Published on 12 November 2020

ASSET-TRACING TOOLS FOR CRYPTOCURRENCY HACKS

[2020] SAL Prac 22

Cryptocurrency hacks have recently become more commonplace. To be able to maximise recovery of the stolen cryptocurrency, plaintiffs must have access to tools that will help them effectively trace and preserve the stolen cryptocurrency. This article outlines the court-based tools available in Singapore to plaintiffs in gathering information and maintaining the status quo to prevent further dissipation of cryptocurrency after the initial hack.

Danny **QUAH**
LLB (National University of Singapore);
Advocate and Solicitor (Singapore);
Counsel, *Providence Law Asia LLC.*

I. Introduction

1 Since the advent of Bitcoin in 2009, over $1.74bn worth of cryptocurrency have been hacked and stolen from cryptocurrency exchanges.[1] Some exchanges manage to recover from the hacks and continue operations. However, there are some reputable cryptocurrency exchanges such as the UK's Cubits[2] and New Zealand's Cryptopia[3] which have been forced into insolvency as a result of the hacks.

2 This article explores the court-based tools available to Singapore lawyers who are assisting plaintiffs affected by the

1 Ledger Academy, "Hacks Timeline" <https://www.ledger.com/academy/crypto/hacks-timeline> (accessed 27 October 2020).
2 William Suberg, "Crypto Platform Cubits Begins Insolvency Procedure After Alleged Hack, Locks Users' Funds" *Cointelegraph.com* (12 December 2018).
3 Yogita Khatri, "Hacked Crypto Exchange Cryptopia Files for US Bankruptcy Protection" *coindesk* (27 May 2019).

hack to recover proceeds of the hack. Due to the unique nature and characteristics of cryptocurrency, this article will also address the challenges and limitations of the court tools in freezing cryptocurrency and/or obtaining information on any fraudulent transfers of cryptocurrency arising from the hack.

II. Asset recovery tools

3 There are three main court-based tools that plaintiffs can potentially use to freeze the proceeds of a cryptocurrency hack and/or obtain information on where the cryptocurrency has been dissipated to:

(a) a Mareva injunction coupled with the requisite ancillary disclosure orders under Order 29 rule 1 of the Rules of Court,[4] followed by an application to cross-examine the defendants for any failure to comply with their disclosure obligations under the ancillary disclosure orders;

(b) an application seeking pre-action discovery under Order 24 rule 6 of the Rules of Court; and

(c) an application seeking pre-action interrogatories under Order 29A rule 1 of the Rules of Court (otherwise more conventionally known as a *Norwich Pharmacal* order).

A. The Mareva injunction with ancillary disclosure orders

4 First, plaintiffs should consider applying for a Mareva injunction to prevent the defendant from "dissipating his assets and thus rendering nugatory a judgment which might eventually be obtained by a plaintiff against him".[5]

5 While the Singapore courts have yet to affirmatively determine that cryptocurrency can be the subject of a Mareva injunction, it is likely that they will have no issue doing so.

4 Cap 322, R 5, 2014 Rev Ed.
5 *Sea Trucks Offshore Ltd v Roomans, Jacobus Johannes* [2019] 3 SLR 836 at [45].

6 In the Singapore International Commercial Court decision of *B2C2 Ltd v Quoine Pte Ltd*,[6] International Judge Simon Thorley ("Thorley IJ") had no difficulty accepting that cryptocurrency could be treated as property in the general sense, for the purposes of determining whether cryptocurrency could be an asset that could be subject to a trust.[7] Thorley IJ observed that cryptocurrencies were not legal tender in the sense of being a regulated currency issued by a government but have the fundamental characteristic of intangible property as being an identifiable thing of value.

7 This aspect of Thorley IJ's decision was challenged on appeal in *Quoine Pte Ltd v B2C2 Ltd*.[8] However, the Court of Appeal found that it was not necessary to decide on this question on the facts of the case as the court was satisfied that the plaintiff's breach of trust claim would fail because there was no certainty of intention to create a trust.[9] As such, Thorley IJ's exposition of cryptocurrency being property remains intact.

