IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

HASH ASSET MANAGEMENT, LTD., Plaintiff, v. DMA LABS, INC., ICHI FOUNDATION, NICK POORE, BRYAN GROSS, TYLER CHRISTIAN PINTER, JULIAN BRAND AKA JULIAN FINCH-BRAND, Defendants.	C.A. No.: 2025-0374-BWD

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. This declaration should be considered an update to a prior declaration of mine dated 12.21.2022, utilizing new information learned or obtained since this date, and I have updated my findings accordingly.

2. More specifically, I have assessed whether 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 CEO of Cryptoforensic Investigators, a blockchain forensics and investigative firm that regularly tackles cybercrime, hacks, frauds,

embezzlement, hidden assets, and market manipulation involving cryptocurrency. My work regularly requires me to analyze cryptocurrency transactions, wallets, and addresses, and make determinations about what can be understood or concluded about cryptocurrency transactions and activity.

4. Using a variety of forensic techniques, cryptocurrency including Ether ("ETH") and USDCoin ("USDC") 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.

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

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

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

9. 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.

10. 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]

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

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

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

12. 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.

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. The chart below details many of the relevant wallet addresses, short names, and lists which are controlled by ICHI, other defendants, and other relevant parties to the extent known. The reasons as to how I have ascertained ownership or control of applicable wallets are detailed later in the report.

Full address	**Short form**	**Owner or controller**	**Bad debt amount**
0xc8b5c6363ad036883fc663766ecd87928ad3dc36	0xc8b5	Unknown, but with link to ICHI team	$15.46 million
0xd4154916d1330a7eab4bf3e21295295805a1ab4f	0xd415	Tyler Pintar	$13.09 million
0xfb06ec3296ae0985f66a72c7efab5b27618d0d00	0xfb06	Julian Brand	$12.21 million
0x4fe5f268e5053a05108ebaf13ebd9a825e6fb6f2	0x4fe	ICHI Team	$5.644 million
0xe4f4d41bd8da7ae7e638aeac9800e67fcd8e2858	0xe4f4	Unknown	$3.103 million

[3] As well as XICHI and LP tokens.

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

0x1fc9cd26854dd3b7c74a36424e130887334a993e	0x1fc9	Unknown, but linked to 0xc8b5	$2.47 million
0x70d08aec714948855fbee7c61b709361be7144b6	0x70d0	Unknown	$2.136 million
0x0ead347d565ac2cf5b42595be53edf343e52b9d9	0x0ead	Unknown, but linked to 0xc8b5	$1.893 million
0xd4099bb6d81e2ea661c6c0417fec4292d48926df	0xd409	Unknown, but linked to 0xc8b5	$1.52 million
0x420b02fbb51d65ed2aa877e8b747160699ae0267	0x420b	Unknown	$1.288 million
0x11111D16485aa71D2f2BfFBD294DCACbaE79c1d4	0x1111	ICHI Team	0
0xC30220fc19e2db669eaa3fa042C07b28F0c10737	0xC302 2	ICHI Team	0
0x0dd4C0c16Fff6693e169Ef89235Cb92F9D8943EE	0x0dd4	ICHI Team	0
0x94A5980d5634533551dcB7108322f6C4f2a80E6B	0x94A5	ICHI Team	0
0x8f3c97DdC88D7A75b8c3f872b525B30932D3014c	0x8f3c	ICHI Team	0
0xcC50953A743B9CE382f423E37b07Efa6F9d9B000	0xcC50	ICHI Team	0
0xD1895682591Ac2751b10c11f0124FA46E8471562	ozgjoker.eth	Possibly Özgün Turan Kaynar	$2,144
0x2dddb6a69f071313580073941a4491313303b1ab	0x2ddd	Unknown, but interacts with 0xc8b5	$812.8k
0x4ac698cEAEbaa59a#A1882960727a44E5d42F8e75d	0x4ac6	BTCTurk Exchange	0
0x639e517d146C8f01d6e20c1B470989Fd778d3602	0x639e	BTCTurk Exchange	0

