Hartley M.K. West (CA Bar No. 191609)
KOBRE & KIM LLP
150 California Street, 19th Floor
San Francisco, California 94111
Hartley.West@kobrekim.com
Telephone: 415-582-4800
Facsimile: 415-582-4811

Benjamin J. Sauter (*pro hac vice*)
Daniel J. Saval (*pro hac vice*)
KOBRE & KIM LLP
800 Third Avenue
New York, NY 10022
Benjamin.Sauter@kobrekim.com
Daniel.Saval@kobrekim.com
Telephone: (212) 488-1200
Facsimile: (212) 488-1220

Attorneys for Petitioners

UNITED STATES BANKRUPTCY COURT

NORTHERN DISTRICT OF CALIFORNIA

In re: Dooga Ltd.,

Debtor in a Foreign Proceeding.

Chapter 15

Case No. 20-30157

DECLARATION OF RICHARD A. SANDERS

I, Richard A. Sanders, pursuant to 28 U.S.C. § 1746, hereby declare under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

1. My name is Richard A. Sanders. I am a Co-Founder and Lead Investigator of CipherBlade, a blockchain forensics and cybercrime investigative firm which consults on some of the most renowned blockchain projects, as well as numerous law enforcement and regulatory investigations, and provides advisory services to cryptocurrency exchanges and other organizations. Prior to co-founding CipherBlade, I was in the United States Army, where I attained the rank of a Staff Sergeant and spent 12 years as a forward observer and PSYOP specialist. A copy of my C.V. is annexed as Exhibit 1.

2. CipherBlade and the CipherBlade staff have experience in some of the most well-known cryptocurrency investigations, including hacks of prominent individuals, in which I served as a lead investigator, gathering evidence which led to the identification, arrest, and prosecution of a notorious theft ring. The takedown of the aforementioned ring is one example in a long resume of accomplishments for the CipherBlade team. There are few experts in the field with expertise in most, let alone all, of the subjects relevant to my duties, which include blockchain forensics, cryptocurrency AML, and cryptocurrency cybercrime investigation.

3. In addition to my duties with CipherBlade, I serve as a volunteer with Crypto Defenders Alliance ("CDA") where I was selected as one of their four administrators due to my demonstrated expertise as a blockchain forensics expert, cybercrime investigation knowledge, and leadership. CDA is an organization with representatives from nearly all major cryptocurrency exchanges and services, with the purpose of combating laundering of illicitly obtained funds. CDA has been a core component in the prevention of laundering of illicitly-obtained funds from many significant cryptocurrency hack and scam situations, as well as numerous major cryptocurrency exchange hacks. My duties within CDA, as well as my duties within CipherBlade, entail on a daily basis determining terminal destinations of stolen cryptocurrency and consulting with legal and law enforcement professionals on the investigative and recovery process.

4. I have been asked by Kobre & Kim on behalf of Dooga Ltd., the Liquidator of Cubits, to analyze the flow of cryptocurrency out of certain Cubits accounts involved in a theft event on February

5, 2018 (the "February 2018 Theft") and to provide this declaration reporting my findings on the connection between the February 2018 Theft and certain cryptocurrency wallets.

5. As set forth below, my investigation has traced the transmittal of value from Cubits' stolen assets into accounts at two U.S. based cryptocurrency exchanges, and therefore I believe that the balances in those accounts represent assets stolen from Cubits.

A. Background on Cryptocurrency and Cryptocurrency Laundering Methodologies

6. Cryptocurrencies are digital representations of value that are secured through cryptography, the enciphering and deciphering of messages in secret code or cipher. Many of them rely on blockchain technology—a distributed ledger of all transactions that is decentralized and unable to be changed under most circumstances. The most well-known form of cryptocurrency is Bitcoin, but there are a number of cryptocurrencies that have been introduced in the past several years, more than 2,000 by some counts. Cryptocurrency is sent and received from or to so-called "wallets," which are locations identified by a combination of letters and numbers called a hash (*e.g.*, 1HpCnC37CQepiL1qwogoZzriGxtishEC6j) that is unique to the holder of the "key" for that wallet address. Wallets are roughly analogous to an email address or bank account. They are a unique and secure identifier that allows for the transmission of cryptocurrency from one user to another.

