EXHIBIT B

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

HASH ASSET MANAGEMENT LTD., TAF CAPITAL PTY LTD, as trustee for the BLUEBOTTLE FUND, and NI KAIHAO, Plaintiffs, v. DMA LABS, INC., ICHI FOUNDATION, NICK POORE, and BRYAN GROSS, Defendants.	CASE NO. **DECLARATION OF PAUL SIBENIK**

I, Paul Sibenik, pursuant to 28 U.S.C. § 1746, declare as follows:

1. I have conducted an investigation concerning the collapse of a cryptocurrency ‘liquidity pool’ known as Rari Pool 136, which was created by and associated with the ICHI Foundation.

2. More specifically, I have assessed if there is reason to believe whether the founders of the ICHI Foundation and/or those closely associated with them, including DMA Labs Inc., maybe have either been behind or played a role in the collapse of Rari Pool 136 itself for their own financial gain. Additionally, I have assessed whether there is any indication of insider trading by individuals that were part of or associated with the ICHI Foundation (the “ICHI Team”).

3. I am the Lead Case Manager at CipherBlade, a leading blockchain forensics and cybercrime investigative firm which consults with blockchain projects, numerous police, law enforcement and regulatory agencies around the world, including the US FBI and US Secret Service, cryptocurrency exchanges, and other organizations. Other CipherBlade staff and I have experience in some of the most high-profile cryptocurrency investigations to date in relation to a wide range of niches including but not limited to cases involving hacking, theft, SIM-Swapping, ransomware, different types of frauds and scams (e.g., involving ICOs, NFTs,

investment fraud, Ponzi Schemes), 'rugpulls,' embezzlement, as well as civil matters such as divorce cases and bankruptcy cases. I am recognized as one of the few experts in blockchain forensics and cryptocurrency cybercrime investigation. This work regularly requires the analysis of cryptocurrency transactions, wallets, and addresses, alongside gathering and analyzing other data sources.

4. In my work, I frequently analyze cryptocurrency transactions and addresses often but not always involving one or more of the investigative niches previously mentioned. Using a variety of forensic techniques, Bitcoin ("BTC") and Ether ("ETH") can be tracked, and assessments can be made to associate wallets and addresses with one another, which enables an investigator like me to discern control or ownership of a given wallet or address, by comparing and cross-referencing public blockchain data with other data sources. I am regularly instructed to track cryptocurrency, and in particular, identify money laundering in my investigations. Individual(s) laundering funds often lack understanding regarding just how cryptocurrency can be tracked; they often "make mistakes" when laundering funds, and it effectively allows me to identify control of given cryptocurrency wallets and addresses. The number of transactions involved is often in the hundreds or even thousands in each case, particularly when the cryptocurrency is broken up into smaller denominations in an attempt to obfuscate the flow of funds.

5. I regularly use blockchain forensics software to assist me in blockchain investigations. In this case, as part of the scope of this declaration, I have utilized Chainalysis Reactor, which is the leading blockchain forensics software available and is utilized by various law enforcement agencies around the world, including the FBI, Secret Service, DHS, and DEA in the United States. Chainalysis Reactor helps professionals to better understand the flow of funds on assets on the Ethereum blockchain (in addition to a variety of other blockchains that Reactor supports, such as Bitcoin). It helps to aggregate and manage large amounts of transaction data and addresses to make the data more parsable. It helps professionals like me to better understand which addresses are under the control of the same individuals or entities, and

for addresses that are under the control of a service or exchange, it is often able to identify the name of that service or exchange. Furthermore, Chainalysis Reactor also provides Open-Source Intelligence (OSINT) on various cryptocurrency addresses, which can help investigators understand what those addresses may be associated with or can provide additional context in situations. I have a Chainalysis Reactor Certification (CRC), which is a certification offered by Chainalysis to certify knowledge and understanding of their Reactor forensics tool. I also have the Chainalysis Investigation Specialist Certification (CISC), an additional certification by Chainalysis designed specifically for the most advanced Reactor users, which dives deep into advanced investigative techniques and obfuscation approaches sometimes used by individuals trying to launder ill-gotten cryptocurrency. I furthermore have the Chainalysis Ethereum Investigations Certification (CEIC), a certification program focused on Ethereum, as well as other EVM (Ethereum virtual machine)-compatible cryptocurrencies.

