IN THE GENERAL DIVISION OF
THE HIGH COURT OF THE REPUBLIC OF SINGAPORE

[2022] SGHC 46

Suit No 470 of 2021
(Summons Nos 2444 and 4880 of 2021)

Between

CLM

… *Plaintiff*

And

(1) CLN
(2) CLO
(3) CLP
(4) CPZ
(5) CQA
(6) CQB
(7) CQC

… *Defendants*

GROUNDS OF DECISION

[Civil Procedure — Amendments]
[Civil Procedure — Mareva injunctions]
[Civil Procedure — Injunctions — Proprietary injunction]
[Civil Procedure — Parties — Joinder]
[Civil Procedure — Service — Substituted service out of jurisdiction]

TABLE OF CONTENTS

CLM
v
CLN and others

[2022] SGHC 46

General Division of the High Court — Suit No 470 of 2021 (Summons Nos 2444 and 4880 of 2021)
Lee Seiu Kin J
8 June, 9 November 2021

4 March 2022

Lee Seiu Kin J:

Introduction

1 The present dispute raised two interesting and novel points of law. First, can stolen cryptocurrency assets be the subject of a proprietary injunction? Second, does the court have jurisdiction to grant interim orders against persons whose identities are presently unknown?

2 The plaintiff had commenced an action to trace and recover 109.83 Bitcoin ("BTC") and 1497.54 Ethereum ("ETH") (collectively, the "Stolen Cryptocurrency Assets") that were allegedly misappropriated from him by unidentified persons (*ie*, the first defendants), a portion of which has been traced to digital wallets that were controlled by cryptocurrency exchanges with operations in Singapore (*ie*, the second and third defendants).

3 In Summons No 2444 of 2021 ("SUM 2444"), which was heard on 8 June 2021, the plaintiff sought the following interlocutory relief via an *ex parte* application:[1]

> (a) A proprietary injunction prohibiting the first defendants from dealing with, disposing of, or diminishing the value of the Stolen Cryptocurrency Assets.
>
> (b) A worldwide freezing injunction prohibiting the first defendants from dealing with, disposing of, or diminishing their assets up to the value of US$7,089,894.68, being the value of the Stolen Cryptocurrency Assets.
>
> (c) Ancillary disclosure orders against the second and third defendants to assist in the tracing of the Stolen Cryptocurrency Assets and the identification of the first defendants.

4 In Summons No 4880 of 2021 ("SUM 4880"), the plaintiff sought, via an *ex parte* application, leave to join persons as defendants to the action because they were either (a) individuals believed to have participated in or assisted with the theft or (b) entities who had received the Stolen Cryptocurrency Assets.[2]

5 I allowed the above applications and I set out the grounds of my decision below.

---

1 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 3.

2 Plaintiff's Skeletal Submissions dated 29 October 2021 at para 2(a).

SUM 2444

The parties

6 The plaintiff is a national of the United States of America and an entrepreneur, who claims to be the owner of the Stolen Cryptocurrency Assets.[3]

7 The first defendants are persons unknown, which refer to any person or entity who carried out, participated in, or assisted in the theft of the Stolen Cryptocurrency Assets, save for entities involved in the provision of cryptocurrency hosting or trading facilities in the ordinary course of business. At the time of the hearing for SUM 2444, the plaintiff was unable to identify specifically who the first defendants may be.[4]

8 The second and third defendants are entities that are incorporated in the Cayman Islands and Seychelles respectively, and who operate cryptocurrency exchanges with operations in Singapore. Portions of the Stolen Cryptocurrency Assets have been traced to digital wallets in the exchanges operated by the second and third defendants. Nonetheless, at the time of application, the plaintiff believed that the second and third defendants were innocent third parties and asserted no substantive claims against them apart from disclosure.[5]

The nature of BTC and ETH

9 For context, I briefly set out the nature of the Stolen Cryptocurrency Assets.

---

3 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 6.

4 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 7.

5 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 8.

10 BTC and ETH are commonly referred to as cryptocurrencies. While the word "currency" connotes a medium of exchange, a cryptocurrency is not associated with any physical object (unlike how a currency such as the US Dollar is). In essence, BTC and ETH are records in a network of computers associated with that cryptocurrency. These records are stored in publicly available ledgers that provide a digital record of every BTC or ETH transaction that has taken place. The records, in a form known as blockchain, provide an accurate, verifiable, and permanent audit trail with which one can track the transmission of cryptocurrencies.[6] The following explanation in Kelvin F K Low and Ernie G S Teo, "Bitcoins and other cryptocurrencies as property?" (2017) 9(2) Law, Innovation and Technology 235 (available at https://ink.library.smu.edu.sg/sol_research/2806) is helpful:

> Bitcoin was conceived by the pseudonymous Satoshi Nakamoto in his seminal white paper first published in 1 November 2008. … Bitcoin was envisaged as "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." As a result of the central role played by cryptography in the system, bitcoin and its derivatives are known as cryptocurrencies. Once properly validated, bitcoin transactions are irreversible, or in the parlance of the bitcoin community, immutable.
>
> Unlike most prior forms of "electronic money", the system is neither derived from nor backed by any fiat currency. Instead, individual bitcoins are first created in the system through a process called mining. This process is intimately connected to the verification process by which transfers are tracked within the system. Instead of a centralised ledger (or register), the bitcoin system employs a decentralised system of ledgers known as the blockchain. The blockchain is essentially a register containing information tracking the creation and transfer of bitcoins much like a bank ledger tracks payments between bank accounts. Unlike bank accounts, however, the blockchain is not maintained by a central authority but instead resides in thousands of computers throughout the world. These computers are connected over the Internet to other computers running the same software, creating a network. When the

[6] Plaintiff's 1st Affidavit dated 27 May 2021 at para 16.

holder of a bitcoin wishes to make a payment in bitcoin, an instruction is sent to this network and the computers on the network (nodes) validate the transaction before it is added to the blockchain files sitting on all the computers in the network. The process of validation involves the solution of a complex mathematical puzzle by nodes operated by users known as miners. Although the puzzles are described as complex, "[i]n fact there is nothing complex about this process, and you can do this by hand without a calculator; it just deliberately takes many computational steps without shortcuts." In essence, this involves the miners' computers engaging in a guessing game and the odds of winning are dependent on how quickly a miner's computer can perform calculations as compared to those of other miners. Such users are described as miners because, in order to incentivise participants to engage in this process of validation, the system rewards the first to solve the puzzle with a preset quantity of new bitcoins. This did not require very much computational power in the beginning and anyone with a computer could mine bitcoin. However, as a result of the design of the bitcoin protocol, the level of difficulty increases with increased computational power participating in the network, and mining progressed from the use ordinary computers to dedicated ASIC (application-specific integrated circuit) chips that are designed to do nothing except mine for bitcoin. Although computationally difficult to solve, the solutions are easily verifiable by other nodes, who may or may not be miners, on the network. Once verified, the transaction is added to the blockchain. This verification process requires a consensus of a majority of nodes in the network so that the likelihood of fraud is dramatically reduced.