8 Further, the Singapore courts may take guidance from foreign judgments which have not found any difficulty in granting injunctions over cryptocurrency. For example:

(a) In *AA v Persons Unknown*,[10] the English High Court granted an interim proprietary injunction against a cryptocurrency exchange over Bitcoin which represented proceeds of ransom moneys paid out to a hacker by the plaintiff. The hackers had installed malware into the plaintiff's computer system and demanded that the plaintiff pay a ransom in Bitcoin to regain access to its system. The ransom was paid in Bitcoin and transferred to the exchange.

(b) In *Vorotyntseva v Money-4 Ltd*,[11] the English High Court granted an *ex parte* proprietary freezing order over some Bitcoin and Ethereum currency, stating

6 [2019] 4 SLR 17.
7 *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17 at [142].
8 *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20 at [138].
9 *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20 at [144].
10 [2019] EWHC 3556 at [57]–[59].
11 [2018] EWHC 2596 (Ch) at [13].

that the defendant in that case had not suggested that cryptocurrency cannot be a form of property.

(c) In *Shair.Com Global Digital Services Ltd v Arnold*,[12] the Supreme Court of British Columbia (Canada) granted an *ex parte* preservation order to the plaintiff against its former chief operating officer with respect to cryptocurrency that might still be in his possession. The court accepted that cryptocurrency could be property within the rules for preservation orders, noting that the defendant had not denied that the plaintiff had an interest to pursue the preservation order.

9 Plaintiffs should also take note of the "ordinary adjunct" of the ancillary disclosure order which accompanies a Mareva injunction.[13] This ancillary order has not been the subject of much legal jurisprudence in Singapore. However, used appropriately, this can be a very powerful tool in obtaining much-needed information on the whereabouts of the hacked cryptocurrency so that appropriate steps can be taken to preserve them pending trial.[14]

10 A Mareva injunction does not give a plaintiff security or a proprietary interest over the defendant's assets, but simply restrains the said assets from being moved. Because the plaintiff is given no interest, security or priority in any of the assets, the only way to allow the plaintiff to effectively police the Mareva injunction is by giving him sufficient information about the location and details of the defendant's assets, so that he can determine whether the defendant has been moving his assets in breach of the Mareva injunction.[15]

11 The ancillary disclosure order is in standard form and is contained in paragraph 2 of Form 7 of Appendix A of the Supreme Court Practice Directions. The standard form requires the defendant to disclose *all* of his assets, "even though the substantive terms of

12 [2018] BCSC 1512.
13 *Sea Trucks Offshore Ltd v Roomans, Jacobus Johannes* [2019] 3 SLR 836 at [45].
14 *Petromar Energy Resources Pte Ltd v Glencore International AG* [1999] 1 SLR(R) 115 at [21].
15 *Sea Trucks Offshore Ltd v Roomans, Jacobus Johannes* [2019] 3 SLR 836 at [45].

the Mareva injunction in the same standard form only restrain the assets of the defendant up to the sum that is reasonably claimed by the plaintiff in the underlying proceedings".[16] As such, the Singapore High Court has recognised that it is a general rule that a defendant will be required to "make disclosure of *all* his assets even though the assets restrained are limited to those of a certain value" [emphasis added].[17]

12 If the plaintiff is having difficulty getting the defendant to comply with the ancillary disclosure order – for example, if the defendant files a "holding affidavit" or an affidavit that omits significant or crucial information – the plaintiff can consider applying to cross-examine the defendant on his affidavits.[18] In this regard, the plaintiff will need to show that, in all the circumstances, it is just and convenient to make the order for cross-examination, subject to the caveat that the application should not be abused to extract material on which to build the plaintiff's case for the main action.[19]

13 That being said, it should be noted that there are limits to an ancillary disclosure order. The disclosed information does not provide a longitudinal view of the defendant's assets. All that is disclosed are the assets standing to the defendant's name at the time disclosure is made.[20] The information will not show whether there has been a systematic and unexplained attrition of the defendant's assets over time and is often "rough and ready".[21]

