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 and CIRCLE INTERNET GROUP, INC.,

Defendants.

Case No. 2025-010992-CA-01

AMENDED COMPLAINT

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

INTRODUCTION

1. This case is about the illegal conversion and laundering of digital assets on May 22, 2025. After the initial Complaint was filed in this matter, the Court entered an Order freezing approximately $61 million of converted assets, and directing Circle Internet Group, Inc. (including related entities, collectively "Circle"), a U.S. public company that does substantial business in this County, and others to freeze and return these assets.

2. With Circle's advice and permission, Plaintiff sought an Amended Order directing Circle to block the transfer of some of the converted assets. Circle blocked these assets, thereby demonstrating its ability to block the transfer of assets immediately and effectively.

3. However, Circle has not transferred the blocked assets to Plaintiff or delivered any assets to Plaintiff. Plaintiff now seeks to recover against Circle for the unjust enrichment that arose from Circle's block. Accordingly, this Amended Complaint adds Circle as a Defendant.

4. Based on Plaintiff's further investigation, Plaintiff now also seeks to recover from Circle for its negligence in failing to block other assets that were illegally converted and laundered, including assets issued by Circle that were transferred using Circle's protocol known as the Circle "Cross-Chain Transfer Protocol," or CCTP. Plaintiff's investigation has revealed that Circle could have blocked the transfer of these other assets immediately and effectively, but it did not.

5. Plaintiff's investigation revealed that Circle, and the crypto assets and protocols it created were at the epicenter of the illegal conversion and laundering of assets. The illegal conversion and laundering could not have happened without Circle's actions and negligence. Circle had a direct relationship with the attacker through the use of the CCTP. But instead of blocking the attacker's transfer of assets, Circle approved and facilitated their transfer. Circle's assets and protocols were neither "safe" nor "secure," as Circle represented, including in public filings. Circle failed to exercise due care with respect to the illegal conversation and laundering of the assets and was unjustly enriched by this failure.

6. The most straightforward way to observe Circle's failure is simply to look at the list of the 62 transactions as they occurred in real time. Each had precisely the same characteristics. Each was an outbound flow from one of two sender addresses to one of two receiver addresses. Each involved the same sender blockchain and the same receiver blockchain. Each involved USDC, an asset issued by Circle and pegged to the U.S. dollar. Each involved Circle's CCTP and an "attestation" from Circle. The most striking similarity is the amounts:

virtually all transactions of just under $1 million: $999,759 just before 10:48am, $999,759 three minutes later, and so on.

Time	Protocol	Asset	Amount	Minutes
10:47:59	circle_cctp	USDC	$999,759	
10:51:02	circle_cctp	USDC	$999,759	03:03
10:51:44	circle_cctp	USDC	$999,759	03:45
10:52:31	circle_cctp	USDC	$999,759	04:32
10:53:40	circle_cctp	USDC	$999,759	05:41
11:04:51	circle_cctp	USDC	$999,801	16:52
11:05:57	circle_cctp	USDC	$999,801	17:58
11:06:41	circle_cctp	USDC	$999,801	18:42
11:07:45	circle_cctp	USDC	$999,801	19:46
11:08:23	circle_cctp	USDC	$999,801	20:24
11:08:55	circle_cctp	USDC	$999,801	20:56
11:09:28	circle_cctp	USDC	$999,801	21:29
11:09:47	circle_cctp	USDC	$999,801	21:48
11:11:14	circle_cctp	USDC	$999,801	23:15
11:12:58	circle_cctp	USDC	$999,801	24:59
11:13:20	circle_cctp	USDC	$999,801	25:21
11:13:52	circle_cctp	USDC	$999,801	25:53
11:14:27	circle_cctp	USDC	$999,801	26:28
11:14:52	circle_cctp	USDC	$999,801	26:53
11:15:11	circle_cctp	USDC	$999,801	27:12
11:15:41	circle_cctp	USDC	$999,801	27:42
11:16:05	circle_cctp	USDC	$999,801	28:06
11:16:48	circle_cctp	USDC	$999,801	28:49
11:17:16	circle_cctp	USDC	$999,801	29:17
11:17:48	circle_cctp	USDC	$999,801	29:49
11:18:09	circle_cctp	USDC	$999,801	30:10
11:18:27	circle_cctp	USDC	$999,801	30:28
11:18:58	circle_cctp	USDC	$999,801	30:59
11:19:17	circle_cctp	USDC	$999,801	31:18
11:20:11	circle_cctp	USDC	$999,801	32:12
11:20:40	circle_cctp	USDC	$999,801	32:41
11:21:02	circle_cctp	USDC	$999,801	33:03
11:21:43	circle_cctp	USDC	$999,801	33:44
11:22:29	circle_cctp	USDC	$999,801	34:30
11:22:47	circle_cctp	USDC	$999,801	34:48
11:23:06	circle_cctp	USDC	$999,801	35:07
11:23:28	circle_cctp	USDC	$999,801	35:29
11:23:50	circle_cctp	USDC	$999,801	35:51
11:24:10	circle_cctp	USDC	$999,801	36:11
11:24:33	circle_cctp	USDC	$999,801	36:34
11:24:54	circle_cctp	USDC	$999,801	36:55
11:25:15	circle_cctp	USDC	$999,801	37:16
11:25:34	circle_cctp	USDC	$999,801	37:35
11:25:54	circle_cctp	USDC	$999,801	37:55
11:26:13	circle_cctp	USDC	$999,801	38:14
11:26:37	circle_cctp	USDC	$999,801	38:38
11:27:05	circle_cctp	USDC	$999,801	39:06
11:27:26	circle_cctp	USDC	$999,801	39:27
11:27:48	circle_cctp	USDC	$999,801	39:49
11:28:09	circle_cctp	USDC	$999,801	40:10
11:28:32	circle_cctp	USDC	$999,801	40:33
11:28:54	circle_cctp	USDC	$999,801	40:55
11:29:17	circle_cctp	USDC	$999,801	41:18
11:29:40	circle_cctp	USDC	$999,801	41:41
11:30:11	circle_cctp	USDC	$999,801	42:12
11:30:30	circle_cctp	USDC	$429,313	42:31
11:37:19	circle_cctp	USDC	$999,801	49:20
11:38:04	circle_cctp	USDC	$999,801	50:05
11:38:46	circle_cctp	USDC	$999,801	50:47
11:39:48	circle_cctp	USDC	$999,801	51:49
11:41:23	circle_cctp	USDC	$999,801	53:24
11:46:42	circle_cctp	USDC	$885,527	58:43