A holder of bitcoins possesses a public bitcoin address and a private cryptographic key. The bitcoin address is often regarded as a serving a similar function to a bank account number. All that is needed to receive bitcoins is this public bitcoin address. Like a bank account, it is possible to have as many bitcoin addresses as one can be bothered to create. In order to transfer bitcoins out of the address, however, one requires both the address and the private cryptographic key. Whilst sometimes considered the equivalent of a password, the private cryptographic key is mathematically linked to the public address so that it is not possible to change the private key unlike a conventional password. One of the attractions of bitcoins is its relative anonymity compared with other payment systems. … However, bitcoin addresses are not completely anonymous but only pseudo-anonymous. While the identity of the address holder is not known, all transactions related to the address are in fact transparent and tracked in the blockchain. With the appropriate information, including publicly available information, it is possible to track some bitcoin transactions. …

11 BTC and ETH are sent between users electronically by sharing public "wallet" addresses on the blockchain. These wallets are represented by a string of numbers and letters, and loosely function like an account number. Unlike traditional bank accounts, however, all transactions to and from a given wallet can be viewed on the public blockchain.[7]

12 For security, BTC and ETH wallets employ one or more "private keys" that should be known only to the wallet owner. The private key functions like a signature that confirms that any given transaction is authorised by the wallet owner. Private keys are represented by a string of 64 numbers and alphabets. Thus, anyone in possession of the private key can access the linked wallet and transfer BTC and ETH out. Likewise, losing the private key means that the funds held in the wallet cannot be accessed. As there are more than a billion permutations for what a private key may be, it is virtually impossible for one to guess the private key of a digital wallet.[8]

13 Given the risks associated with the loss of the private key, most private keys are backed up by a "recovery seed" that can restore access to the private key in the event of loss.[9]

Background to the theft

14 Prior to the theft, the Stolen Cryptocurrency Assets were accessible through two separate digital wallets, controlled by two software applications

---

7 Plaintiff's 1st Affidavit dated 27 May 2021 at para 17.

8 Plaintiff's 1st Affidavit dated 27 May 2021 at paras 18 and 19.

9 Plaintiff's 1st Affidavit dated 27 May 2021 at para 20.

which were downloaded onto the plaintiff's mobile phone and marketed publicly as "Exodus" and "BRD".[10]

15 BRD and Exodus wallets are decentralised "hot" wallets (*ie*, wallets that are connected to the Internet) that are accessible through a free mobile application that is locked by either a password or a biometric key. BRD and Exodus provide users with a public wallet address and allow the private key to be stored directly on the user's phone. BRD and Exodus wallets do not themselves hold cryptocurrencies but rather manage the private key through which a user can access those cryptocurrencies (which are maintained on the BTC or ETH blockchain).[11]

16 While the plaintiff had locked both his Exodus and BRD wallets with a password, both wallets employed recovery seeds that could be used to recover the passwords and could therefore allow him to gain access to the cryptocurrencies in the event that his mobile phone was lost or destroyed.[12]

17 In January 2021, the plaintiff and seven acquaintances were on vacation at his apartment in Mexico. On the night of 7 January 2021, the plaintiff and one acquaintance went out while the rest of the group remained at his apartment. As he needed some money, the plaintiff called one member of the group at his apartment, [E], and requested that [E] retrieve some cash that the plaintiff had kept in the safe in the master bedroom of his apartment. The plaintiff read the safe combination to [E] and [E] repeated the combination to the plaintiff to confirm that he had gotten it right. According to the plaintiff, during the call,

---

10 Plaintiff's 1st Affidavit dated 27 May 2021 at para 21.

11 Plaintiff's 1st Affidavit dated 27 May 2021 at paras 22 and 23.

12 Plaintiff's 1st Affidavit dated 27 May 2021 at para 25.

some members of the group were in the same room as [E], while two other members were in a nearby bedroom. The plaintiff therefore claimed that anyone in the apartment could have heard the safe combination being said out loud. [E] later brought to the plaintiff the requested cash, and the three of them returned to the apartment at around 2.00am on 8 January 2021.[13]

18 At around 8.00pm on 8 January 2021, the plaintiff accessed his Exodus and BRD wallets and discovered that his BTC and ETH had been withdrawn without his knowledge or consent.[14]

19 The transaction records of the BRD and Exodus applications showed that on 8 January 2021, the following transfers were made to three different wallet addresses that the plaintiff did not control or own:[15]

(a) at 7.16pm, 59.38 BTC was transferred from the Exodus wallet to wallet address [address redacted];

(b) at 7.17pm, 50.45 BTC was transferred from the BRD wallet to wallet address [address redacted]; and

(c) at 7.19pm, 1497.54 ETH was transferred from the Exodus wallet to wallet address [address redacted].

20 The plaintiff claimed that, since his mobile phone was with him when the above transactions took place, the first defendants could not have effected the transfers using the BRD and Exodus applications on his mobile phone. Hence, the plaintiff believed that the first defendants obtained the plaintiff's

---

13 Plaintiff's 1st Affidavit dated 27 May 2021 at paras 26 and 27.

14 Plaintiff's 1st Affidavit dated 27 May 2021 at para 28.

15 Plaintiff's 1st Affidavit dated 27 May 2021 at para 29; Plaintiff's Skeletal Submissions dated 4 June 2021 at para 10.

recovery seeds by accessing his safe, sometime between the time he read the safe combination aloud to [E] the night before and the time at which the transactions were made. The first defendants entered the plaintiff's recovery seeds into the BRD and Exodus applications via a separate mobile device to access the plaintiff's private keys, which they then used to transfer the Stolen Cryptocurrency Assets.[16]

21 Subsequently, the plaintiff's investigations and tracing efforts determined that the first defendants had dissipated the stolen assets through a series of digital wallets.[17] Ultimately, the relevant transfers are as follows:[18]

(a) on or around 17 April 2021, 15.0 BTC traceable to the Stolen Cryptocurrency Assets was transferred to wallet address [address redacted], which is controlled by the second defendant (the "second defendant's account"); and

(b) on or around 25 April 2021, 0.3 BTC traceable to the Stolen Cryptocurrency Assets was transferred to wallet address [address redacted], which is controlled by the third defendant (the "third defendant's account").

22 Hence, the plaintiff sought a proprietary injunction and a worldwide freezing injunction against the first defendants, as well as ancillary disclosure orders against the second and third defendants for information and documents

---

16 Plaintiff's 1st Affidavit dated 27 May 2021 at para 30.

17 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 55(b).

