IN THE CIRCUIT COURT OF THE ELEVENTH JUDICIAL CIRCUIT IN AND FOR MIAMI-DADE, COUNTY, FLORIDA

CETUS TECHNOLOGY LIMITED, a British Virgin Islands Company,

Plaintiff,

v.

DOE NOS. 1-25

Defendants.

Case No. _____

(Injunctive Relief Requested)

COMPLAINT

CETUS TECHNOLOGY LIMITED ("Plaintiff"), by and through its undersigned counsel, Xander Law Group ("Plaintiff Counsel"), brings this Complaint for claims of conversion and related equitable remedies, and alleges as follows:

INTRODUCTION

1. This case is about the illegal conversion of digital assets on May 22, 2025. Approximately $61 million of the converted assets are in two cryptocurrency wallets controlled by Defendants. Plaintiff seeks to enjoin these assets immediately, before they are lost forever.

2. Plaintiff's principal place of business is in the British Virgin Islands, but it conducts substantial business throughout the United States, including within the jurisdiction of this Court.

3. The conversion scheme was a brazen theft that involved the Cetus Protocol, which Plaintiff operates. Understanding the details of the illegal conversion requires a brief explanation of a few cryptocurrency terms: DEX, blockchain, and smart contracts.

4. First, the Cetus Protocol is a decentralized crypto exchange, or "DEX." A DEX is a kind of peer-to-peer marketplace, where individuals and businesses trade digital assets directly, instead of going through a centralized intermediary such as a bank or securities exchange. Plaintiff operates the Cetus Protocol.

5. Second, the Cetus Protocol facilitates transactions on the Sui "blockchain." A blockchain is a kind of accounting platform, a decentralized ledger that records digital transactions. The transactions that were part of the Cetus Protocol conversion scheme were recorded on the Sui blockchain.

6. Third, the Cetus Protocol relies on "smart contracts," self-executing agreements written in computer code. Smart contracts automate the execution of digital asset transactions, like an online vending machine. An individual or business deposits funds, pulls a virtual lever by indicating an intent to transact, and then automatically receives a digital asset.

7. Accordingly, Plaintiff, by operating the Cetus Protocol, facilitates digital asset transactions for individuals and businesses throughout the world. Substantial transactions on the Cetus Protocol arise in, and involve residents of, Florida, including Miami-Dade County, Florida.

8. On May 22, 2025, one or more individuals ("Defendants") illegally manipulated part of the Cetus Protocol. As described in more detail below, Defendants thereby converted Cetus Protocol digital assets and transferred them elsewhere (the "Cetus Hack"). The effect of the Cetus Hack was to transfer assets held virtually by Plaintiff to Defendants' possession, so that they could illegally convert them for their own use. As operator of the Cetus Protocol, Cetus asserts the claims alleged herein as the

lawful owner of the digital assets associated with members of the Cetus Protocol community before these assets were unlawfully taken.

9. After the Cetus Hack, Plaintiff contacted Inca Digital ("Inca"), a fintech intelligence company, which traced transactions related to the Cetus Hack and confirmed that the transactions were part of a conversion scheme.

10. According to Inca's investigation, Defendants converted Cetus Protocol assets and then sent them through a web of transactions designed to hide their trail. However, Inca was able to trace and connect Defendants' transactions, follow the trail, and identify certain cryptocurrency wallets that held converted assets.

11. A portion of the illegally converted assets – approximately $61 million worth – are currently held by Defendants in Ethereum, a cryptocurrency, and in USDC, a stablecoin pegged to the U.S. dollar and issued by Circle Internet Group, Inc. (including related entities, collectively "Circle"), a U.S. public company that does substantial business in this County. Inca's investigation has identified the two wallets that hold these assets.

12. This lawsuit is brought to halt any activity in these wallets immediately and to enjoin Defendants immediately from transferring or laundering the assets in these wallets. With respect to the Ethereum assets, Plaintiff requests an immediate injunction to prevent Defendants and other digital asset launderers from transferring the assets using specific cryptocurrency money laundering techniques, including Tornado Cash. With respect to the USDC assets, Plaintiff requests an immediate injunction to prevent Circle from transferring the assets to anyone other than Plaintiff or its counsel.

13. Plaintiff also asks this Court to order the return of the frozen assets to Plaintiff in an orderly and timely fashion, within 30 days (or longer if deemed appropriate), and in a manner deemed viable by the entity holding or controlling the assets, including Circle. Once the assets are enjoined from immediate transfer, there will be time to determine whether any further transfer also would be an illegal conversion and how any future transfer to Plaintiff should occur. But now time is of the essence: if Defendants transfer Plaintiff's assets out of the two cryptocurrency wallets Inca has identified to a mixer or exchange that is difficult to trace through, these assets may be lost forever.

JURISDICTION AND VENUE

14. Plaintiff's principal place of business is the British Virgin Islands, but it conducts substantial business in the United States, including within the jurisdiction of this Court.