7. The repeated pattern is instantly recognizable. The first column shows the time of the transaction. The second column shows the protocol used for each of the transfers: Circle's CCTP in each case. The third column shows the asset transferred: Circle's USDC in each case. The fourth column shows the amounts; most are suspiciously just under $1 million. The final column shows the elapsed minutes from the beginning of the attack until each transaction.

8. After a few minutes, it was obvious what was happening. It took nearly an hour to complete all of the transactions, a lifetime for digital assets. Circle should have recognized the attack and laundering, halted Circle's attestation of each transaction, and blocked further transactions from and into the same wallets.

9. Instead, again and again, in dozens of transactions, like a criminal cashing checks for just under $10,000, the attacker bridged amounts of just under $1 million worth of the Circle-issued asset using Circle's CCTP protocol. Circle's CCTP has a maximum bridge amount of $1 million, so any transactions just under the maximum $1 million amount would be red flags. In fact, the first five transactions, during the first seven minutes, were for precisely $999,759. Then the amount increased slightly, to $999,801, and that transaction was repeated 55 times. Two transactions were for lower six-figure amounts. The total amount transferred was $61,302,690.

10. Circle should have recognized the above pattern and blocked the transfers immediately and effectively, as they have demonstrated they can. Instead, Circle's protocol approved the above transactions, and the assets were laundered and lost forever. Circle, as a key player in the digital asset market, was obligated to follow a higher standard of care.

11. Cetus committed to compensate its users for their losses. Cetus obtained a $30 million loan in response to the attack and used its cash reserves of approximately $7 million plus

additional digital assets to cover its user's losses. As a result, Cetus was damaged by at least $61 million overall.

12. Plaintiff brings this amended action (1) to recover on the blocked assets given that the block has unjustly enriched Circle, and (2) to hold Circle accountable for the other assets whose transfer it could and should have prevented. Specifically, with details provided below and in the Appendix, Plaintiff seeks to collect the following assets that were converted and laundered in the attack: (1) $932,137.18 for the transfer of USDC from wallet address 0x89012a55cd6b88e407c9d4ae9b3425f55924919b that is now blocked pursuant to the Amended Order, and (2) $60,370,553, the U.S. dollar equivalent of 3,144 ETH, a digital asset, assets that were transferred from wallet address 0x89012a55cd6b88e407c9d4ae9b3425f55924919b, plus the U.S. dollar equivalent of 20,000 ETH, assets that were transferred from wallet address 0x0251536bfcf144b88e1afa8fe60184ffdb4caf16.