18 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 11.

relating to the accounts that were credited with the 15.0 BTC and 0.3 BTC that are traceable to the Stolen Cryptocurrency Assets.[19]

My decision

Jurisdiction against persons unknown

23 As stated above (at [7]), the identity of the first defendants were unknown at the time of the application in SUM 2444. There is therefore a preliminary issue of whether the court has jurisdiction to grant interim orders against the first defendants even though their identities were unknown at that time. The plaintiff submitted in the affirmative, with the following authorities in support.[20]

24 In the UK, the jurisdiction to grant orders against persons unknown was recognised in *Bloomsbury Publishing Group Ltd and another v News Group Newspapers Ltd and others* [2003] 1 WLR 1633 ("*Bloomsbury*"). There, the court granted the plaintiff's application for an interlocutory injunction against unknown persons who had taken copies of an unpublished book, enjoining such persons to deliver up the copies of the book and restraining them from disclosing to any person any information derived from the book (at 1634). The court noted that the UK Civil Procedure Rules ("CPR") Practice Directions para 4.1(1) merely required that the title of the proceedings "*should* state … the full name of each party" [emphasis added] and not that a defendant *must* be named (at [16] and [19]). Moreover, the court considered CPR 3.10, which states as follows:

---

19 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 13.

20 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 25.

> **General power of the court to rectify matters where there has been an error of procedure**
>
> **3.10** Where there has been an error of procedure such as a failure to comply with a rule or practice direction —
>
> (a) The error does not invalidate any step taken in the proceedings unless the court so orders; and
>
> (b) the court may make an order to remedy the error.

The court noted that "[CPR] 3.10 confers on the court a general power of dispensation where there has been a procedural error and provides that such error does not invalidate any step taken in the proceedings unless the court so orders" (at [15]). From this premise, the court distinguished the pre-CPR case of *Friern Barnet Urban District Council v Adams and others* [1927] 2 Ch 25, where it was held *inter alia* that the prescribed form of writ required the defendant to be named. Because of the different regime introduced by the CPR, the court held (at [19]) that "[t]he proper application of [CPR] 3.10 is incompatible with a conclusion that the joinder of a defendant by description rather than by name is for that reason alone impermissible". Importantly, the court set out the appropriate test as follows (at [21]):

> … The crucial point, as it seems to me, is that the description used must be sufficiently certain as to identify both those who are included and those who are not. If that test is satisfied then it does not seem to me to matter that the description may apply to no one or to more than one person nor that there is no further element of subsequent identification whether by service or otherwise.

25 In *CMOC v Persons Unknown* [2017] EWHC 3599 (Comm) ("*CMOC*"), the plaintiffs claimed against unidentified defendants who misappropriated £6.3m by infiltrating the email account of the plaintiff's senior management and issuing payment instructions without the plaintiff's authorisation (at [1]). The court recognised *Bloomsbury* as authority for the proposition that the courts have jurisdiction to grant interlocutory injunctions

against persons unknown and held that there was "no reason in principle against, and indeed a good arguable case for, saying that this should extend to a freezing injunction" (at [4]). The court thereby granted the plaintiff's application for a worldwide freezing injunction against persons unknown, and ancillary disclosure orders against certain banks who had received the stolen proceeds (at [9]–[10]).

26 In *Zschimmer & Schwarz GmbH & Co KG Chemische Fabriken v Persons Unknown & Anor* [2021] 7 MLJ 178 ("*Zschimmer*"), the plaintiff, a German company, was defrauded by unidentified persons to make payments to a bank account in Malaysia, which the plaintiff thought were genuine commission payments to a South Korean business partner. In granting a proprietary injunction and a freezing injunction against persons unknown, the Malaysian High Court considered *CMOC*, and noted that it was affirmed by the UK Supreme Court in *Cameron v Liverpool Victoria Insurance Co Ltd* [2019] 3 All ER 1 and applied in at least two other English decisions (at [44]–[48]). Importantly, the court reasoned as follows (at [40] and [49]):

> 40 It is not usually the case that a defendant is described as 'persons unknown'. Nevertheless, the court can grant interlocutory orders against the first defendant — being persons unknown. In cases like the present which involve cyber fraud and fake email addresses, the fraudster or fraudsters are unknown. English case law have allowed for similar injunctive orders against 'persons unknown'. There is nothing in our Rules of Court 2012 that would prevent the writ of summons and applications from being filed against persons unknown.
>
> …
>
> 49 As stated above, *there is nothing in our Rules of Court 2012 prohibiting the making of an order against persons unknown.* In fact, *O 89 of the Rules of Court 2012 for summary proceedings for possession of land allows for a defendant reference to persons unknown* (see *Fauziah bt Ismail & Ors v Lazim bin Kanan & Ors (as person occupying GM 820, Lot 1642, Mukim Kajang, Daerah Hulu Langat, Negeri Selangor Darul Ehsan without the applicants' consent)* [2013] 5 MLJ 423; [2013]

> 7 CLJ 37 (CA) the commentary in *Foong's Malaysia Cyber, Electronic Evidence and Information Technology Law*, para [8.098] to [8.100]).
>
> [emphasis added]

27 In my view, the reasoning in the above authorities is instructive and readily applicable to our legal context.

28 To begin with, like in the case of the UK and Malaysia, there is nothing in our Rules of Court (Cap 322, R5, 2014 Rev Ed) ("ROC") that requires a defendant to be specifically named. While the prescribed form for commencing an action by writ (Form 2 under Appendix A of the ROC) contains fields for the plaintiff to state the name and address of the defendant, O 1 r 7 of the ROC clarifies that: "the Forms in Appendix A to these Rules shall be used where applicable *with such variations as the circumstances of the particular case require*" [emphasis added].

29 Moreover, similar to CPR 3.10 in the UK (as relied on by the court in *Bloomsbury*), O 2 r 1 of our ROC expressly provides that even if the commencement of proceedings against persons unknown contravenes the ROC, such a contravention is treated as a mere irregularity, and will not result in the nullification of proceedings unless the court exercises its discretion to order the same:

> **Non-compliance with Rules (O. 2, r. 1)**
>
> **1.**—(1) Where, in beginning or purporting to begin any proceedings or at any stage in the course of or in connection with any proceedings, there has, by reason of anything done or left undone, been a failure to comply with the requirements of these Rules, whether in respect of time, place, manner, form or content or in any other respect, *the failure shall be treated as an* ***irregularity*** *and* ***shall not nullify*** *the proceedings, any step taken in the proceedings, or any document, judgment or* ***order*** *therein.*

> (2) Subject to paragraph (3), the Court ***may***, on the ground that there has been such a failure as is mentioned in paragraph (1), and on such terms as to costs or otherwise as it thinks just, set aside either wholly or in part the proceedings in which the failure occurred, any step taken in those proceedings or any document, judgment or ***order*** therein or exercise its powers under these Rules to allow such amendments (if any) to be made and to make such order (if any) dealing with the proceedings generally as it thinks fit.
>
> …
>
> [emphasis added in bold italics and italics]

Plainly, the reference to "order" in the above provision covers interim orders such as injunctions.