B. Pre-action discovery

14 Second, if the hacked cryptocurrency can be traced to have been transferred to another cryptocurrency exchange, the

16 *Sea Trucks Offshore Ltd v Roomans, Jacobus Johannes* [2019] 3 SLR 836 at [52].
17 *Sea Trucks Offshore Ltd v Roomans, Jacobus Johannes* [2019] 3 SLR 836 at [52].
18 *Sea Trucks Offshore Ltd v Roomans, Jacobus Johannes* [2019] 3 SLR 836 at [61]; *Bouvier, Yves Charles Edgar v Accent Delight International Ltd* [2015] 5 SLR 558 at [105].
19 *OCM Opportunities Fund II, LP v Burhan Uray* [2004] 4 SLR(R) 74 at [34]–[35].
20 *Bouvier, Yves Charles Edgar v Accent Delight International Ltd* [2015] 5 SLR 558 at [103].
21 *Bouvier, Yves Charles Edgar v Accent Delight International Ltd* [2015] 5 SLR 558 at [103].

plaintiff should consider applying for pre-action discovery against the recipient exchange. Such pre-action discovery could include disclosure of the following documents:

(a) Know Your Customer ("KYC") documents such as account opening forms and other related documents submitted for the purpose of opening the said account;

(b) transaction statements in respect of those accounts which set out all transfers into and/or from the accounts; and

(c) payment instructions relating to the transfers above.

15 KYC documents may be particularly useful in the context of seeking disclosure from cryptocurrency exchanges as, in Singapore, cryptocurrency exchanges are likely to be regulated under the Payment Services Act 2019[22] ("Payment Service Providers").

16 In this regard, Payment Service Providers are obliged to obtain the following information from their customers as part of their Customer Due Diligence ("CDD"):[23]

(a) full name, including any aliases;

(b) unique identification number;

(c) residential address or registered/business address;

(d) date of birth, establishment, incorporation or registration; and

(e) nationality, place of incorporation or place of registration.

17 Payment Service Providers are also obliged to conduct independent verification of the identity of the customer using "reliable, independent source data, documents or information",[24]

22 Act 2 of 2019.

23 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services)" (5 December 2019) at para 7.6.

24 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of

(cont'd on the next page)

and inquire if there exists any beneficial owner(s) of the corporate customer or if the customer is acting on behalf of another.[25]

18 In the premises, there is potentially a wealth of information that would assist a plaintiff in seeking to trace the whereabouts of the hacked cryptocurrency and the potential recipients of the hacked cryptocurrency.

19 It is, however, not easy to apply for pre-action disclosure. As the Court of Appeal noted in *Dorsey James Michael v World Sport Group Pte Ltd*[26] ("*Dorsey*"), "pre-action disclosure, while not exceptional, is not usual".[27] The Court of Appeal noted that a court should not make an order if it has not been provided with sufficient information to adequately assess the necessity of disclosure. Reasons ought to be given why it is neither convenient nor just for that information to be sought after proceedings have been commenced against an already identifiable party. Ordinarily, the court is always placed in a better position in matters where proceedings have already been commenced as it can then additionally examine the pleadings of all the parties to assess the merits of an application.[28]

20 That said, on the appropriate occasion (in particular where a cryptocurrency hack is clearly involved), a plaintiff should consider applying for pre-action disclosure. To do so, the plaintiff will need to satisfy three requirements:[29]

> (a) First, the person from whom discovery is sought must have had been involved in the wrongdoing, even if the involvement may be completely innocent.

Payment Services Licence (Specified Payment Services)" (5 December 2019) at para 7.9.

25 Monetary Authority of Singapore, "Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services)" (5 December 2019) at paras 7.10–7.14.

26 [2014] 2 SLR 208.

27 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [49].

28 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [49].

29 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [39]–[45].

(b) Second, the plaintiff must be able to show a reasonable *prima facie* case of wrongdoing against the person whose information or identity is sought.

(c) Third, the plaintiff must show that the disclosure sought is necessary to enable him to take action, or at least that it is just and convenient in the interests of justice to make the order sought. Two significant considerations on this issue are whether there exists an alternative and more appropriate method to obtain the information and whether the order is proportionate in the circumstances.