7. Bitcoins are completely fungible and are not serialized or labeled like, for example, individual dollar bills. As a result, it is impossible to state that any particular Bitcoin is the subject of any specific transaction at any specific time. Instead, a Bitcoin transaction is best understood as a unit of value being transferred from one wallet to another. The blockchain is the record of all such transactions over time. For that reason, as explained more below, to "follow the money" after a theft of a particular amount of Bitcoin, one has to follow the value being transmitted from wallet to wallet, rather than attempting to focus on any "specific" Bitcoin.

8. With the rise in popularity of cryptocurrencies, there have inevitably been a number of thefts of cryptocurrency. Indeed, as noted above, I and my firm CipherBlade have been retained by private parties and law enforcement alike to assist and investigate in the aftermath of many of these hacks and thefts. These thefts commonly occur when a user's account or wallet is compromised (for

example, by theft or hacking of a password or key), and value is transferred out of the account or wallet to other wallets.

9. Following a theft, the culprits often attempt to launder the proceeds of their criminal activity to make it more difficult to trace, through several means. The first is using a cryptocurrency "mixer" or "blender." This is essentially an intermediary service that will take in cryptocurrency from many sources and distribute it back out in differing amounts to one or several accounts controlled by the thieves. The source for these funds will differ from the initial deposit from the user; funds are deposited into a "mixing pool" combining other users' deposits in the mixing service. For example, if a criminal were to steal 5 Bitcoins and give them to a blender, the blender may then output 2 Bitcoins to one account controlled by the thief, 2 Bitcoins to a second account, and 1 Bitcoin to a third. By breaking up the amounts and distributing them to several different wallets with varied sources, it becomes more difficult to determine where the stolen value has gone. Blenders are, in a very real sense, tailor made and designed to engage in money laundering.

10. Cryptocurrency thieves also engage in so-called "chain hopping" to launder the proceeds of thefts. As noted above, the ownership of cryptocurrency is known to anybody who has visibility into that cryptocurrency's blockchain—the ledger of who owns how much of a cryptocurrency. However, users can exchange one cryptocurrency for another, making tracing the value more difficult. For example, a thief can exchange a stolen Bitcoin for twenty Ethereum coins, with the stolen value now being present in the Ethereum blockchain, not the Bitcoin blockchain. An example of how a third party would do this is depositing Bitcoin on a cryptocurrency exchange, trading that Bitcoin for Ethereum, and withdrawing the Ethereum to a wallet they control. Without getting information from the exchange itself, an investigator will only be able to follow the blockchain trail to that exchange and would not know what cryptocurrency trades or withdrawals took place within or between the user's exchange wallet(s). This "chain hopping" technique is also often used to make it more difficult and time consuming to ascertain where the value of stolen cryptocurrency has been transmitted.

B. My Work Tracing the Proceeds of the February 2018 Theft

11. In April of 2020, I was retained to analyze the location of assets that I understand were stolen from Cubits in February 2018 (the "February 2018 Theft"), and attempt to find the terminal

destination of these assets. To perform this task, I was aided by information provided by certain exchanges that had been subpoenaed by the Foreign Representatives as part of this proceeding. In making my assessments, I also relied on my independent analysis and expertise and experience in blockchain forensics.

12. Blockchain forensics is an evolving science that requires a multi-faceted approach: access to technological resources and insight into the functioning of the cryptocurrency world and its players. To perform the analysis, I used best-in-class technological tools such as Chainalysis Reactor (the most well-known blockchain forensics tool), CipherTrace, or our own proprietary in-house tools. These tools allow an investigator to see relationships between cryptocurrency wallets by tracking the flows of value between various locations, permitting the investigator to generate a graphical representation of the flow of funds that can reveal relationships and laundering methodologies. Building on these tools, I used my extensive experience as a cryptocurrency investigator, which provided key context to understand the flows of cryptocurrency within the system and recognize laundering methodologies used by cybercriminals.