JURISDICTION AND VENUE

13. Plaintiff is incorporated in the British Virgin Islands. Its platform has been accessed by more than 17 million unique global wallet addresses, of which many are from the United States, including within the jurisdiction of this Court.

14. Defendant Circle is a U.S. public company that does substantial business in this County.

15. Circle holds Florida Money Transmitter License FT230000121 through its subsidiary, Circle Internet Financial, LLC, NMLS #1201441, and accordingly operates in Florida as a regulated money transmitter.

16. At least one member of Circle's Executive Leadership Team resides and works in Miami, Florida.

17. Circle includes a provision in its legal and privacy notice online directing Florida residents with unresolved complaints to contact Florida regulators, labeling this notice as "By the Florida Office of Financial Regulation" and stating: "After first contacting Circle, if you still have an unresolved complaint regaing [sic] the company's regulated activity, please direct your complaint to: Florida Office of Financial Regulation, Division of Finance 200 E. Gaines Street Tallahassee, FL 32399-0376 Toll-Free Number: 1-800-848-3792 NOTICE: By the Florida Office of Financial Regulation".

18. The non-Circle Defendants are persons of unknown citizenship, including indivduals who perpetrated the wrongdoing alleged herein. The true identities and residences of the non-Circle Defendants are currently unknown and are subject to ongoing investigation. Plaintiff will attempt to identify the non-Circle Defendants through discovery served on third parties with whom they interacted.

19. 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 attack.

20. 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

21. The conversion scheme at issue here 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.

22. 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.

23. 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.

24. 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.

25. Accordingly, Plaintiff, by operating the Cetus Protocol, facilitates digital asset transactions for individuals and businesses throughout the world. As noted above, substantial transactions using the Cetus Protocol arise in, and involve residents of, Florida, including Miami-Dade County, Florida.

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

27. Essentially, Defendants attacked the 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.

28. 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.

29. Upon identification of the attack, Cetus Protocol paused smart contracts to prevent further damage. Simultaneously, Sui validators coordinated to implement transaction filtering, freezing funds in attacker-controlled wallets. Approximately $61 million of cryptocurrency assets remain unrecovered.

30. 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.

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

32. The portion of the illegally converted assets that were not recovered, approximately $61 million worth, were held by Defendants in ETH, known as Ethereum, a cryptocurrency, and in USDC, a stablecoin pegged to the U.S. dollar and issued by Circle. USDC was transferred repeatedly during the attack.

33. As noted above, Circle is the creator of the "Cross-Chain Transfer Protocol (CCTP)," a utility that facilitates the transfer of USDC and was used repeatedly during the exploit. The CCTP's "Attestation Service" observes the "burn events" that are required before USDC can be transferred from one blockchain to another and issues a signed "attestation" of that

transaction. This CCTP Attestation Service was used repeatedly during the exploit and Circle repeatedly provided the "attestations" necessary for the transfers to occur.

34. The timeline is as follows. First, at 10:47:59 on May 22, 2025, the attacker bridged $999,759 of USDC from the Sui blockchain to the Ethereum blockchain. The attacker used the CCTP for this transfer and Circle facilitated this bridge by issuing a signed "attestation."

35. Just over three minutes later, at 10:51:02, the attacker bridged another $999,759 of USDC from Sui to Ethereum, likewise facilitated by Circle, likewise using Circle-created services.

36. Again and again during the next hour, like a criminal cashing checks for just under $10,000, the attacker bridged amounts of just under $1 million worth of USDC. The first five transactions, during the first seven minutes, were for $999,759. Then the attacker increased the amounts slightly, to $999,801, and repeated that transaction 55 times. Two transactions were for lower six-figure amounts. The total amount transferred was $61,302,690.

37. It is not a coincidence that the transactions were just under $1 million. It does not appear that there was ever previously a USDC bridge transfer using the CCTP from the Sui to Ethereum blockchains that exceeded $1 million.

38. The details of these transactions are set forth in the Appendix, with transaction hashes. All of this information is publicly available and was available immediately during the exploit.

39. At the time of the attack, and during the preceding months, Circle repeatedly had represented the "safety" and "security" of both USDC and CCTP, including Circle's Attestation Service.

40. As noted above, Circle is the issuer of USDC, a crypto asset that was transferred repeatedly during the exploit. USDC is a "digital dollar," which is fully backed and redeemable 1:1 for US dollars. Circle describes USDC as a "stablecoin" because it is backed 100% by highly liquid cash and cash-equivalent assets. Circle represents that USDC provides "rapid, secure, and cost-efficient transactions for digital payments." So-called "Circle Mint" customers are able to directly mint and redeem USDC with Circle, meaning that they can exchange USDC for "fiat currency." Other end-users can transfer USDC for fiat currency in the secondary market.