0x545683Ae74cFC8845e7033e0B0C91cE6623Dd2a6	0x5456	Binance exchange	0
0x591583182fC7D28a52477444dBc597636ac44FBC	0x5915	Unknown	$186.5k
0x71cEC0e5114798F5C369C3Ce931095dACCB17B5C	0x71cE	Unknown	$194k
0x82ceb7ce20e4c7531643ecf4b026caba5b9d3a05	0x82ce	Julian Brand	0
0xc10822bA46825317EE4134545d4FC7d30B6740EA	0xc209	FTX Exchange	0
0x8DD2E2189B2a2b9c98217690c5A0dbdD450EC66c	0x8DD2	Binance exchange	0
0x57c590086f4d7786eaA3398F9a39194aE689C0F6	0x57c5	Stake.com	0
0xB3a6CAD440F2189CCF8d6386E27C8190DE35a4c2	0xB3a6	Kraken exchange	0
0x96d7A68A509901D6C96036bFF96C48d61180da54	0x96d7	Kraken exchange	0
0x83792d023563864291822F35322ABF4B9409D041	0x8379	Kraken exchange	0
0x5A855887713271e802c7Cd224b628a1FEDa49Ea5	0x5A85	Binance exchange	0
0x43CE461d1bb2AcCd2EB028292E086E50d1e31f87	0x43CE	Binance exchange	0
0xde6568418D895cB8817f4A28Cc62a5CA5a879D1f	0xde65	Binance exchange	0
0x3Bbb7F2d18e4c942fD77591cfdecdab085c946AB	0x3Bbb	Binance exchange	0

18. 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 '0x1111'

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 0x1111 is responsible for doing this, 0x1111 is controlled by someone (or multiple people) on the ICHI Team.

b) 0xC30220fc19e2db669eaa3fa042C07b28F0c10737

'0xC3022'

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

'0x0dd4'

Description: ICHI Deployer 1

---

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

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

'0x94A5'

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

'0x8f3c'

Description: Rari Pool 136 admin

Summary: 0x8f3c 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 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 0x8f3c is the admin of Rari Pool 136, it must therefore be controlled by the ICHI Team.

---

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

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

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

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

f) 0x4Fe5f268e5053a05108eBAF13EbD9a825e6fB6f2

'0x4Fe5f'

Description: ICHI Pool deployer

Summary: Rari Pool 136 is associated with ETH contract address 0xAbDFCdb1503d89D9a6fFE052a526d7A41f5b76D6, and this smart contract was deployed by 0x4Fe5f. 0x4Fe5f 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, 0x4Fe5f would be controlled by the ICHI Team. 0x4Fe5f is the fourth largest holder of bad debt with $5.64M USD of bad debt.

g) 0xcC50953A743B9CE382f423E37b07Efa6F9d9B000

'0xcC509'

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.

19. 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 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 benefited since they ended up not paying back debts that they owe to Rari Pool 136.

20. 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.

21. 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.

22. 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.

23. 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 '0x2ddd', 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 '0xFb06' – with approximately $12.2M USD of bad debt, this is the third largest holder of bad debt. For reasons I will later evidence, this address is very likely controlled by Julian Brand. It received 1852 ICHI from directly '0x4fe5' 'ICHI Pool Deployer,' which, as discussed, should be controlled by the ICHI Team.

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 '0x420b' – 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 0x420b could be the same as the owner of '0xc8b5.'

26. 0x2dddb6a69f071313580073941a4491313303b1ab '0x2ddd' – 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 '0x4ac6' – 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

---

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.

‘0xc8b5’, ‘ozgjoker’eth,’ 0x4ac6, and 0x71cEC0e5114798F5C369C3Ce931095dACCB17B5C to name a few.

28. 0x639e517d146C8f01d6e20c1B470989Fd778d3602 ‘0x639e’ – 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 0x4ac6, however.

29. 0x545683Ae74cFC8845e7033e0B0C91cE6623Dd2a6 ‘0x5456’ – A Binance deposit address that receives transactions from various addresses with significant amounts of bad debt, including 0x591583182fC7D28a52477444dBc597636ac44FBC, 0x71cEC0e5114798F5C369C3Ce931095dACCB17B5C, and 0x0EAd347d565aC2Cf5b42595be53EDF343E52B9d9.

30. 0xd4154916d1330A7eAb4bF3e21295295805A1AB4f ‘0xd415’– The second largest holder of bad debt, approximately $13 million of bad debt. This address is controlled by Tyler Pintar, for reasons I evidence below.

31. 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:

- 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)

32. I am instructed that Julian Brand is a former ICHI staff member, and Tyler Pintar is his associate, which makes it particularly suspicious given that are at least two insiders both with an extremely large amount of bad debt, one of whom owns the wallet with the second largest amount of bad debt, and the other of whom owns the wallet with the third largest amount of bad debt.