30 Furthermore, just as how O 89 of the Malaysian Rules of Court 2012 allows for a reference to persons unknown in summary proceedings for possession of land (as noted in *Zschimmer*), so does O 81 of our ROC, which governs the same. Order 81 r3 of the ROC provides as follows:

> **Form of originating summons (O. 81, r. 3)**
>
> 3. An originating summons filed under this Order shall include the following note at the end thereof:
>
> > "*Note*: Any person occupying the premises who is not named as a defendant by this originating summons may apply to the Court personally or by solicitor to be joined as a defendant. If a person occupying the premises does not attend personally or by solicitor at the time and place abovementioned, such order will be made as the Court may think just and expedient.".

In *Singapore Civil Procedure 2021* vol 1 (Cavinder Bull gen ed) (Sweet & Maxwell, 2021) ("*White Book*") at para 81/3/1, the learned author states:

> **Persons unknown—**The originating process under this rule must be in Form 4 and shall contain the note as set out in this rule. Where the identity of persons in occupation is unknown to the plaintiff they may be described as "Persons Unknown": see *Bristol Corp. v. Persons Unknown* [1974] 1 W.L.R. 365; [1974] 1 All E.R. 593.

Since persons whose identities are unknown can be described as "persons unknown" in such summary proceedings, I see no reason in principle why they cannot be so described for the purposes of interim orders.

31 Hence, in my opinion, this court has the jurisdiction to grant interim orders against the first defendants, who are persons unknown.

32 However, I do stress that, following *Bloomsbury*, the description of the first defendants must be sufficiently certain as to identify both those who are included and those who are not.

33 In *Zschimmer*, the persons unknown were described as follows (at [42]):

> …
>
> (a) any person or entity who carried out and/or assisted and/or participated in the fraud;
>
> (b) any person or entity who received any of the EUR123,014.65 misappropriated from the plaintiff (including any traceable proceeds thereof) other than in the course of a genuine business transaction with either another defendant or a third party; and
>
> (c) in either case of para 2(i) or (ii), other than by way of the provision of banking facilities.

34 In the present dispute, the following description was used:[21]

> [A]ny person or entity who carried out, participated in or assisted in the theft of the Plaintiff's Cryptocurrency Assets on or around 8 January 2021, save for the provision of cryptocurrency hosting or trading facilities.

35 I was satisfied that the present description describes with sufficient certainty the persons who fall within and outside of the description.

---

[21] Plaintiff's Skeletal Submissions dated 4 June 2021 at para 34.

Proprietary injunction

36 As stated above (at [3(a)]), the plaintiff sought a proprietary injunction prohibiting the first defendants from dealing with, disposing of, or diminishing the value of the Stolen Cryptocurrency Assets.

37 Pursuant to s 18(2) read with para 5(a) of the First Schedule of the Supreme Court of Judicature Act (Cap 322, 2007 Rev Ed), the General Division of the High Court has the power to grant interim proprietary injunctions.

38 As set out in *Bouvier, Yves Charles Edgar and another v Accent Delight International Ltd and another and another appeal* [2015] 5 SLR 558 ("*Bouvier*") at [143]–[164], the applicant must prove the following to obtain a proprietary injunction:

(a) there is a serious question to be tried; and

(b) the balance of convenience lies in favour of granting the injunction.

This is because the usual principles in *American Cyanamid Co v Ethicon Ltd* [1975] AC 396 apply.

(1) Serious question to be tried

39 As stated by the Court of Appeal in *Bouvier* (at [151]), in respect of an application for an interlocutory proprietary injunction, the first requirement of showing that there is a serious question to be tried will be satisfied as long as "the plaintiffs have a seriously arguable case that they [have] a proprietary interest". In this regard, the court does not engage in complex questions of law or fact at the interlocutory stage.

40 The important issue which arose here was therefore whether the Stolen Cryptocurrency Assets, being cryptocurrency, were capable of giving rise to proprietary rights which could be protected via a proprietary injunction.

41 It is apposite to first refer to the classic definition of a property right in *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175 ("*Ainsworth*") at 1248:

> [I]t must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability.

42 In *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17, the Singapore International Commercial Court held (at [138]–[146]) that it was possible for cryptocurrencies to be held on trust, and that the defendant in that case did hold BTC on trust for the plaintiff. In so holding, the court reasoned that cryptocurrencies meet the four requirements set out in *Ainsworth* and "have the fundamental characteristic of intangible property as being an identifiable thing of value" (at [142]). However, it should be noted that since this point was undisputed by the parties, the court was satisfied that cryptocurrencies could be created as property in a generic sense and left open the question of what the precise nature of this property right was.

43 On appeal however, the parties disputed the issue of whether cryptocurrencies were a species of property that was capable of being held on trust: see *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20 at [137]. The Court of Appeal reasoned that it was unnecessary to consider this issue because even if it was answered affirmatively, there was no certainty of intention to create a trust on the facts (at [144]). Nevertheless, the court canvassed in detail the authorities in support of treating cryptocurrencies as property (at [139]–[143]):

139 There have been some other cases in the Commonwealth that have implicitly accepted that cryptocurrency may be regarded as property, although we are not aware of any court that has attempted to identify the precise nature of the property right if any. In *Elena Vorotyntseva v Money-4 Limited and others* [2018] EWHC 2596 (Ch), the English High Court issued a proprietary injunction preventing the removal of specific ETH and BTC holdings. In coming to his decision, Birss J observed that there had been no suggestion that cryptocurrencies could not be a form of property.

140 In *Copytrack Pte Ltd v Wall* [2018] BCSC 1709, the Supreme Court of British Columbia ordered that some C$400,000 worth of ETH be traced, which suggests that ETH was recognised as a species of property susceptible to tracing. The action was brought by Copytrack Pte Ltd ("Copytrack"), a company engaged in the business of digital content management and automated copyright enforcement. Copytrack created its own cryptocurrency, Copytrack tokens, and mistakenly transferred a more valuable cryptocurrency, ETH, to the defendant investor instead of Copytrack tokens. The ETH was then transferred by the defendant to third parties. Copytrack sought to trace and recover the ETH. The court characterised the issue of whether the property law doctrines of conversion and wrongful detention could apply to cryptocurrencies as a "critical issue'" and the "real issue on this application". While the court did not go so far as to rule on whether cryptocurrencies could, in fact, be subject to specific property law claims, the court held that it would be unreasonable and unjust in the circumstances to deny Copytrack a remedy, and so allowed Copytrack to trace and recover the wrongfully transferred ETH.

