightly under 100,000 DAI each.

[12] Kalo's report concluded that it is more likely than not, given the number and size of payments in and out of Tornado Cash and the relatively short time between transfers in and out, that the twenty four transfers from the three hacker wallets are linked to the twenty four transfers made to the fourth wallet. In my judgment ChainSwap has established a good arguable case that this fourth wallet, the wallet that received the tokens from Tornado Cash, was owned or associated with the hackers for the purposes of the application before me.

[13] ChainSwap has identified that the fourth wallet interacted with a centralised cryptocurrency exchange located in Croatia called Electrocoin d.o.o., which by its terms of service, should hold "know your client" information relating to the owner of the fourth wallet, including the owners' name and address. I accordingly signed a letter of request addressed to the Croatian Courts.

[14] The tokens that were misappropriated following the hacking incidents were not owned by ChainSwap. However, ChainSwap claims that the actions taken by the hackers have damaged its reputation and caused it to suffer loss, including loss of income due to confidence in the security of the cross-chain bridges being undermined. In order to mitigate the damage to its reputation, ChainSwap compensated the users and projects affected by the hacks. ChainSwap says that the amount of compensation paid is the minimum amount of loss it has suffered. In my judgment ChainSwap showed a good arguable case that they had a claim for that sum.

[15] Although the application to continue the worldwide freezing order was made on notice to the respondents and served in accordance with the alternative service provisions of the ex parte order, the respondents have so far not made an appearance in these proceedings and the application before me therefore remains uncontested.

[16] ChainSwap did not seek a proprietary injunction, since it was not asserting a proprietary right in the digital assets. Had ChainSwap been able to establish an arguable case that the stolen tokens were its property then that is a form of relief which this Court would have been able to grant. Cryptocurrencies are a form of property: **Philip Smith and Jason Kardachi (in their capacity as joint liquidators) v Torque Group Holdings Ltd**.[3] However, there is no difficulty in my judgment in granting a freezing order on the usual test for those orders: **The Niedersachsen**.[4] There is an obvious risk of dissipation if no freezing order is granted.

Adrian Jack
Commercial Court Judge [Ag.]

By the Court

Registrar

[3] [2021] ECSCJ No 627 (Wallbank J), applying AA v Persons Unknown; Re Bitcoin [2019] EWHC 3556 (Comm), [2020] 4 WLR 35.
[4] Ninemia Maritime Corporation v Trave Schiffahrtsgesellschaft mbH & Co KG (The Niedersachsen) [1983] 1 WLR 1412 (Court of Appeal); and [1984] 1 All ER 398 (Mustill J at p 400 and the Court of Appeal at p 415).