MAPLES GROUP

UPDATE

ChainSwap: BVI Court Injuncts Assets of Unidentified Owners of Crypto Wallets

In a first for the territory, the British Virgin Islands ("BVI") Commercial Court has granted a worldwide freezing order against persons unknown, being those allegedly responsible for cybercrime consisting of the theft of digital assets. At the same time, the applicant was granted: (a) permission to serve its claim on the persons unknown out of the jurisdiction and by alternative means; and (b) a letter of request to be issued from the BVI court to the Croatian authorities seeking the provision of evidence from a crypto exchange in Croatia, including information that is highly likely to identify the unknown defendant(s).

Background

The background is neatly set out in the judgment and the key parts of that background are replicated below in summary fashion.

The applicant, Chainswap Limited ("ChainSwap"), is a company incorporated in the BVI. It 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. Its bridges redirect tokens that are sent to its contract addresses into a specific wallet that acts as a vault.

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 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 ChainSwap's vault wallet. 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.

Tokens that were taken during the cyberattacks 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').

ChainSwap, with the help of forensic professionals at Kalo Advisors, undertook a tracing exercise and as a result they were able to identify specific transactions and wallets which,

on balance, are likely to have been used by the unknown hackers for the onward flow of the misappropriated funds. One such wallet identified by ChainSwap is thought to have 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 (KYC) information relating to the owner(s) of the wallet in question, including information pertaining to name(s) and address(es).

The Judgment

The judge held that ChainSwap had established a good arguable case that the index wallet was owned or associated with the hackers. Accordingly, the court granted the relief sought, including the issuance of a letter of request to the Croatian courts which is intended to lift the veil of anonymity enjoyed thus far by the hackers.

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. In order to mitigate the reputational damage, ChainSwap compensated the users and projects affects by the hacks, which sums it now seeks to be compensated for. The court found that it had a good arguable case and claim for recovery of those sums.

Comment

This judgment highlights that the BVI court is readily prepared to grant injunctive remedies to hold alleged perpetrators of cybercrime to account, unperturbed by the aliases or anonymity behind which such perpetrators routinely sit.

The jurisprudence in this area continues to develop at an increasing rate, and the BVI is fast establishing itself as a jurisdiction firmly at the forefront of those developments.
For further information, please reach out to your usual Maples Group contact or any of the persons listed below.

British Virgin Islands

Adrian Francis
+1 284 852 3016
adrian.francis@maples.com

Matthew Freeman
+1 284 852 3011
matthew.freeman@maples.com

Scott Tolliss
+1 284 852 3048
scott.tolliss@maples.com

May 2022