41. Circle creates USDC through the process called "minting," and uses the proceeds from issuing the USDC to purchase reserve assets. At the relevant times, Circle had the capability to take USDC out of circulation through a process called "burning," and also had the capability to "block" instantaneously certain USDC transactions from occurring. As a result, the amount of USDC in circulation depended on actions taken by Circle.

42. Circle maintains reserves that back its obligations to redeem USDC for Circle Mint customers. For example, as of March 31, 2025, Circle held approximately 90% of its USDC reserves in the Circle Reserve Fund, a government money market fund, pursuant to Rule 2a-7 under the Investment Company Act of 1940. The Circle Reserve Fund is managed by BlackRock, one of the world's largest asset managers, and these funds are available only to Circle . The assets within the Circle Reserve Fund are held in the custody of The Bank of New York Mellon, one of the largest asset custodians in the world.

43. As a result of Circle's block pursuant to this Court's Amended Order, no Circle Mint customer will be able to obtain the blocked USDC. Yet Circle continues to hold reserve assets in the Circle Reserve Fund that back its obligations to redeem that USDC. Because Circle retains the assets backing the USDC, it also receives reserve income on those assets, even though

no one is able to redeem the USDC. Circle recorded approximately $1.66 billion of reserve income overall during 2024. A portion of Circle's reserve income during 2025 appears to be from reserve assets backing the blocked USDC.

44. As noted above, Circle also is the creator of the "Cross-Chain Transfer Protocol," or CCTP, a utility that facilitates the transfer of USDC and was used repeatedly during the exploit. The CCTP "Attestation Service" observes the "burn events" that are required before USDC can be transferred from one blockchain and issues a signed attestation of the transfer. Circle thus attests electronically to the transfer of assets. The attacker repeatedly used the CCTP to transfer assets during the exploit, and Circle thus repeatedly provided the "attestations" necessary for the transfers to occur.

45. Circle has repeatedly represented that the CCTP is safe and secure. For example, in offering documents for its initial public offering, Circle stated: "With CCTP, end-users can safely and cost-efficiently transfer USDC from one supported blockchain to another." Circle has represented that its transfer protocol is "[t]he most secure way to transfer USDC crosschain" and that "every crosschain transfer is validated by Circle, the same company you already trust for holding and transaction with USDC." Circle has stated: "We build and support stablecoin infrastructure that is designed to enable Circle stablecoins to flow safely and easily across blockchain networks and remove friction and complexity in the end-user experience for stablecoin transactions. Finally, we provide easy-to-use, cloud-based tools that aim to simplify the underlying technology for developers (whether at startups or within major institutions), and make it easier for them to build, deploy, and operate innovative applications, with strong out-of-the-box features for using the Circle stablecoin network."

46. Circle had the ability to block the transfer of assets stolen in the exploit. Indeed, when Plaintiff notified Circle that some of the stolen USDC had become trapped within Wormhole, a messaging protocol that can be used to transfer USDC from one blockchain to another, Circle "blocked" the wallet that otherwise would have received USDC. This block was immediate and effective. Circle only blocked this wallet and did not block any of the other transactions.

47. As a centrally important market participant in digital assets, and a regulated entity, including as a Florida money transmitter, Circle is held to a standard of care that focuses on ensuring the security and legality of digital asset and money transmission operations. If the assets involved in the Cetus Protocol exploit had been cash instead of crypto, Circle would have had regulatory obligations not to facilitate the laundering of money by repeatedly certifying suspicious transaction. Circle is held to a standard of care applicable to its central role as the issuer of USDC and creator of the CCTP.

48. Instead of blocking the assets as the standard of care required, Circle, through the CCTP, signed or "attested" to each of the transactions, one after another, even after it should have been clear to Circle that the USDC it issued was being laundered using its CCTP protocol.

