Common law remedies for an Evolving World - How the Court can help you recover your Misappropriated Cryptoassets

Singapore has fast emerged as one of the leading jurisdictions for technology innovation and has recently welcomed web 3.0 companies, including those whose businesses focus on cryptoassets and blockchain technologies, to set up shop in the city state. This is part of a growing trend as economies seek a slice of the exponentially growing crypto industry pie. However, with its increase in profile and rise in value, cryptocurrencies are now a very attractive target for malicious actors, including those who might misappropriate cryptocurrencies by hack, cyber fraud or other criminal wrong doing.

GET IN TOUCH
View Nicola Roberts's LinkedIn Profile
View Jayesh Chatlani's LinkedIn Profile
Find out more about Harneys

BY:
NICOLA ROBERTS
Partner and Head of Litigation, Insolvency and Restructuring in Singapore, Harneys

JAYESH CHATLANI
Counsel in Singapore, Harneys

The common law courts have had to tackle this issue, and there is an increasing body of industry professionals, including lawyers and forensic analysists who can assist in identifying malicious actors, tracking down cryptocurrencies and recovering them through the civil courts. Each case must be taken on a case by case basis, and the options available will invariably vary if a fraud has taken place, between two private individuals transacting through their own wallet addresses as opposed to a hack on an exchange which may have required a malicious actor to 'onboard' on an exchange and provide requisite know-your-customer and identifying information.

For any misappropriation of funds involving cryptoassets, an important first step is to review the blockchain ledgers relating to the fraudulent transactions in order to track the assets across different wallets and blockchains. Once the wallet address(es) to which misappropriated crypto funds have been transferred have been identified, common law courts will usually grant an injunction in respect of those assets. Common law courts have regularly treated cryptoassets as property and therefore have been willing to grant propriety relief. This was the position taken in *Vorotyntseva v Money-4 Ltd (t/a Nebeus.com)* [2018] EWHC 2596 (Ch) and upheld in *AA v Persons Unknown* [2019] EWHC 3556. Helpfully this means that common law courts will usually make a declaration that the misappropriated assets are the property of the claimant, and this is often helpful in pursuing further action against the victims once identified.

In order to obtain an injunction, a claimant will need to satisfy the usual American Cyanamid test and demonstrate that there is a risk of dissipation, there is a serious issue to be tried, that damages are not an adequate remedy and that the balance of convenience favours the granting of an injunction. In the typical context of a fraud case involving cryptocurrencies this will likely be met, and the common law courts have been willing to grant orders in this regard against 'persons unknown', acknowledging the difficulty in identifying the wrongdoers, particularly at the early stages of proceedings.

NICOLA ROBERTS
Harneys

In practice, a large amount of misappropriated funds make their way towards cryptocurrency exchanges or custodians as malicious actors seek to off-ramp their cryptoassets to fiat currencies. Cryptocurrency exchanges and custodians are very accustomed to this, and almost all cryptocurrency exchanges will disable the functionality of offending accounts if they are in receipt of misappropriated assets, effectively freezing them in place. Just as crucially, most crypto exchanges and custodians will have sophisticated know-your-client information regarding the controller of the wallet, and can be compelled to provide that information by way of third party disclosure orders, including orders for Norwich Pharmacal relief, bankers trust orders or similar relief. This provides a means to identify wrongdoers, including their jurisdiction in order to pursue related legal action in those jurisdictions, as well as to seek further disclosure orders to trace the assets.

In the case of misappropriated assets that do not end up in a cryptocurrency exchange or custodian, it is prudent that those wallets be monitored for suspicious activity (such as laundering the assets through a cryptocurrency laundering service such as tornado cash). Such activities are often preliminary steps towards a malicious actor seeking to convert the funds into 'clean' cryptocurrencies or fiat. In any event notice of the illegal funds or misappropriation should be given

to major cryptocurrency exchanges and custodians to ensure that malicious actors are brought to justice in the event they seek to benefit from the misappropriated funds. Indeed, it was a continuous monitoring of stolen assets that eventually led to the recent arrest (in 2022) of the perpetrators of the 2016 Bitfinex hack.

The authors of this article have successfully represented victims of hacking and other malicious actions in recovering cryptoassets in the courts of the British Virgin Islands and the Cayman Islands and have cooperated with counsel in a number of jurisdictions, including England, Singapore, Hong Kong, Egypt, Morocco and South Korea to recover stolen cryptocurrencies.

Should you have any questions or would like to discuss further please contact the authors
Nicola Roberts: nicola.roberts@harneys.com
Jayesh Chatlani: jayesh.chatlani@harneys.com

JAYESH CHATLANI
Harneys