15. Defendants are persons of unknown citizenship who perpetrated the wrongdoing alleged herein. The true identities and residences of Defendants are currently unknown and are subject to ongoing investigation.

16. Plaintiff will attempt to identify Defendants through discovery served on third parties with whom Defendants interacted.

17. Venue is proper in this Court as a substantial part of the events giving rise to the claims occurred in Miami-Dade County, Florida, which was targeted by the Defendants' conversion scheme.

18. The Plaintiff reserves the right to amend this Complaint to include additional parties as Defendants, upon further investigation and discovery of their identities, roles, and residences.

STATEMENT OF FACTS

19. On May 22, 2025, Cetus Protocol, the primary DEX on the Sui blockchain, was exploited via a vulnerability in the "integer-mate dependency," as described below. The exploit resulted in a theft of over $223 million in digital assets from more than 200 liquidity pools.

20. Essentially, Defendants attacked Cetus Protocol using a flaw in the math system that Cetus relied on to manage numbers in its smart contracts. The attacker used a trick called a "flash loan" to borrow tokens for just a few seconds, enough time to create a problem arising from the math system in the code and thereby profit.

21. When the math system tried to calculate how much the attacker needed to pay, it underestimated the amount by a large margin because of a "math overflow," meaning the number became too large and "wrapped around" so it looked like a small number, like an old calculator that cannot display more than eight digits. The exploit resulted in a theft of over $223 million in digital assets from more than 200 liquidity pools. As of the date of this Complaint, approximately $61 million of cryptocurrency assets remain unrecovered.

22. Upon identification of the attack vector, Cetus Protocol paused smart contracts to prevent further damage. Simultaneously, Sui validators coordinated to implement transaction filtering, freezing funds in attacker-controlled wallets.

23. Inca traced two key wallets that received the stolen funds:

a. Wallet 1 (Frozen):

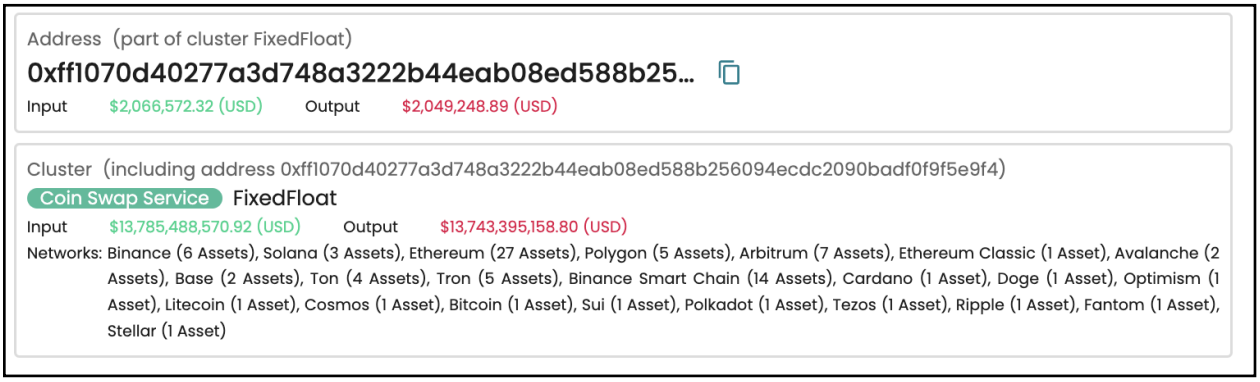
0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06

b. Wallet 2 (Frozen):

0xcd8962dad278d8b50fa0f9eb0186bfa4cbdecc6d59377214c88d0286a0ac9562

24. These wallets collectively received approximately $163 million of the total $223 million of the stolen funds. With the cooperation of Sui validators, transactions from these wallets were frozen via transaction filtering at the mempool level.

25. Wallet 1 was funded three days before the exploit by 0xff1070d40277a3d748a3222b44eab08ed588b256094ecdc2090badf0f9f5e9f4. Inca identified this address as one of FixedFloat's main wallets, along with Twitter (X) posts mentioning this wallet as having been involved in a previous scam.[1]



FixedFloat Hot Wallet Attribution

[1] X: G0ODMONEY; 2025 May 5.

Twitter (X) post mentioning funding wallet

26. The attacker bridged approximately $61 million in USDC to Ethereum via the Wormhole bridge in multiple 1,000,000 USDC transactions.