49. The details of the transactions in the exploit are set forth in the Appendix. Inca's investigation traced two Sui wallets that received stolen funds:

Wallet 1:

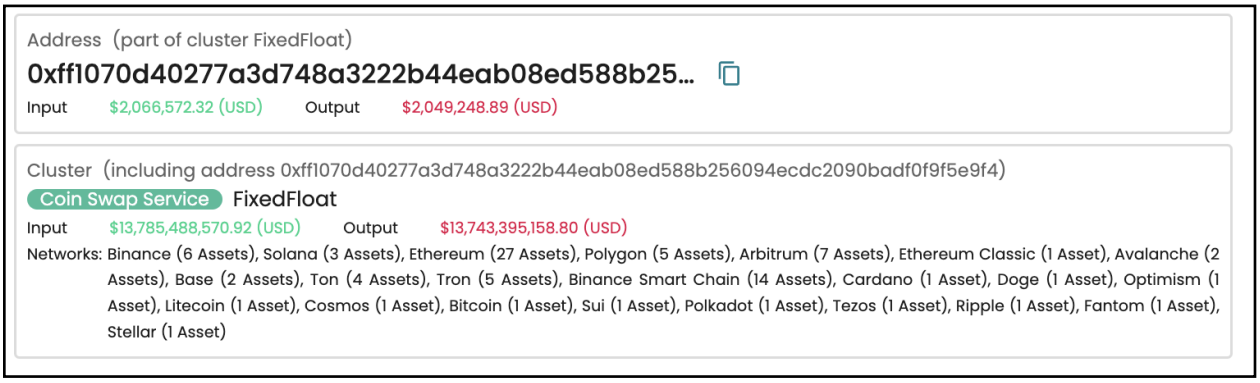
0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06

Wallet 2:

0xcd8962dad278d8b50fa0f9eb0186bfa4cbdecc6d59377214c88d0286a0ac9562

50. 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 what is known as the mempool level.

51. Wallet 1 had been funded three days before the exploit by 0xff1070d40277a3d748a3222b44eab08ed588b256094ecdc2090badf0f9f5e9f4. Inca identified this address as one of FixedFloat's main wallets.



52. Inca further identified Twitter (X) posts mentioning this wallet as having been involved in a previous scam. For example, at X the following post was made by G0ODMONEY on May 5, 2025.

53. As noted above, the attacker also bridged approximately $61 million in USDC in transactions that were not frozen. The bridged funds were distributed to two Ethereum wallets. Approximately $8 million was distributed to Wallet 3: 0x89012a55cd6b88e407c9d4ae9b3425f55924919b. Approximately $53 million was distributed to Wallet 4: 0x0251536bfcf144b88e1afa8fe60184ffdb4caf16.

54. On May 22, 2025, Wallet 1 bridged funds to Wallet 3, including an Ethereum bridge transaction that involved $932,137.18 of USDC at issue here. The transaction is recorded at:

https://suivision.xyz/txblock/A9AK5FvtpBNUsB676KCaY4Wq3BwhmayyHWZB3cxPWHvh.

These USDC assets are the assets that this Court previously ordered Circle to block, and that Circle immediately and effectively blocked.

55. As a result of Circle's block of these assets, Circle holds $932,137.18 of reserve assets that are no longer associated with an obligation of Circle. Circle has thus been unjustly enriched by $932,137.18. Plaintiff's claim for unjust enrichment and constructive trust applies to this $932,137.18 of USDC that the attacker once held, but that is now permanently blocked, due in significant part to Circle's action. For clarity, before the block, Circle had a USDC obligation of $932,137.18 and corresponding reserve assets of $932,137.18. Now, Circle has no USDC obligation yet still possesses those reserve assets. Accordingly, Circle has been unjustly enriched and should pay Plaintiff the value of these assets. Circle could satisfy this claim by transferring its reserve assets and the income it has earned on these assets to Plaintiff.

56. Plaintiffs claim for negligence applies to the additional USDC that the attacker previously held, and was able to launder, due in significant part to Circle's failure and inaction. Circle was provided with notice of the Cetus Protocol hack immediately and had the capacity to

monitor the USDC transactions in real time. Circle had control of the CCTP protocol throughout the attack. The transactions involved USDC issued by Circle. With respect to the unblocked transfers set forth in the Appendix, Circle did not observe the required standard of care.

FIRST CAUSE OF ACTION (Against the Non-Circle Doe Defendants)
CONVERSION

57. Plaintiff realleges and incorporates by reference paragraphs 1-56 as if stated fully in herein.

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

59. The non-Circle Doe 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.

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

SECOND CAUSE OF ACTION (Against Circle)
NEGLIGENCE

61. Plaintiff realleges and incorporates by reference paragraphs 1-56 as if stated fully in herein.

62. Defendant Circle owed a duty to Plaintiff arising from its special role as the issuer of USDC, the creator of the CCTP, and its role in implementing the CCTP.

63. Defendant breached its duty by failing to block the transactions set forth in the Appendix, and by permitting the Doe Defendants to use Circle as a platform to transfer and traffic in Plaintiff's stolen funds.