33. Julian Brand is known to have operated under the alias 'bluejay', and I am instructed that Julian operated the Twitter account associated with the handle @onebluejayy. This Twitter account was active until the ICHI ecosystem collapsed, after which point the Twitter account was deleted. On December 2, 2021, the user tweeted his Ethereum wallet address when responding to another cryptocurrency project for an opportunity to receive cryptocurrency tokens from that project as part what's known as an 'airdrop.' In this response, the user provided the address 0x82ceb7ce20e4c7531643ecf4b026caba5b9d3a05 '0x82ce' as theirs.[11]

34. There are many transfers between 0x82ce (the address Julian tweeted) and 0xFb06 (the third largest debt holder, and one of the wallets involved

[11] Although the tweet was deleted, it has been archived on Waybackmachine -- https://web.archive.org/web/20211202120820/https://twitter.com/onebluejayy/status/1466378509518000135

in the exploit). The considerable number of transfers from the former address to the latter combined with the fact that they send cryptocurrency to the same FTX deposit address 0xc10822bA46825317EE4134545d4FC7d30B6740EA are amongst the reasons that these wallets are controlled by the same individual in my opinion. A list of transactions that 0x82ce has sent to 0xFb06 are:

- 0x0bf1ceda17656cbe3a0dea1b229814df1bebdc4d056af7adaa14f3b72dafb6e0 (10,000 USDT)
- 0x127a482de73642f9929a7c6414a9483a1023678f4dddcce206ba6a9fa37429b3 (0.076851 ETH)
- 0x00e196f8238248d332d335f99d92881daf9eff5dc0fde784661eb65f69eb7ecf (34,742 USDC)
- 0x88e67eca24502f971c2afa24dead51722c9f2b6533a6d4ebe8261bce46c5dcde (5,580 USDC)

35. The wallet 0xd415 is associated with an Opensea profile named 'thisguyty'.[12] Opensea is marketplace for cryptocurrency NFTs (Non-fungible tokens) where users can set up profiles and link their wallets. 0xd415 is linked to the profile 'thisguyty'.

36. I am instructed that 0xd415 belongs to Tyler Pintar, which would be consistent with handles Mr. Pintar has used elsewhere. For example, on Twitter, Mr. Pintar used the handle @this_guyty and on Instagram Mr. Pintar used the handle "thisguytypi."

37. This suggests that a wallet belonging to Tyler Pintar was the second largest bad debt holder.

38. Some suspicious activity that I have identified at this stage which suggests insider involvement is that on April 6, 2022, Julian borrowed 1.8 million

[12] https://opensea.io/thisguyty

USDC. Hours later on April 7, the ICHI team transferred $5 million USDC and 43 wBTC from the Treasury into the Rari pool[13] which I understand was done without a community governance vote that should have been required.[14]

39. Hours later on April 7, Tyler borrowed 1.414 million USDC tokens. On April 8, Julian borrowed an additional 3 million USDC as well as an additional $658k USD worth of oneBTC tokens and $1.5 million oneUNI tokens. Tyler borrowed 927k USDC on April 8. Additional funds were borrowed from Rari capital pool by both Julian and Tyler on April 9, and additional capital was moved by the ICHI team into Rari protocol to support the increasing and unsustainable amount of cryptocurrency being borrowed by the largest debt holders.

40. On April 11, the day the price of ICHI tokens collapsed the most, the ICHI team pulled a net amount of 10.42 million oneUNI of liquidity from Uniswap.[15] Shortly thereafter, also on April 11, Julian borrowed an additional $1.25 million of oneUNI tokens after the LTV ratio had increased which was then redeemed for USDC. At roughly the same time on April 11 Tyler borrowed $1 million worth of oneBTC tokens and 2 million USDC; the oneBTC was quickly redeemed for USDC.

---

13 https://etherscan.io/tx/0xf2d02b76ad2b35886dd6a9f7edd4f5dbf3d957f1866ed1ab1386a9d6e0f4643b

14 https://web.archive.org/web/20210725101650/https:/docs.ichi.farm/onetokens/dma , https://web.archive.org/web/20210614050511/https:/docs.ichi.farm/onetokens/dma/community-treasury , https://web.archive.org/web/20210613213321/https://docs.ichi.farm/onetokens/core-technical-concepts/governance/treasury-governance

15 https://etherscan.io/tx/0xf2ba9db143270832f6bbb3493ecbc3ac24548cd5d5c97b04c349de8fda2ffe2c

41. As previously mentioned, the ICHI team moved cryptocurrency out of the community treasury into Rari pool 136 without the required community vote that was required per the terms. I have identified the following movements of treasury funds without the required community vote:

a) $5 million USDC & 43 WBTC -- https://etherscan.io/tx/0xf2d02b76ad2b35886dd6a9f7edd4f5dbf3d957f1866ed1ab1386a9d6e0f4643b

b) $1.99 million USDC -- https://etherscan.io/tx/0xfce190dd37ecf05973fbf5593877e70e38a8641d7a385039a92b48fc780d71a8

c) $2 million USDC -- https://etherscan.io/tx/0x3e633b557788fb68615fdd90ce602dba97b0ea300a47a17d2eb41908492f4485

42. The actions of the ICHI team to move the funds from the treasury are highly problematic and detrimental to users of the protocol that were not involved in the exploit for the following reasons:

a) The notion that it was supposed to be users, rather than the ICHI Team or DMA labs that decides when or if collateral is withdrawn from the community treasury was expressly and repeatedly mentioned as something the users would have control over.[16]

b) One of the things that community votes are designed to help prevent are poor or shortsighted decisions, as well as helping to prevent the effect