6. Additionally, a large portion of my work involves consulting with blockchain companies in various capacities pertaining to preventative measures they can or should take to reduce risks and mitigate the amount of cybercrime that their company is exposed to. This involves consulting on security practices, including those pertaining to cryptocurrency storage and management. This also involves consulting on matters of compliance so as to significantly mitigate the likelihood and/or frequency of ill-gotten funds being laundered through their service and reduce the amount of various types of fraud, including investment scams, romance scams, impersonation scams, and money muling.

7. A copy of my CV is attached in Appendix A.

8. I have provided some relevant definitions in Appendix B.

9. I reserve the right to amend the views expressed in this declaration should any additional evidence be disclosed at a later stage.

10. Prior to accepting instructions to act in this matter, I made reasonable inquiries to identify any actual or potential conflicts of interest in connection with the parties concerned. No matters arose.

11. Rari Pool 136 was built using Fuse protocol, which is a permissionless protocol.[1] The protocol allows individuals and teams to create 'pools' consisting of cryptocurrency deposits of various depositors. However, pool creators and operators (including the ICHI Team) must design and specify various parameters of the pool. It is critically important for 'pools' to be designed in a sound and secure manner to prevent an exploit or undue manipulation from happening.[2]

12. It is evident that a series of design flaws in the Rari Pool 136 existed.

13. Many of these flaws that increased the risk of collapse include but are not limited to:

a) An 85% Loan-to-value (LTV) ratio.

b) Users were permitted to deposit an unlimited amount of ICHI tokens as collateral to borrow stablecoins.

c) There was no supply cap on the amount of assets that could be deposited into Rari Pool 136.

14. The collapse of Rari Pool 136 came about because select user(s) came up with and utilized the following scheme to make money:

a) First, the cryptocurrency issued by the ICHI Team, ICHI, were deposited into the Rari Pool 136 and used as collateral.

b) Second, select user(s) would then borrow stablecoins from the pool.

c) Third, the stablecoins acquired could then be used to buy more ICHI. This would naturally create demand for ICHI and caused the price of ICHI (relative to USD) to increase considerably.

d) Fourth, ICHI could then also be deposited into the Rari Pool 136 as collateral to borrow even more stablecoins. And the cycle continued thereafter.

[1] https://sports.yahoo.com/news/ichi-tokens-plunged-90-bad-095919003.html.

[2] https://twitter.com/JackLongarzo/status/1513587620198207494.

15. The sustainability of Rari Pool 136 for a short time was made possible by an ever-increasing price of ICHI tokens. The ICHI price increase was caused, in part, by the borrowing of funds from Rari Pool 136 itself. As soon as there wasn't enough buying demand for ICHI to sustain the inflated price, the Rari Pool 136 began to collapse. This quickly led to cascading liquidations of assets in the Rari Pool 136, of which an increasingly large portion of assets had become ICHI.[3] This caused the price of ICHI to collapse further. The price ended up collapsing from ~$142 USD to as low as $1.79, a drop of 99%. The majority of the drop occurred on April 11, 2022.[4]

16. In the paragraphs below, I provide some abbreviated technical evidence that suggests the individual(s) on the ICHI Team, many of whom operated anonymously and are unknown at this time, may have been involved in the exploitation of design flaws of Rari Pool 136 and/or engaged in insider trading with those who were involved. Or both. Exploitation and manipulation of Rari Pool 136 was done for financial gain.

17. There are a variety of different cryptocurrency addresses that are relevant. Below I have listed some of the relevant addresses that are controlled by the ICHI Team, and additionally, I include the reasons why such addresses are controlled by the ICHI Team:

a) 0x11111D16485aa71D2f2BfFBD294DCACbaE79c1d4

Description: Legacy ICHI Deployer / ICHI.farm deployer

Summary: This address deployed the legacy ICHI token contract 0x903bef1736cddf2a537176cf3c64579c3867a881 in transaction 0x9b1e9353dca3301faa911b5073c751a8195c66c4bdfa2d34ddc7b9ba1c3c385d and is labeled as 'ICHI.farm deployer' on Etherscan. Since the ICHI Team created the ICHI token (and ICHI token contract) and since 0x11111D16485aa71D2f2BfFBD294DCACbaE79c1d4 is responsible for doing this,

[3] As well as XICHI and LP tokens.

[4] https://www.coingecko.com/en/coins/ichi.