64. Defendant Circle's breach caused Plaintiff damages and continues to cause Plaintiff damages.

65. Plaintiff was harmed from Defendant Circle's breach in the amount of $61,302,690.

THIRD CAUSE OF ACTION (Against Circle)
UNJUST ENRICHMENT AND IMPOSITION OF CONSTRUCTIVE TRUST

66. Plaintiff realleges and incorporates by reference paragraphs 1-56 as if stated fully herein.

67. Circle was conferred a benefit with respect to the USDC that were stolen by the Doe Defendants and that are now blocked by Circle.

68. Circle is currently in possession of reserve assets backing the USDC it has blocked and retains the benefit conferred onto it by Plaintiff indirectly.

69. It would be inequitable and unconscionable to permit Circle to retain the above property and proceeds.

70. To redress this inequity and prevent further harm, Plaintiff seeks restitution and the imposition of a constructive trust on the $932,137.18 of reserve assets held at Circle, the amount of the USDC assets stolen from Plaintiff and blocked by Circle.

71. Plaintiff has no adequate remedy at law to recover specific property or to prevent future harm from further transfer, waste, or alienation of the its stolen property.

FOURTH CAUSE OF ACTION (Against All Defendants)
DECLARATORY JUDGMENT

72. Plaintiff realleges and incorporates by reference paragraphs 1-56 as if stated fully herein.

73. This is a claim for declaratory relief pursuant to Chapter 86, Florida Statutes.

74. A bona fide, actual, present, and practical need exists for a judicial declaration as to the rights, powers, and obligations of the parties arising from theft of cryptocurrency by the Doe Defendants, including assets blocked by Circle.

75. Upon information and belief, Circle does not claim any ownership interest in the disputed USDC that Circle has blocked.

76. Plaintiff contends the stolen sums should be returned to the Plaintiff, and that Plaintiff's interest is superior to that of the Defendants.

77. Circle is essentially a stakeholder, and the full sum of $932,137.18 should be deposited into the Court registry in an interpleader action, so that the Plaintiff and the Doe Defendants can contest the ownership of the funds.

78. The declaration sought herein relates to a present, ascertained controversy arising from a specific and identifiable illicit transfer of cryptocurrency, which is now being held by a third party, Circle.

79. Accordingly, Plaintiff and Defendants have real, present, adverse, and antagonistic interests in the subject matter of this action that are appropriate for resolution through declaratory judgment.

80. These interests are all before the Court by proper process and are not hypothetical or speculative.

81. A declaratory judgment is necessary to resolve the parties' legal and equitable rights with respect to the ownership and possession of the USDC.

82. Without such a declaration, Plaintiff faces irreparable harm to its rights.

Wherefore, Plaintiff respectfully requests: (1) an Order rescinding the freeze of wallet 0x89012a55cd6b88e407c9d4ae9b3425f55924919b and directing Circle to unblock this wallet and to return any of the previously blocked $932,137.18 that subsequently is received by this wallet, or to otherwise deliver the sum of $932,137.18 to Plaintiff, within 30 days of receipt by any reasonable means; (2) an award to Plaintiff of damages in the amount of $60,370,553, the value of all assets illegally converted and laundered but not blocked, as set forth in the Appendix, including the U.S. dollar equivalent of 3,144 ETH transferred from wallet address 0x89012a55cd6b88e407c9d4ae9b3425f55924919b and the U.S. dollar equivalent of 20,000 ETH transferred from wallet address 0x0251536bfcf144b88e1afa8fe60184ffdb4caf16; (3) pre-judgment interest; (4) attorneys' fees and costs incurred in prosecuting this action; and (5) any other relief that the Court finds just and proper.

Dated: September 22, 2025

CERTIFICATE OF SERVICE

I hereby certify that on this 22nd day of September, 2025, the foregoing Amended Complaint has been served on the Doe Defendants who have not yet entered an appearance on this case, by placing the foregoing and all attachments in the service website which was authorized by the Court in its Order of June 29, 2025. Circle will be served pursuant to Chapter 48 of the Fla. Stat.