141 Academic commentators broadly agree that BTC may be regarded as a property right, although they disagree as to the precise nature of this right. In Jean Bacon *et al*, "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" (2018) 25(1) Rich J L & Tech 1, the authors suggest (at para 182) that holders of digital tokens such as BTC should be regarded as having a property interest at common law, because they hold a bundle of rights that include the right to control the token. This interest is identifiable through entries on the blockchain, can be transferred by entries of the blockchain, and has a high degree of permanence and stability.

142 To similar effect is Kelvin F K Low and Ernie G S Teo, "Bitcoins and other cryptocurrencies as property?" (2017) 9(2) *Law, Innovation and Technology* 235 (available at https://ink.library.smu.edu.sg/sol_research/2806), where the authors argue that the property right relating to BTC is the right

> to have one's public BTC address appear as the last entry in the blockchain in relation to a particular BTC. Such a right provides exclusive control to the holder in the form of universal exigibility and can be seen as involving a true property transfer when one transfers BTC from one's public BTC address to another's BTC address.
>
> 143 Most recently, the UK Jurisdiction Taskforce ('UKJT') chaired by Sir Geoffrey Vos released its "Legal Statement on Cryptoassets and Smart Contracts" (November 2019), where it considered the question of whether English law would treat a particular cryptoasset as property. The UKJT defined cryptoassets as generally having the following characteristics (at para 31): (a) intangibility; (b) cryptographic authentication; (c) use of a distributed transaction ledger; (d) decentralisation; and (e) rule by consensus. The UKJT stated (at para 85) that cryptoassets have all the indicia of property, and that their novel or distinctive features as aforementioned do not disqualify them from being property. The UKJT also stated that cryptoassets are not disqualified from being property simply because they might not be classifiable either as things in possession or as things in action. The UKJT therefore concluded that cryptoassets could be treated, in principle, as property.

Ultimately, the court observed (at [144]) that "[t]here may be much to commend the view that cryptocurrencies should be capable of assimilation into the general concepts of property".

44 The plaintiff referred me to the New Zealand case of *Ruscoe v Cryptopia Ltd (in liq)* [2020] 2 NZLR 809 ("*Ruscoe*"), where the High Court held, following a comprehensive discussion (at [102]–[120]), that (at [120]):

> [C]ryptocurrencies meet the standard criteria outlined by Lord Wilberforce [*ie*, the four requirements set out in *Ainsworth*] to be considered a species of "property". They are a type of intangible property as a result of the combination of three interdependent features. They obtain their definition as a result of the public key recording the unit of currency. The control and stability necessary to ownership and for creating a market in the coins are provided by the other two features – the private key attached to the corresponding public key and the generation of a fresh private key upon a transfer of the relevant coin.

45 In this regard, the court examined the four requirements in *Ainsworth* in turn:[22]

(a) The first requirement is that the right must be "definable" – the asset must hence be capable of being isolated from other assets whether of the same type or of other types and thereby identified (*Ruscoe* at [104]). To this end, cryptocurrencies are computer-readable strings of characters which are recorded on networks of computers established for the purpose of recording those strings, and are sufficiently distinct to be capable of then being allocated to an account holder on that particular network (*Ruscoe* at [105]).

(b) The second requirement is that the right must be "identifiable by third parties", which requires that the asset must have an owner being capable of being recognised as such by third parties (*Ruscoe* at [109]). An important indicator is whether the owner has the power to exclude others from using or benefiting from the asset (*Ruscoe* at [110]). In this vein, excludability is achieved in respect of cryptocurrencies by the computer software allocating the owner with a private key, which is required to record a transfer of the cryptocurrency from one account to another (*Ruscoe* at [112]).

(c) The third requirement is that the right must be "capable of assumption by third parties", which in turn involves two aspects: that third parties must respect the rights of the owner in that asset, and that the asset must be potentially desirable (*Ruscoe* at [114]). The fact that these two aspects are met by cryptocurrencies, is evidenced by the fact

---

22 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 45.

that many cryptocurrencies, certainly BTC and ETH, are the subject of active trading markets (*Ruscoe* at [116]).

(d) The fourth requirement is that the right and in turn, the asset, must have "some degree of permanence or stability", although this is a low threshold since a "ticket to a football match which can have a very short life yet unquestionably it is regarded as property" (*Ruscoe* at [117]). In this respect, the blockchain methodology which cryptocurrency systems deploy provides stability to cryptocurrencies, and a particular cryptocurrency token stays fully recognised, in existence and stable unless and until it is spent through the use of the private key, which may never happen (*Ruscoe* at [118]).

46 Having considered the extant case law and especially the analysis in *Ruscoe*, I was of the view that cryptocurrencies satisfied the definition of a property right in *Ainsworth*. The plaintiff was therefore able to prove a serious arguable case that the Stolen Cryptocurrency Assets were capable of giving rise to proprietary rights, which could be protected via a proprietary injunction. I reiterate that the court does not engage in complex questions of law or fact at the interlocutory stage (see [39] above). Hence, the first requirement of showing that there is a serious question to be tried was satisfied.

(2) Balance of convenience

47 The balance of convenience is assessed by considering the potential prejudice that the applicant may suffer if the injunction is not granted, against the prejudice to the respondent in the event that the injunction is granted and the applicant's hypothesis is refuted at the trial (*Bouvier* at [161]).

48 In my view, the balance clearly lay in favour of granting the proprietary injunction. If it were not granted, there would be a real risk that the first defendants would dissipate the Stolen Cryptocurrency Assets, which would prevent the plaintiff from recovering those assets even if he successfully obtained a judgment in his favour. Conversely, even if the plaintiff's case were later refuted, the first defendants would only suffer losses arising from their inability to deal with the Stolen Cryptocurrency Assets, which could be compensated by way of damages.[23]

(3) Conclusion

49 For the above reasons, I granted the proprietary injunction prohibiting the first defendants from dealing with, disposing of, or diminishing the value of the Stolen Cryptocurrency Assets.

Mareva injunction

50 In addition to the proprietary injunction, the plaintiff also sought a worldwide freezing injunction to restrain the first defendants from dealing with, disposing of, or diminishing the value of, their assets up to the value of US$7,089,894.68, being the value of the Stolen Cryptocurrency Assets (see [3(b)] above).

51 To obtain a freezing injunction, the applicant hasto prove two requirements (*Bouvier* at [36]):

(a) First, the applicant must have a good arguable case on the merits of its claim.

---

[23] Plaintiff's Skeletal Submissions dated 4 June 2021 at para 48.

(b) Second, there must be a real risk that the defendant will dissipate his assets to frustrate the enforcement of an anticipated judgment of the court.