0x11111D16485aa71D2f2BfFBD294DCACbaE79c1d4 is controlled by someone (or multiple people) on the ICHI Team.

b) 0xC30220fc19e2db669eaa3fa042C07b28F0c10737

Description: New ICHI Deployer

Summary: Listed as 'ICHI: Deployer' on Etherscan. Created numerous ICHI contracts including 'ICHICompositeOracle.'[5] Sent a transaction to 'ICHI Deployer 2 (0xbf1bfd4352564eca6b7b1a2f0169b1081f73cf03),' which in turn created the new ICHI token contract (0x111111517e4929D3dcbdfa7CCe55d30d4B6BC4d6).

c) 0x0dd4C0c16Fff6693e169Ef89235Cb92F9D8943EE

Description: ICHI Deployer 1

Summary: Labelled as 'ICHI: Deployer 1' on Etherscan. This address is supposedly controlled by the CTO of ICHI, who goes by the name '37aces.'[6] The address also previously held the ENS domain '37aces.eth.'[7]

d) 0x94A5980d5634533551dcB7108322f6C4f2a80E6B

Description: ICHI Multisig

Summary: Labelled as 'ICHI Multisig' on Etherscan. This is a Gnosis multisig wallet controlled by member(s) of the ICHI Team.

e) 0x8f3c97DdC88D7A75b8c3f872b525B30932D3014c

Description: Rari Pool 136 admin

Summary: 0x8f3c97DdC88D7A75b8c3f872b525B30932D3014c is listed as the 'admin' of Rari Pool 136 on Rari capital's website.[8] It was created by 0x7b7B9e93CDAc35bba1927FCE27c156D83488ab60. Collectively, the two addresses send

[5] https://ww6.etherscan.io/address/0x6f85eb17955257a39fd78692f6884ebe6531fd8b#code.

[6] https://forums.dydx.community/account/0x0dd4C0c16Fff6693e169Ef89235Cb92F9D8943EE/.

[7] https://etherscan.io/nft/0x57f1887a8bf19b14fc0df6fd9b2acc9af147ea85/108738658586001166097941560871784711007330529340630702375356477043542709697822.

[8] https://app.rari.capital/fuse/pool/136/info.

and receive multiple transactions from other known ICHI-controlled addresses, including ICHI.farm deployer, ICHI Deployer 1, and New ICHI Deployer. This address is under the ICHI Team's control because the ICHI Team is publicly known to be the owner and operator of Rari Pool 136 and Rari Capital has confirmed this.[9] Thus, since 0x8f3c97DdC88D7A75b8c3f872b525B30932D3014c is the admin of Rari Pool 136, it must therefore be controlled by the ICHI Team.

f) 0x4Fe5f268e5053a05108eBAF13EbD9a825e6fB6f2

Description: ICHI Pool deployer

Summary: Rari Pool 136 is associated with ETH contract address 0xAbDFCdb1503d89D9a6fFE052a526d7A41f5b76D6, and this smart contract was deployed by 0x4Fe5f268e5053a05108eBAF13EbD9a825e6fB6f2. 0x4Fe5f268e5053a05108eBAF13EbD9a825e6fB6f2 receives 4.33 ETH from the ICHI.farm deployer and 2.4 ETH from ICHI Deployer 1. It is publicly known that the ICHI Team created, designed, and operated Rari Pool 136, and thus, 0x4Fe5f268e5053a05108eBAF13EbD9a825e6fB6f2 would be controlled by the ICHI Team. 0x4Fe5f268e5053a05108eBAF13EbD9a825e6fB6f2 is the fourth largest holder of bad debt with $5.64M USD of bad debt.

g) 0xcC50953A743B9CE382f423E37b07Efa6F9d9B000

Description: ICHI Token distributor

Summary: This address was created by the ICHI.farm deployer which is controlled by the ICHI Team. The address was primarily used to distribute small amounts of ICHI.farm tokens to many different users.

18. Before going further, it is important for me to discuss the concept of 'bad debt' and why it's important. The holders of 'bad debt' deposited assets into Rari Pool 136 before the collapse of Rari Pool 136 in order to take out loans. The value of the assets that were held in collateral in Rari Pool 136 collapsed leading to the aforementioned cascading liquidations. But

[9] https://twitter.com/RariCapital/status/1513567245565321232.

for holders with bad debt, the collateral they deposited to Rari Pool 136 ended up not being sufficient to cover their liabilities. This means that holders of bad debt have unjustly benefitted since they ended up not paying back debts that they owe to Rari Pool 136.