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

Appendix (Sui to Ethereum USDC Bridge Transaction Details)

Date/Time	Sender Address	Recipient Address	$ Amount	Transaction Hash
5/22/25 11:46	0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5dc8ff06	0x89012a55cd6b88e407c9d4ac9b3425f55924919b	885,527.33	4ja25Jhz1TQLzacviefnXn8vGVHBmMELwKqpNCEqahzC
5/22/25 11:41	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	4Pb4Sp2a2MhGArbFi9fYLhGc2PuyygQa2nJVmSchGTKp
5/22/25 11:39	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	HWd9KkWPeNRvEHF2bCqcjxb67kn5z3gbi7diHuzpp3ju
5/22/25 11:38	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	7gikH1pGQcyP9m2bzMiWAypaRkwK2JhNeuGU8CnPdCw9
5/22/25 11:38	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	Aw2r3yG7ucpysGFfGtheoCfM6m3MkJwh6fGpBhWbyfKt
5/22/25 11:37	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	FRw8KZVzyaAEggtr4Srhx7ax22YoJtkkBHrpnDga4kzp
5/22/25 11:30	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	429,312.80	5zt4BxGuCVw5wFxWfZ2x7sf3Pdkp3pF5LXAU88eeZxib
5/22/25 11:30	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	EtNPxe2mw46SAaAhSXrXDykczVY8gBn976oP7Gzt2qF
5/22/25 11:29	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	FdUPsGam1MVGdbWkT3rCrggUEF7CBoz63ep619RsHW3G
5/22/25 11:29	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	H6WrQmUgPBAFLSguW8R1EfKkVnKWR3sBLTDAKgAQzaSJ
5/22/25 11:28	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	8UwnAzdeuLip9WcYygfE9wGwLr1j59iUuHKwWucDzE52
5/22/25 11:28	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	vmDpSCp7MEBGiyMooRzqyyCou6sMyVpucXbUPAibXFv
5/22/25 11:28	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	E1baWqHUiKmhG3npdwmcb4L6YzYX4eDndSm7UyQfSG7Y
5/22/25 11:27	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	HG3eVmgk2iN8C97Xcc78GvMHLvbSHssLWPAdLVQRCUja
5/22/25 11:27	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	EuHes8rMeSc23o2jDJqaeA7tRZ21XjAgZ4wCTS9tqWNB
5/22/25 11:27	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	ByZZZ6fuwCXEcXpgXGD9sKtZVvS6aaCeyBcr9Bs1hGUu
5/22/25 11:26	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	DpUxAeMStvCQpi2rvACBBecRg3zrCcdyuJqYriGcy4xx
5/22/25 11:26	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	2vmt82AyMQNZ4ouQjNw3MiqNq6heuF74G61yKdQDKX95
5/22/25 11:25	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	EWcFxbqHENXt9zavWo6DfassKA94sA6ZtyQs9uqfbp6Q
5/22/25 11:25	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	38nQQwTdXzmjTk5s76LfVmU8DDWJhjkDDiXdBjmddzWk
5/22/25 11:25	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	DqptYYYnqFvgziuT4vmYTQH3KVpNmfWmCp8EQVYcQCpB
5/22/25 11:24	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	GQAArGh6URPMx2i7hUW68gMBGH2jMadUT6RCkMR9F81s
5/22/25 11:24	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	BRBNH9wKsZycqfhkNTNdbXByB9jBYyzzFmgfXWdM4QsB
5/22/25 11:24	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	9sWeYQHGKzfHLgydwXETVAYegzZr1bKoutNgqfVU6WB6
5/22/25 11:23	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	6Em1Kb4XJgJPYDDpwqrA34P4rp5w7uCBeg2SVuBjL2Qx
5/22/25 11:23	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	5tHgthw3oKFK9Mhx241W3yHYhkF1jDP59uiRw1TVjvED
5/22/25 11:23	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	AZKYBygx8rKaTnQtkwA1aHMPWScFg34wqE1uVtQPLhBc
5/22/25 11:22	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	7UcdrMquakrAmirC71kArPUHAvGAFzpuc9S3A743oWTZ
5/22/25 11:22	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	2vM3swpkciR5fJgbHcA6wLi9Ug7weSGA8FAJfa6xZFqC
5/22/25 11:21	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	8iLTz3xm6iuYFGG6wY42qVEZ3R7Vr3ARDPqTxZjQURRP
5/22/25 11:21	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	4m2BJjJ5CXrne55oSkwMCVRPPdd3R7XkBx1wKRkSQhdW
5/22/25 11:20	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	6jogQUhvthRCipTkbzU21Ez42TzTJNHCtncKzN3TDegF
5/22/25 11:20	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	DdRhe8f3TZ2nLzr9q9cGuUhG1xaRzPv86PgDSnA1PjKn
5/22/25 11:19	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	2fJFaJaB4TLboeCZZgrFYuc4moQE9AMqBmVe9EqAWH4F
5/22/25 11:18	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	7TVrCpxEr6iiWTjFgy1L54PvSNzkA4PgazBMAwJ2zbtW
5/22/25 11:18	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	64cdvsr5sJf4F11hUSsn1ypahooBQtiLdoRqKp6LVpVh
5/22/25 11:18	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	9GCd1cz6ob4fzD6hSBVChATVZwjanS252dBxPtvnbNrE
5/22/25 11:17	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	CokaMXYB1oZpyVQDzPnyPaJdmV1uSeCQtMES2e2WSMux