16 https://web.archive.org/web/20210725101650/https:/docs.ichi.farm/onetokens/dma
https://web.archive.org/web/20210613213321/https://docs.ichi.farm/onetokens/core-technical-concepts/governance/treasury-governance

of any malicious actions or efforts to exploit the project, including potential actions by developers or the ICHI Team.

c) It is likely that many users would not have deposited assets into Rari pool 136 at all, had they know the funds could or would be taken out of the treasury without the necessary authorization. The funds in the treasury are ultimately the collateral belonging to depositors. Without the collateral, the oneTokens would be worthless, hence when users have a vested interest in voting themselves and maintaining good governance.

d) If funds had not been moved from the treasury without a required community vote, and assuming a community vote did not pass, then it is likely those responsible for exploiting the protocol would not have profited nearly as much as they did. And even if Rari pool 136 collapsed anyway, then there would be far more assets in the community treasury to pay off depositors.

e) The decision by the ICHI Team to move millions of dollars from the community treasury in a desperate attempt to prop up Rari pool 136, without a community vote, led to a very small group of wallet owners to profit handsomely off the exploit. Some of the wallet owners that profited are known (such as Tyler Pintar and Julian Brand), while other wallet owners haven't been fully identified yet, but many of those wallet owners repeatedly transact with one another, suggesting collusion and/or common ownership of many of the other wallets with the highest bad debt holders.

43. I have conducted some tracing to identify where most of the largest debt holders sent a lot of their proceeds

f) 0xc8b5 (largest bad debt holder) sent proceeds to 0x8DD2E2189B2a2b9c98217690c5A0dbdD450EC66c (Binance), 0x57c590086f4d7786eaA3398F9a39194aE689C0F6 (stake.com), and 0x4ac698cEAEbaa59A1882960727a44E5d42F8e75d (BTCTurk)

g) 0xd4154916d1330A7eAb4bF3e21295295805A1AB4f (Tyler Pintar) sent a large portion of the proceeds to 0xB3a6CAD440F2189CCF8d6386E27C8190DE35a4c2 (Kraken).

h) 0xFb06EC3296Ae0985f66a72C7efAB5b27618D0D00 (Julian Brand) sent a large portion of the proceeds to 0x96d7A68A509901D6C96036bFF96C48d61180da54 and 0x83792d023563864291822F35322ABF4B9409D041 (both Kraken).

i) 0xe4f4d41bd8da7ae7e638aeac9800e67fcd8e2858 (Fifth largest bad debt holder) sent proceeds to Binance.com exchange, specifically to 0x5A855887713271e802c7Cd224b628a1FEDa49Ea5, 0x43CE461d1bb2AcCd2EB028292E086E50d1e31f87, 0xde6568418D895cB8817f4A28Cc62a5CA5a879D1f, and 0x3Bbb7F2d18e4c942fD77591cfdecdab085c946AB

44. There are notable connections between the wallets 0xE4f4, 0x1fc9, 0x0ead, 0xd409, 0x420b, 0x2dDd, 0x71cE, 0x5915 (5th 6th, 8th, 9th, 10th, 11th, 19th, and 20th largest bad debt holders) as well as ozgjoker.eth which all transact with 0xc8b5c (largest bad debt holder) in such a way that it could suggest the possibility common ownership amongst some of the wallets. A forensic graph that shows this is included in Appendix C.

45. In addition to these addresses transacting with 0xc8b5c, typically repeatedly, the cryptocurrency from many of these addresses is sent to many of the same cryptocurrency exchange accounts at BTCTurk exchange and Binance exchange.

46. Given both these factors, it strongly suggests that many of the largest debt holders colluded with each other and know each other, and is suggestive of insider involvement in this scheme to exploit Rari pool 136.

47. The wallets I have identified as belonging to Tyler Pintar and Julian Brand, do not interact with the collection of wallets shown in the forensics graph.

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

j) 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.

k) 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.

l) 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 multiple individuals, some known and others unknown, who played a critical role in the collapse of Rari Pool 136.

m) Julian Brand and Tyler Pintar attempted to borrow as much as they could from Rari pool 136 in the days prior to the collapse, and during the collapse itself, while at the same time the ICHI team moved assets from the treasury to Rari pool 136 without having conducted the required community vote, allowing insiders, including Brand and Pintar to profit more and more from the inherent flaws in the protocol.

n) Insiders were able to deplete Rari protocol of the limited USDC available before other users could redeem, possibly due to inside information that insiders like Brand and Pintar may have had.

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 August 2025.

DATED: August 21, 2025
Kelowna, British Columbia, Canada

By:_____
Paul Sibenik