19. When a user has some ‘bad debt’ it does not necessarily suggest purposeful exploitation of Rari Pool 136 by those users. In many cases, particularly for addresses with small amounts of bad debt, there is no reason to assume malicious intentions on the part of those users. However, users that managed to accrue a large amount of bad debt (some in the millions of dollars) should be assessed more critically, since it suggests that some of those users could have known that they were exploiting design flaws in Rari Pool 136 and knew it would likely collapse at some point as a result of continuing to leverage ICHI and borrowing stablecoins.

20. Just as critically as having large amounts of bad debt, is how closely connected the addresses of many of the largest ‘bad debt’ holders are on the Ethereum blockchain, oftentimes directly to one another, and at other times to known addresses belonging to the ICHI Team. In my opinion, it’s very suspicious and indicative of insider involvement.

21. Some of the most pertinent addresses that I have identified that are relevant to this matter are indicated in the paragraphs below. Some addresses are likely to be controlled by ICHI Team members, some may be controlled by ICHI Team members, and some may be controlled by individuals or entities ICHI Team members transacted with. Some addresses withdrew significant amounts of stablecoins from Rari Pool 136 in the lead up to its collapse, and some of the addresses listed below could aptly be described as suspicious.

22. 0xc8b5c6363ad036883fc663766ecd87928ad3dc36 ‘0xc8b5’ – this address is the largest holder of bad debt (over $15.4M USD).

a) It received 10 ICHI directly from the ICHI.farm deployer address in transaction 0x11966040c6ec5e30db80b77ad8243aff49de34b3807d70f44dd1406ad94d858f. The reasons for this transfer are unclear. While it is quite a small amount of money, the significance should not be understated. This suggests, at the very least, that the ICHI Team knows and has a relationship with the owner of '0xc8b5.' But it's also distinctly possible that the owner of '0xc8b5' may be part of the ICHI Team.

b) This address received 580 ICHI in transaction 0x4f3c548cf4ccc208611f72bf2659c628075dc9ab91a25d7520012ad2a365c74b from 0x2dddb6a69f071313580073941a4491313303b1ab, which in turn interacts with various known ICHI-controlled addresses, including the ICHI.farm deployer address.

c) There is evidence that suggests that the owner of '0xc8b5' may control a variety of other addresses that also have bad debt. This includes the addresses 0xD1895682591Ac2751b10c11f0124FA46E8471562 and 0x420b02fbb51D65ed2Aa877e8b747160699ae0267. For reference, this information could be utilized to help identify the owner of '0xc8b5' if needed.

d) It is directly connected to many other addresses that also have a significant amount of debt, even if the owner of the '0xc8b5' doesn't control those addresses. The address sent a considerable amount of ICHI to other addresses that have significant bad debts, and those addresses then leveraged ICHI tokens in the same manner. This could be indicative of an insider trading scheme that would have played a critical role in the downfall of Rari Pool 136.

23. 0xFb06EC3296Ae0985f66a72C7efAB5b27618D0D00 – with ~$12.2M USD of bad debt, this is the third largest holder of bad debt. It received 1852 ICHI from directly '0x4fe5' 'ICHI Pool Deployer,' which, as discussed, should be controlled by the ICHI Team. This suggests that 0xFb06EC3296Ae0985f66a72C7efAB5b27618D0D00 could belong to an insider.

24. 0xD1895682591Ac2751b10c11f0124FA46E8471562 'ozgjoker.eth' – This address has a minimal amount of bad debt. However, the owner of this address could be the same as the owner of '0xc8b5' based on blockchain analysis I have conducted. The two addresses interact with each other numerous times. This address owns the ENS domain 'ozgjoker.eth.' I have not found anyone publicly claiming to own the ozgjoker.eth handle, but

a quick Google search reveals someone using the handle ‘ozgjoker’ who appears to be Turkish and claims his name is ‘Özgün Turan Kaynar.’[10]

25. 0x420b02fbb51d65ed2aa877e8b747160699ae0267 – This address has ~$1.29M USD of bad debt. It sends and receives numerous transactions to/from ‘0xc8b5’, and additionally, it sends multiple transactions to the same BTCTurk deposit address that ‘0xc8b5’ and ‘ozgjoker.eth’ sent cryptocurrency to. Thus, the owner of 0x420b02fbb51d65ed2aa877e8b747160699ae0267 could be the same as the owner of ‘0xc8b5.’