5/22/25 11:17	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	Bt6bcFAvq7zNus1jAQxDUz5WtDecitY67AhZtfAfPf2d
5/22/25 11:16	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	B8YdU6Wutn86VRXY7eSr4oB6eahtZnUWqRYrP1udgVxu
5/22/25 11:16	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	GTGKViDGp84mX31f6cFwpWTbrDcrj8LwRSbrTuaWy2zF
5/22/25 11:15	0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06	0x89012a55cd6b88e407c9d4ac9b3425f55924919b	999,801.00	EGJwgj5A5eA6ez8mym1DGNZQFksRfuN8VTfjNyWjwHGS
5/22/25 11:15	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	7fK6ZwQ65SCieALBeEuGaFLnaMrjSK83LeHJZNniiRTp
5/22/25 11:14	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	3qxJSMQon1YVZSuA9VXZG3LN7VrTnTSXvjKV2qqxwuvT
5/22/25 11:14	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	DuaJGMf7wZLjNrcD4xMLKEwr7YsF9RAHj6uBp2f2tbWk
5/22/25 11:13	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	Dc5eKFJc2dHbXATQs8CJWyZjeDrxMwW8awUeHoT6EPc7
5/22/25 11:13	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	EJxFDJiADMpLZM1q7BFgdZ1DFNUR6hRFXsoztTfUGzXH
5/22/25 11:12	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	Hi1yQB22vV1xxeGAUhMp2hzmkqXUoyF4S3QWrjaPda2H
5/22/25 11:11	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	9vEa4RiHqS9QyqCVnofcfqg3ZkwXxRvjRi3xGPYfxpix
5/22/25 11:09	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	B2fKTanbV5c3bvwHdMmoTLob7omKxWNiqa8cRVa65TGD
5/22/25 11:09	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	CwrqZtGVcYE96RVCtNG84b64Ci5fqHcGwmxGw1qrx6u
5/22/25 11:08	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	Dv2cn3cSuShmXi8sxJPePUi6x1FYH4Q7SL9BmaWhPJFT
5/22/25 11:08	0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06	0x89012a55cd6b88e407c9d4ac9b3425f55924919b	999,801.00	636mENWdF15LZZkRdxGEmU68Mkwdx28wvP6oT6PKRkAT
5/22/25 11:07	0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06	0x89012a55cd6b88e407c9d4ac9b3425f55924919b	999,801.00	B1gmQY1mx9wizkmqYKco1ikAa8ngUSxVekfVs9crF95e
5/22/25 11:06	0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06	0x89012a55cd6b88e407c9d4ac9b3425f55924919b	999,801.00	8YtbaVThREJphZZdLb5QTQiV6cuHGsHDhe6efuL82dLD
5/22/25 11:05	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	H9hBZPEtLdyg1n7huAcyLRo2WR15GzFuTPJEc8PLvALY
5/22/25 11:04	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,801.00	EkqjJ17YAseUj4WrzDdHi7VH6djeB7FUgFbwuRWSRCqF
5/22/25 10:53	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,759.00	eHAFc5ctXE1Kg8HMWhUqBDtT53hdMnd4bZSCYxWBxyj
5/22/25 10:52	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,759.00	7uSED3JRT3qVW9HKZ9BmyEzBPeCVM4JRNugGXh6iqUtG
5/22/25 10:51	0x94ba2717436c9fd765ba44831d23d7c4a0910a8aa33f32c242f6de561c89f8c4	0x875d6d37ec55c8cf220b9c5080717549d8aa8eca	999,759.00	6jMEFeap2GqxcdFJPrQckmPwC78FeFodmkdCCjnFRWWb
5/22/25 10:51	0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06	0x89012a55cd6b88e407c9d4ac9b3425f55924919b	999,759.00	7o468B3ZYTeJ9TMW1y2xsQhNvT35apTUZX5TWc4K1oaz
5/22/25 10:47	0xe28b50cef1d633ea43d3296a3f6b67ff0312a5f1a99f0af753c85b8b5de8ff06	0x89012a55cd6b88e407c9d4ac9b3425f55924919b	999,759.00	2bzu8xPvgF4R9fBqspHVweZx2y55whVQcCwb2qxfxV3D