21 There are two additional considerations which the plaintiff should also keep in mind when applying for pre-action disclosure.

22 First, the plaintiff must adduce credible evidence that the intended proceedings have a Singapore nexus.[30] It is not sufficient to merely assert that the hack took place or was actionable in Singapore.[31] In this regard, establishing a Singapore nexus means something beyond the mere possibility that the plaintiff could potentially bring a cause of action in Singapore. This is a "broad brush" analysis that does not require a detailed analysis of where the witnesses and evidence are located, or other connecting factors that may be relevant to a *Spiliada* enquiry.[32]

23 Second, as confidentiality obligations are likely to be at stake, the plaintiff must prove that his interest in ascertaining the viability of his intended claim outweighs the defendant's interest in maintaining any measure of confidentiality regarding the documents to be disclosed.[33] In this regard, since there is likely to be fraud involved in the hack, this issue is unlikely to pose too much difficulty for the plaintiff. In any event, it would also be in the commercial interest of the cryptocurrency exchange not to resist too hard given the potential reputational damage that would accompany a refusal to comply with such a discovery application.

30 *Intas Pharmaceuticals Ltd v DealStreetAsia Pte Ltd* [2017] 4 SLR 684.
31 *Intas Pharmaceuticals Ltd v DealStreetAsia Pte Ltd* [2017] 4 SLR 684 at [53].
32 *Intas Pharmaceuticals Ltd v DealStreetAsia Pte Ltd* [2017] 4 SLR 684 at [57]–[60].
33 *Intas Pharmaceuticals Ltd v DealStreetAsia Pte Ltd* [2017] 4 SLR 684 at [62].

C. Pre-action interrogatories

24 Finally, plaintiffs should consider applying for pre-action interrogatories against third parties who may be associated with the parties suspected to be involved in the cryptocurrency hack in some way. For example, the plaintiff may ask the following interrogatories of the third parties:

(a) What is the third party's relationship to the hacker?

(b) When was the last time the third party communicated with the hacker?

(c) If there was recent communication, what were the contents of such communication?

(d) Were any documents provided by the hacker?

25 The objective of such interrogatories would again be to facilitate the information gathering process and help the plaintiff find out who the appropriate parties to sue are, or whether there is even any cause of action against them.[34]

26 At this juncture, it should be noted that the principles underlying both pre-action interrogatories and pre-action discovery are broadly the same.[35] Therefore, the principles laid out above will similarly apply.

27 Fundamentally, both forms of disclosure are to save costs and time in avoiding litigation or identifying the real issues in dispute, and efficiently manage court processes.[36] However, this is subject to safeguards such as ensuring that the application is confined strictly to what is necessary for disposing fairly of the cause or matter or for saving costs. Fishing expeditions will not be permitted.[37]

28 As with pre-action discovery, relevance and necessity are the main cornerstones in determining whether pre-action

34 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [27].
35 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [25].
36 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [26].
37 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [27].

interrogatories will be ordered.[38] In this regard, the clearer the cause of action that a claimant is able to put before the court, the easier it is to ascertain the relevance and necessity of the pre-action interrogatories to the intended proceedings.[39] Further, other facts of necessity such as notions of proportionality, the availability of other avenues to obtain the information and how intrusive those interrogatories are would be taken into consideration as well.[40]

29 The court will ultimately take a multi-factorial view and question whether it is just and necessary for the plaintiff to secure the information sought even before any proceedings are commenced. In general, the plaintiff must show that the circumstances are such that the case differs from the normal.[41] In the case of a cryptocurrency hack, this is likely to be satisfied.

III. Conclusion

30 In conclusion, plaintiffs who have been victimised by cryptocurrency hacks would do well to consider the entire arsenal of tools available to them under the Rules of Court. This will ensure that they are able to obtain maximum recovery before the proceeds of the cryptocurrency fraud are too far gone.

38 Rules of Court (Cap 322, R 5, 2014 Rev Ed) O 26A r 2.
39 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [47].
40 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [48].
41 *Dorsey James Michael v World Sport Group Pte Ltd* [2014] 2 SLR 208 at [50].