26. 0x2dddb6a69f071313580073941a4491313303b1ab – This address has ~$812k USD of bad debt, and it interacts with various known ICHI-controlled addresses, including the ICHI.farm deployer address. It also interacts with ‘0xc8b5.’ This suggests that the address could be controlled by an insider.

27. 0x4ac698cEAEbaa59A1882960727a44E5d42F8e75d – This is a BTCTurk deposit address that ends up receiving a considerable amount of funds associated with the exploit (well into the millions of dollars) from a variety of different addresses that had significant amounts of bad debt, to include ‘0xc8b5’, ‘ozgjoker’eth,’ 0x420b02fbb51D65ed2Aa877e8b747160699ae0267, and 0x71cEC0e5114798F5C369C3Ce931095dACCB17B5C to name a few.

28. 0x639e517d146C8f01d6e20c1B470989Fd778d3602 – An additional BTCTurk deposit address that receives transactions from various addresses with significant amounts of bad debt, including ‘0xc8b5.’ The amount of money involved is noticeably lower than 0x4ac698cEAEbaa59A1882960727a44E5d42F8e75d, however.

[10] https://www.instagram.com/ozgjoker/?hl=bn, https://tr.pinterest.com/ozgjoker/_saved & https://www.youtube.com/playlist?list=PL8KFClGPp7LLv9KpHGk7t72LOJs3zvLMn (webpages have also been archived in case they are deleted). Note that the unused pinterest profile contains the following statement “Can Someone Please Show Me How Deep The Rabbit Hole Goes?” While the rabbit hole idiom originates from Alice in Wonderland, the concept of ‘going down the rabbit hole’ with respect to cryptocurrency is a common expression that cryptocurrency users describe. Additionally, at least one of the videos on the Youtube playlist has a focus on cryptocurrency staking.

29. 0x545683Ae74cFC8845e7033e0B0C91cE6623Dd2a6 – A Binance deposit address that receives transactions from various addresses with significant amounts of bad debt, including 0x591583182fC7D28a52477444dBc597636ac44FBC, 0x71cEC0e5114798F5C369C3Ce931095dACCB17B5C, and 0x0EAd347d565aC2Cf5b42595be53EDF343E52B9d9.

30. Apart from some of the addresses already mentioned, I've included a short list of some of the addresses that '0xc8b5' (which, as mentioned, has connections to the ICHI Team) directly interacts with, which also happen to have notable bad debts:

- 0xd4154916d1330A7eAb4bF3e21295295805A1AB4f (~$13M USD) (second largest holder of bad debt)
- 0x1fc9cd26854dd3b7c74a36424e130887334a993e (~$2.47M USD)
- 0xE4f4d41Bd8DA7AE7e638aEaC9800E67FCd8E2858 (~$3.1M USD)
- 0x0ead347d565ac2cf5b42595be53edf343e52b9d9 (~$1.89M USD)
- 0xD4099Bb6D81E2eA661C6C0417fEC4292D48926Df (~1.52M USD)
- 0x1830955Ba1Ca0a0319857015184E56981ce4877c (~$295k USD)
- 0x591583182fC7D28a52477444dBc597636ac44FBC (~$186k USD)
- 0x71cEC0e5114798F5C369C3Ce931095dACCB17B5C (~$194k USD)

31. Based on my analysis of blockchain data, events, and the situation thus far, I have come up with the following conclusions:

a) Many of the addresses with significant amounts of bad debts are often directly connected to one another. This suggests a small number of user(s) were involved in the exploit of Rari pool #136.

b) It appears that at least one address that can be ascertained to be controlled by the ICHI Team has a significant amount of bad debt.

c) Some of the other addresses with significant amounts of bad debt might also be controlled by individuals that were part of or affiliated with the ICHI Team.

d) The ICHI Team directly transacted numerous times with multiple suspicious addresses that have significant amounts of bad debt. This is suggestive of insider trading by the ICHI Team with an unknown individual(s) who played a critical role in the collapse of Rari Pool 136.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on the 21st day of December 2022.

DATED: December 21, 2022
Vancouver, British Columbia, Canada

Paul

By:__________________________________
Paul Sibenik