13. My investigation started with the following wallet addresses, which were the ones that had been used to receive the stolen Bitcoin directly from Cubits on February 5, 2018:

[redacted]

14. From there, I traced flows from these wallets in an attempt to tie them to known destinations.

C. Relationship Between the February 2018 Theft and Coinbase Accounts Associated with [redacted]

15. One focus of my investigation was a number of accounts at a cryptocurrency exchange called Coinbase, which, according to subpoena responses from Coinbase, are purportedly owned by an individual named [redacted]. I understand that [redacted], [redacted] [redacted] I also understand that there are a number of details that link [redacted] to the February 2018 Theft and make it likely that his cryptocurrency accounts, including his accounts at Coinbase, would be receiving funds stolen from Cubits.

16. My review has found links between [redacted] Coinbase accounts and cryptocurrency wallets that initially received the stolen funds from Cubits. Put differently, a straight line of value transfer can be traced from the Cubits theft to [redacted], notwithstanding attempts at money laundering transactions in the middle.

17. To begin, I analyzed the flows from one of the initial receiving wallets, [redacted]. Using blockchain forensic techniques, it became clear that funds were being moved from account to account in a laundering methodology, and these accounts ultimately deposited nearly [redacted]. At the time of the February 2018 Theft, 26 Bitcoin would have had a value of more than $260,000. A graphical representation of this movement is below:

[redacted]

18. The quantity of intermediary wallets between the initial theft wallet and terminal destination in my analysis is very small for thefts of cryptocurrency. In my experience, it is rare to have such a minimal number of "hops" between wallets to demonstrate a flow of funds in a case of this nature. The fact that three of [redacted] Coinbase accounts can be so closely tied to the wallets initially receiving the stolen Cubits funds demonstrates to me that the funds received by [redacted] are very likely to be the proceeds of the Cubits theft.

19. In addition, the wallet address immediately preceding the distribution to [redacted] appears to have previously received funds from other well-known cryptocurrency theft events. In other words, the assets from Cubits appear to have been run

through a pre-existing system for laundering the proceeds of illicit activity (largely and specifically, activity with known shared laundering actors), and then transmitted to [redacted].

20. There are also further indicia of illicit activity in [redacted] accounts related to the Cubits theft. For example, one of [redacted] This confirms that the funds directed to [redacted] are derived from a well-established laundering system.

21. The amount of the inflows that can be directly tied to the Cubits theft—nearly 26 Bitcoin valued at more than $260,000 in February 2018—exceeds the current balance of [redacted], corresponding to [redacted] In my assessment, the value of likely stolen Cubits assets directed to [redacted] exceeds their present balance, and so the entirety of the present balance represents value derived from Cubits assets.

D. Relationship Between the February 2018 Theft and Certain Bittrex Wallet Addresses

22. My review also identified links between the initial wallets containing Cubits' stolen assets and certain accounts at another U.S.-based cryptocurrency exchange, Bittrex.

23. These wallets show significant evidence of money laundering activity, and, in my assessment, are likely tied to illicit activity. For example, one of the wallets, [redacted]

[redacted] This is a textbook example of the “chain hopping”.

24. The other target Bittrex wallet, [redacted] Here too, the transaction activity clearly reflects indicators of money laundering and chain-hopping.

25. In addition to these red flags of criminal activity, there are clear connections between Cubits’s stolen funds and these accounts. As with [redacted], there is a line of value transfer from the initial wallets containing Cubits’ stolen Bitcoins to the two Bittrex wallets, shown below:

[redacted]

26. The value transfer to these accounts—[redacted] As a result, the value of stolen Cubits assets directed to those accounts exceeds their current balance.

E. Conclusion

27. For the reasons set forth above, it is my assessment that the [redacted] is exceeded by the value of stolen Cubits assets directed to his Coinbase accounts, and that therefore the value in these accounts is attributable to stolen Cubits assets.

28. Similarly, it is my assessment that the balance in two Bittrex accounts, [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] is exceeded by the value of stolen Cubits assets directed to these accounts, and that therefore the value in these accounts is attributable to stolen Cubits assets as well.

Executed this 7th day of October 2020.

Richard A. Sanders