52 The applicable test for a worldwide freezing injunction is the same as that for a domestic one. However, the circumstances that will have to be established in order to cross the threshold of necessity will likely be more exacting where a worldwide freezing injunction is concerned (*Bouvier* at [36]–[37]). There is also a further consideration of whether the defendant has sufficient assets within the jurisdiction to satisfy the prospective judgment: generally, the fewer the assets within the jurisdiction, the greater the necessity for taking protective measures in relation to those outside it (*Guan Chong Cocoa Manufacturer Sdn Bhd v Pratiwi Shipping SA* [2003] 1 SLR(R) 157 at [29]).

53 A good arguable case is one which is "more than barely capable of serious argument, but not necessarily one which the judge considers would have a better than 50 per cent chance of success" (*Bouvier* at [36]). The plaintiff has two claims against the first defendants. First, that the first defendants hold the Stolen Cryptocurrency Assets on a constructive trust for the plaintiff. Second, that the first defendants were enriched at the expense of the plaintiff in circumstances that were unjust, because the first defendants obtained the plaintiff's assets without his consent or authority.[24] In respect of the first claim, it is hornbook law that where a person misappropriates the property of another without consent, a constructive trust arises by operation of law over the stolen assets, as it would be unconscionable for the misappropriating party to assert any beneficial interest in the property or their traceable proceeds (*Yuanta Asset*

[24] Plaintiff's Skeletal Submissions dated 4 June 2021 at paras 37 to 39 and 53.

Management International Ltd and another v Telemedia Pacific Group Ltd and another and another appeal [2018] 2 SLR 21 at [113]). In my view, this alone was sufficient to show that the plaintiff had a good arguable case against the defendants.

54 As for proving a real risk of dissipation, there must be some "solid evidence" to demonstrate the risk, and not just bare assertions to that effect (*Bouvier* at [36]). Importantly, a well-substantiated allegation that a defendant has acted dishonestly can and often will be relevant to whether there is a real risk that the defendant may dissipate his assets (*Bouvier* at [94]). In this regard, the plaintiff rightly submitted that the first defendants had acted dishonestly in misappropriating the Stolen Cryptocurrency Assets. Having examined the evidence, I found that the first defendants dissipated the stolen assets through a series of digital wallets that appear to have been created solely for the purpose of frustrating the plaintiff's tracing and recovery efforts, and which had either no or negligible transactions other than the deposit and withdrawal of the Stolen Cryptocurrency Assets.[25] Moreover, the risk of dissipation in the present case is heightened by the nature of the cryptocurrency: the Stolen Cryptocurrency Assets are susceptible to being transferred by the click of a button, through digital wallets that may be completely anonymous and untraceable to the owner, and can be easily dissipated and hidden in cyberspace.[26]

55 I also agreed with the plaintiff's submission that the first defendants likely would not have sufficient assets in Singapore to satisfy an award for damages. Primarily, this was because the value of the plaintiff's claim is in excess of US$7m, while less than US$1m worth of the Stolen Cryptocurrency

---

25 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 55(b).

26 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 55(c).

Assets are known to have been transferred to digital wallets owned by the second and third defendants, which have operations in Singapore. Moreover, it was also unlikely that the first defendants would hold all of their remaining ill-gotten gains in Singapore.[27]

56 Hence, I granted the worldwide freezing injunction sought by the plaintiff to restrain the first defendants from dealing with, disposing of, or diminishing the value of, their assets up to the value of US$7,089,894.68, being the value of the Stolen Cryptocurrency Assets.

Disclosure orders

57 The plaintiff sought the following ancillary disclosure orders requiring the second and third defendants to disclose to the plaintiff:[28]

(a) the current balances of the second and third defendants' accounts that were credited with the 15.0 BTC and 0.3 BTC respectively, that are traceable to the Stolen Cryptocurrency Assets;

(b) information and documents collected by the second and third defendants in relation to the owners of the relevant accounts in the second and third defendants; and

(c) details of all transactions involving the relevant accounts in the second and third defendants from the dates on which the stolen assets were credited against the accounts.

---

27 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 56.

28 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 60.

58 As stated by the court in *Sun Electric Pte Ltd and another v Menrva Solutions Pte Ltd and another* [2020] 4 SLR 978 at [81], the source of the statutory power to grant interlocutory relief is s 4(10) of the Civil Law Act (Cap 43, 1999 Rev Ed). Hence, the power to grant disclosure orders ancillary to a freezing injunction originates from the same provision.

59 The plaintiff made submissions on the basis that the ancillary disclosure orders sought were *Bankers Trust* orders (from the case of *Bankers Co Trust v Shapira* [1980] 1 WLR 1274 ("*Bankers Trust*")), which were orders compelling *non-parties* to provide documents to assist with the applicant's tracing claim where there was a *prima facie* case of fraud: *Success Elegant Trading Ltd v La Dolce Vita Fine Dining Co Ltd and others and another appeal* [2016] 4 SLR 1392 at [26].[29] In my decision, it was unnecessary to consider such principles given that the second and third defendants *are* parties to the present dispute. The court was therefore empowered by s 4(10) of the Civil Law Act to grant interlocutory relief "either unconditionally or upon such terms and conditions as the court thinks just, in all cases in which it appears to the court to be just or convenient that such order should be made".

60 In the present case, I was of the view that the disclosure orders sought were just and convenient. The plaintiff required the information sought to understand what remained of the stolen assets that were transferred to the second and third defendants, the extent that they have been transferred to other persons or accounts, as well as the whereabouts of such assets. The information sought would also facilitate the identification of the first defendants, or any

[29] Plaintiff's Skeletal Submissions dated 4 June 2021 at para 63.

persons that may have assisted or acted in concert with them.[30] I therefore granted the ancillary disclosure orders sought by the plaintiff.

SUM 4880

61 As a result of the plaintiff's subsequent investigations and disclosure by the second and third defendants, he managed to identify two persons, CPZ and CQA, within the first defendants. In SUM 4880, heard on 9 November 2021, he sought leave to join these two persons as the fourth and fifth defendants to the action. Accordingly, he also sought leave to amend the Writ of Summons to, *inter alia*, include claims against these two defendants.[31]

62 The plaintiff also discovered that further portions of the Stolen Cryptocurrency Assets had been dissipated to a cryptocurrency exchange and a digital payment services company:[32]

> (a) First, the plaintiff traced 0.0996 BTC of Stolen Cryptocurrency Assets that had been withdrawn from the third defendant's account. The plaintiff discovered that approximately 0.08432778 BTC traceable to the 0.0996 BTC withdrawn from the third defendant's account was ultimately transferred to digital wallets owned and controlled by CQB, via three transactions between 29 June 2021 and 10 July 2021. CQB is a United States incorporated entity that maintains a cryptocurrency exchange.

---

30 Plaintiff's Skeletal Submissions dated 4 June 2021 at para 65.

31 Plaintiff's Skeletal Submissions dated 29 October 2021 at paras 6 to 13 and 51; Writ of Summons (Amendment No 1), Annex A.