Type	Activity Details	Activity With	Gas Fee	Age
Contract Interaction 7TVrCpxE•••AwJ2zbtW	-1,000,000 USDC		5 0.001651532 SUI	1d
Contract Interaction 64cdvsr5•••Kp6LVpVh	-1,000,000 USDC		5 0.001651532 SUI	1d
Contract Interaction 9GCd1cz6•••PtvnbNrE	-1,000,000 USDC		5 0.001651532 SUI	1d
Contract Interaction CokaMXYB•••2e2WSMux	-1,000,000 USDC		5 0.001651532 SUI	1d
Contract Interaction Bt6bcFAv•••tfAfPf2d	-1,000,000 USDC		5 0.001651532 SUI	1d

SuiScan: Example transactions bridging USDC from Sui to Ethereum

27. The bridged funds were distributed to two Ethereum wallets:

Wallet 3: 0x89012a55cd6b88e407c9d4ae9b3425f55924919b (~$8M)

Wallet 4: 0x0251536bfcf144b88e1afa8fe60184ffdb4caf16 (~$53M)

28. On May 22, 2025, Wallet 1 bridged funds to Wallet 3. This Ethereum bridge transaction involved $932,137.18 USDC. The transaction is recorded at:

https://suivision.xyz/txblock/A9AK5FvtpBNUsB676KCaY4Wq3BwhmayyHWZB3cxPWHvh

29. Inca is successfully working with the Wormhole team to delay this transaction, but the ability to return the USDC will ultimately rely on action from Circle.

30. Inca discovered that the attacker tested the exploit mechanism in advance. On April 3, 2025, a wallet (0x2ed9af930f01308a87885151de177f44872f0bbf27ab66a22420fa6e32ccf21f) interacted with the `compute_swap_step` and `checked-shlw` functions on-chain, the same vulnerable pathway exploited in the main attack.

31. This test wallet was funded by another wallet (0x7e0b3d475ebbc26e3d9e9017e4bb41a10710365b94ed460ac3a1688421cbc54a) associated with a pseudonymous actor known online as "Defigen," a high-volume DeFi participant. The funding path and wallet activity showed a tight operational link between the test and exploit phases.

32. According to Inca, behavioral and transactional evidence strongly suggests Defigen operates numerous wallets across Sui, Ethereum, and other chains, and has shown patterns of advanced smart contract knowledge, exploit pre-testing, and privacy preservation. While Inca has not concluded that Defigen directly perpetrated the Cetus exploit, the funding of the test wallet from an address linked to Defigen supports further inquiry into possible facilitation or material support by this actor.

FIRST CAUSE OF ACTION
CONVERSION

33. Plaintiff realleges and incorporates by reference paragraphs 1-32 as if stated fully in herein.

34. Plaintiff has lawful ownership and rights of possession of the property described herein.

35. Defendants intentionally and unlawfully took possession of the Plaintiff's funds, converting them for their own use through wrongful acts and in a manner that is inconsistent with plaintiff's property rights.

36. This act of conversion has caused significant damages and financial harm to the Plaintiff.

SECOND CAUSE OF ACTION
REQUEST FOR INJUNCTIVE RELIEF

37. Plaintiff realleges and incorporates by reference paragraphs 1-32 as if stated fully herein.

38. Plaintiff requests an Order (1) immediately enjoining Defendants, Tornado Cash, and Circle from entering into transactions that involve the transfer of assets from 0x89012a55cd6b88e407c9d4ae9b3425f55924919b ($932,137.18 of USDC and 3,144 ETH) or 0x0251536bfcf144b88e1afa8fe60184ffdb4caf16 (20,000 ETH), directly or indirectly, except transactions with Plaintiff or Plaintiff's counsel, and (2) directing Circle to return the USDC in 0x89012a55cd6b88e407c9d4ae9b3425f55924919b to Plaintiff within 30 days by any reasonable means available to Circle.

39. Such action is necessary to preserve the possibility of restitution for the Plaintiff and other victims.

40. Plaintiff has no adequate remedy at law.

41. Plaintiff will suffer irreparable harm if an injunction is not issued by this Court.

42. Plaintiff has a clear legal right to the property contained in the wallets sought to be enjoined.

43. It is in the public interest for the Plaintiff's property to be preserved through injunctive relief.

Wherefore, Plaintiff respectfully requests that this Court enter a temporary restraining order immediately enjoining Defendants, Tornado Cash, and Circle from entering into transactions that involve the transfer of assets from Wallets 3 or 4, directly or indirectly, except transactions with Plaintiff or Plaintiff's counsel, and awarding: (1) damages in the amount of the value of Plaintiff's stolen assets at the time of the theft; (2) pre-judgment interest; (3) an injunction ordering the return of any remaining stolen assets or the proceeds derived from the same, including an injunction directing Circle to return the USDC in Wallet 3 to Plaintiff within 30 days by any reasonable means; (4) attorneys' fees and costs incurred in prosecuting this action; and (5) any other relief that the Court finds just and proper.

Dated: June 11, 2025

Respectfully submitted,
By: /s/*Jose Teurbe-Tolon*
JOSE TEURBE-TOLON, ESQ.
Fla. Bar No. 87791
XANDER LAW GROUP, P.A.
25 S.E. 2nd Avenue, Suite 808
Miami, Florida 33131
Telephone: (305) 767-2001

Facsimile: (855) 926-3370
jose@xanderlaw.com
service@xanderlaw.com

Attorney for Plaintiff