32 Plaintiff's Skeletal Submissions dated 29 October 2021 at para 14.

(b) Second, the plaintiff's tracing of the 0.0996 BTC also revealed that a further 0.00685635 BTC which are traceable to the 0.0996 BTC withdrawn from the third defendant's account was ultimately transferred to a digital wallet owned and controlled by CQC via one transaction on 13 July 2021. CQC is a United States incorporated entity which provides financial and digital payment services.

(c) Third, the plaintiff also discovered that a further 0.64360035 BTC of the Stolen Cryptocurrency Assets had been transferred to digital wallets that are associated with the second defendant, via three transactions between 13 October 2021 and 14 October 2021.

63 The plaintiff therefore sought leave in SUM 4880 to join CQB and CQC as the sixth and seventh defendants to the action. Similar to the second and third defendants (see [8] above), the plaintiff believed that the sixth and seventh defendants are innocent third parties and asserted no substantive claims against them apart from disclosure.[33]

64 The plaintiff also applied for leave to serve the cause papers and relevant documents on the fourth to seventh defendants (the "additional defendants") out of jurisdiction. Specifically, for the fourth and fifth defendants, the plaintiff applied for leave to serve them by way of email, *ie*, via substituted means.

Joinder and amendment of writ

65 Under the ROC, O 15 r 4(1) provides that any person may be joined to the action if: (a) there exists a common question of law or fact that would arise in the event that separate actions are commenced against the defendants; and

[33] Plaintiff's Skeletal Submissions dated 29 October 2021 at para 15.

(b) all the plaintiff's rights to relief against both defendants arise out of the same transaction or series of transactions.

66 In my view, it was clear that common questions of law and fact will arise in separate claims against the first defendants and the additional defendants.

(a) First, the documentary evidence, which largely consisted of the registration details and transaction history of the relevant accounts disclosed by the second and third defendants and another cryptocurrency exchange,[34] showed that the fourth and fifth defendants were involved in the transfers of assets traceable to the Stolen Cryptocurrency Assets in rather suspicious circumstances. Hence, they were persons identified from the group of unknown persons constituting the first defendants. The plaintiff's claims against the fourth and fifth defendants include a claim that they had unlawfully conspired with the first defendants to cause loss to the plaintiff by way of the theft, and/or had dishonestly assisted the first defendants with the theft. Hence, common questions of law and fact would arise as to whether the theft had occurred in the first place, and whether the defendants have any factual or legal basis to retain the stolen assets.[35]

(b) Second, the sixth and seventh defendants were similar to the second and the third defendants in that they were entities whose accounts were involved in the transfer of assets traceable to the Stolen Cryptocurrency Assets.[36] Also, the plaintiff's right of disclosure against

---

34 Plaintiff's Skeletal Submissions dated 29 October 2021 at paras 8 and 9; Plaintiff's 2nd Affidavit dated 6 August 2021 at paras 13 to 30, DH-15 to DH-19.

35 Plaintiff's Skeletal Submissions dated 29 October 2021 at para 21(a).

36 Plaintiff's Skeletal Submissions dated 29 October 2021 at Annexes A to C.

> the sixth and seventh defendants was predicated on, *inter alia*, the plaintiff's proprietary interest in the assets transferred to them, which was a crucial element in the plaintiff's proprietary claim against the first defendants for the Stolen Cryptocurrency Assets.[37]

67 Moreover, it was eminently clear that the plaintiff's rights to relief against the additional defendants all arose out of the same transaction vis-à-vis the existing defendants, *ie*, the theft and dissipation of the Stolen Cryptocurrency Assets.

68 Hence, the requirements under O 15 r 4(1) were satisfied and I granted the plaintiff's joinder application. Accordingly, I also granted the plaintiff leave to amend the Writ of Summons to include claims against the fourth and fifth defendants, pursuant to O 20 r 5(1).

Service out of jurisdiction

69 The plaintiff applied for leave to serve the cause papers and relevant documents on the fourth to seventh defendants out of jurisdiction.

70 As stated by the Court of Appeal in *Zoom Communications Ltd v Broadcast Solutions Pte Ltd* [2014] 4 SLR 500 ("*Zoom Communications*") at [26], three requirements must be satisfied before leave to serve out of jurisdiction is granted:

> (a) the plaintiff's claim must come within one of the heads under O 11 r 1 of the ROC;
>
> (b) the plaintiff's claim must have a sufficient degree of merit; and

---

37 Plaintiff's Skeletal Submissions dated 29 October 2021 at para 21(b).

(c) Singapore must be the proper forum for the trial of the action.

71 With regard to the first requirement, the sixth and seventh defendants have wholly owned subsidiaries in Singapore, and they therefore have assets in Singapore in the form of shares in the Singapore subsidiaries.[38] Hence, the requirement under O 11 r 1(a) of the ROC that the person is domiciled, ordinarily resident, carrying on business or has property in Singapore is satisfied. As for the fourth and fifth defendants, O 11 r 1(c) provides that service out of jurisdiction is permissible where "the claim is brought against a person duly served in or out of Singapore and a person out of Singapore is a necessary or proper party thereto". In this regard, a person is a "proper party" if, had he been within the jurisdiction, he would have been properly joined as a defendant pursuant to O 15 of the ROC (*J H Rayner (Mincing Lane) Ltd v Teck Hock and Co (Pte) Ltd and others* [1989] 2 SLR(R) 683 at [17]–[19]; *White Book* at para 11/1/19). This was the case here (see [65]–[68] above).

72 With regard to the second requirement, the plaintiff has to show that there is a serious question to be tried on the merits of the claim (*Bradley Lomas Electrolok Ltd and another v Colt Ventilation East Asia Pte Ltd and others* [1999] 3 SLR(R) 1156 at [19]–[20]). In my view, this threshold was met. The documents disclosed by the second and third defendants reveal that the accounts registered by the fourth and fifth defendants were likely created for the sole purposes of dissipating the stolen assets, which suggests that the fourth and fifth defendants were likely to have been amongst the conspirators who had planned to and did indeed steal the Stolen Cryptocurrency Assets from the plaintiff.[39] As for the sixth and seventh defendants, which are a cryptocurrency exchange and

---

38 Plaintiff's Skeletal Submissions dated 29 October 2021 at para 36.

39 Plaintiff's Skeletal Submissions dated 29 October 2021 at para 45.

a digital payment services company respectively, the plaintiff would have a meritorious claim in seeking disclosure of relevant information against them, just as they did against the second and third defendants (see [57]–[60] above).

73 As for the last requirement, the plaintiff bears the burden of proving that Singapore is the proper forum (*Zoom Communications* at [71]–[75]). In this regard, as set out in *Spiliada Maritime Corporation v Cansulex Ltd* [1987] AC 460 (affirmed in *Siemens AG v Holdrich Investment Ltd* [2010] 3 SLR 1007 ("*Siemens AG*") at [5]–[6]), the courts will assess whether Singapore is the most appropriate forum to hear the substantive dispute, by considering what factors there are which point in the direction of Singapore as the appropriate forum. The following statements by the Court of Appeal were instructive (*Siemens AG* at [4], [7] and [8]):

> 4 … The purpose of the *forum conveniens* analysis is to identify the most appropriate forum in which to try the substantive dispute. It is wrong to say that Singapore is *forum non conveniens* simply because the connecting factors which point to Singapore are outweighed by all the connecting factors which point away from Singapore. The connecting factors which point away from Singapore must point to a more appropriate forum than Singapore, and they might not do so if those connections are dispersed amongst several jurisdictions. Quite simply, Singapore is *forum non conveniens* only if there is a more appropriate forum than Singapore.
>
> …
>
> 7 However, in recognition of the primarily territorial nature of the court's jurisdiction, the court begins with the location of the defendant when it decides whether it has jurisdiction over a dispute – thus, jurisdiction over a defendant who is within the territory is as of right, while jurisdiction over a defendant who is outside the territory is discretionary. In this sense, there is a burden – *viz*, the burden of displacing the *prima facie* weight given to the location of the defendant. But, despite the use of the term, the burden is not strictly one of proof. Instead, the burden is one of demonstrating the normative weight to be given to each connecting factor in the light of all the circumstances of the case. The ease of discharging the burden would similarly depend on the facts of

> each case – again, as Lord Goff himself noted in *Spiliada* (at 481), the circumstances described in the English equivalent of our O 11 r 1 are "of great variety, ranging from cases where … the discretion would normally be exercised in favour of granting leave … to cases where the grant of leave is far more problematical". In the same vein, Lord Goff also remarked (at 481) that the importance to be attached to any particular ground invoked by the plaintiff in seeking leave for service out of jurisdiction might vary from case to case.
>
> 8 Separately, we do not think that it is necessary for a plaintiff who seeks leave for service out of jurisdiction to show that Singapore is "clearly" the *forum conveniens* if, by this, it is meant that Singapore must be not only the most appropriate forum in the final analysis, but also the most appropriate forum by far. No doubt, there will be cases where the *forum conveniens* is clear beyond contest. But, in the case of an international dispute where the connecting factors are finely balanced, a requirement that there must be a forum which is clearly the most appropriate forum would necessarily condemn the dispute to jurisdictional limbo. Such a result does the doctrine of *forum non conveniens* no credit. In our view, therefore, *it is sufficient for a plaintiff seeking leave for service out of jurisdiction to show that Singapore is, on balance and in the final analysis, the most appropriate forum to try the dispute, and it matters not whether Singapore is the most appropriate forum by a hair or by a mile.*
>
> [emphasis in original omitted; emphasis added in italics]

74 In my decision, I placed much weight on: (a) the fact that the second and third defendants are based in Singapore and have complied with disclosure orders; and (b) the fact that the sixth and seventh defendants have wholly owned subsidiaries in Singapore and were likely to comply with disclosure orders. They were sufficient to show that Singapore was the most appropriate forum even though the fourth and the fifth defendants are foreign nationals.

75 Hence, I granted the plaintiff's application for leave to serve the cause papers and relevant documents on the additional defendants out of jurisdiction.

Substituted service out of jurisdiction

76 The plaintiff applied to serve the cause papers and relevant documents on the fourth and fifth defendants by way of email.

77 Pursuant to O 11 r 3(1) read with O 62 r 5 of the ROC, the court may grant leave for substituted service out of jurisdiction (*Petroval SA v Stainby Overseas Ltd and others* [2008] 3 SLR(R) 856 ("*Petroval*") at [26]). Under O 62 r 5(1), substituted service may be ordered where "it appears to the Court that it is *impracticable for any reason* to serve that document personally on that person" [emphasis added]. Order 11 r 3(1) then provides, *inter alia*, that O 62 r 5 "shall apply in relation to the service of an originating process out of Singapore".

78 In *Petroval*, in allowing substituted service, the court had regard to the impracticality of effecting personal service on the defendants and the effectiveness of the chosen mode of substituted service in notifying the defendants of the Singapore action and the Singapore order (*Petroval* at [26]). Similarly, I found that these considerations were present on the facts.

79 First, it was impractical to serve the cause papers in the present action on the fourth and fifth defendants personally, as their physical whereabouts are presently unknown.[40] Moreover, it was unlikely that they would agree to come forward to accept service willingly. The plaintiff had previously served the injunction and disclosure order on the first defendants via the fourth and fifth defendants (who were unnamed and part of the first defendants prior to this application). However, the fourth and fifth defendants did not respond to the emails effecting service. Also, both the fourth and fifth defendants had used

[40] Plaintiff's Skeletal Submissions dated 29 October 2021 at para 55.

Virtual Private Network services to obscure the locations from which they had accessed their accounts in the second and third defendants, seemingly to avoid being located physically in the event that their identities are uncovered.[41]

80 Second, sending the cause papers and relevant documents to the fourth and fifth defendants' email addresses would likely bring the present suit to their attention, as they had recently used these email addresses less than five months ago to register their accounts. There was also evidence that the fourth defendant had used her email address as recently as June 2021.[42]

81 Third, and in my view this was the most important reason, the accounts in the second and third defendants were opened by the fourth and fifth defendants via email. Although the identity documents provided showed their physical addresses,[43] it does not seem that the onboarding process involved verification of the veracity of those physical addresses. The operative contact point was always their email addresses as all communications between them were done by way of email. It was clear that service by email would most certainly bring the Writ to the attention of the account holders, *viz*, the fourth and fifth defendants.

82 In the circumstances of the present case, I was of the view that the only practical means by which the plaintiff could effect service on the fourth and fifth defendants was by way of email and that that mode of service would bring the Writ to the notice of those defendants. Hence, I dispensed with the requirement of two prior reasonable attempts at personal service under para 33(2) of the

---

41 Plaintiff's Skeletal Submissions dated 29 October 2021 at para 56.

42 Plaintiff's Skeletal Submissions dated 29 October 2021 at paras 57 and 58.

43 Plaintiff's 2nd Affidavit dated 6 August 2021 at pp 46 and 74.

Supreme Court Practice Directions and granted the plaintiff's application for leave to serve the fourth and fifth defendants via substituted means, *viz*, by way of email.

Conclusion

83 For the above reasons, I granted the plaintiff's applications in SUM 2444 and SUM 4880, with minor corrections as to the phrasing of the prayers in SUM 4880.

84 As for costs, they are to be in the cause.

Lee Seiu Kin
Judge of the High Court

Ong Tun Wei Danny, Chow Chao Wu Jansen and Yap Zhe You Ryo
(Rajah & Tann Singapore LLP) for the plaintiff;
The defendants absent and unrepresented.