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

SUI FOUNDATION, LTD. d/b/a
DEEPBOOK, a British Virgin Islands
business company,

Plaintiff,

v.

DOE NOS. 1–25,

Defendants.
_____/

COMPLAINT

Plaintiff SUI FOUNDATION, LTD. d/b/a DEEPBOOK ("Plaintiff" or "DeepBook"), by and through its undersigned counsel, Xander Law Group, P.A., hereby sues Defendants DOE NOS. 1–25 (collectively, "Defendants"), and alleges as follows:

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff SUI FOUNDATION, LTD. d/b/a DEEPBOOK is a British Virgin Islands business company that operates and maintains the DeepBook Protocol, a decentralized financial platform and liquidity infrastructure deployed on the Sui blockchain and utilized by individuals and entities throughout the world, including residents of the State of Florida.

2. COINEX TECHNOLOGY LIMITED ("CoinEx") is, upon information and belief, a foreign corporation that owns and operates the CoinEx digital asset exchange, a centralized cryptocurrency trading platform that provides services to users throughout the United States, including residents of Florida.

3. CoinEx provides digital asset exchange, custody, deposit, withdrawal, and related financial services to customers residing in Florida and throughout the United States.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

4. Defendants DOE NOS. 1–25 are individuals and/or entities whose identities are presently unknown. Upon information and belief, these Defendants participated in, directed, assisted, facilitated, benefitted from, or otherwise aided the wrongful conduct alleged herein, including the exploitation of the DeepBook Protocol, the theft and conversion of digital assets, the laundering and transfer of stolen assets, and the concealment of the proceeds thereof. Plaintiff will amend this Complaint to identify such Defendants as their identities become known.

5. This Court has subject matter jurisdiction because the amount in controversy exceeds Fifty Thousand Dollars ($50,000.00), exclusive of interest, costs, and attorneys' fees.

6. This Court has personal jurisdiction over the Doe Defendants because, upon information and belief, they intentionally directed tortious conduct toward Plaintiff and users of the DeepBook Protocol located within Florida and knowingly utilized platforms, services, and infrastructure accessible within Florida in furtherance of their wrongful conduct.

7. Venue is proper in Miami-Dade County, Florida because a substantial portion of the events giving rise to the claims occurred within or were directed toward this County, Plaintiff conducts substantial business affecting residents of this County, Defendants conduct business within this County, and the wrongful conduct alleged herein caused injury to Plaintiff and to users and market participants located in Miami-Dade County.

8. Plaintiff reserves the right to amend this Complaint to identify additional defendants and assert additional claims as discovery and investigation continue.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

STATEMENT OF FACTS

11. DeepBook is a decentralized financial protocol deployed on the Sui blockchain. DeepBook functions as a central liquidity layer within the Sui ecosystem and facilitates digital asset trading and related financial transactions for users located throughout the world, including residents of Florida.

12. As part of its operations, DeepBook offers margin trading functionality through a system that permits users to borrow digital assets against collateral and utilize such assets for trading activities.

13. The DeepBook margin system is comprised primarily of two interconnected components: (a) liquidity pools that hold digital assets supplied by users and serve as lending sources for margin transactions, and (b) margin accounts maintained by borrowers that hold collateral, borrowed assets, and trading positions.

14. To protect the integrity of the protocol and the assets deposited by users, DeepBook employs risk-management mechanisms designed to ensure that borrowers maintain sufficient collateral to support outstanding obligations.

15. Among these safeguards is a requirement that each margin account maintain a minimum collateralization threshold relative to its outstanding debt. If a margin account falls below the required threshold, the account is intended to become subject to liquidation procedures designed to protect deposited assets and preserve the solvency of the protocol.

16. On or about May 9, 2026, unknown threat actors identified and exploited a vulnerability within the DeepBook Margin Protocol.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

17. The vulnerability arose from a flaw in the protocol's margin trading logic whereby certain transactions could be executed without adequately verifying the continued solvency of a borrowing account after completion of the transaction.

18. Although the protocol verified certain pricing parameters associated with individual trades, the protocol did not consistently recalculate whether the borrowing account remained sufficiently collateralized following execution of those trades.

19. Defendants knowingly exploited this vulnerability by utilizing accounts under their control to engage in a coordinated series of manipulative transactions designed to extract value from the protocol.

20. Specifically, Defendants controlled both the borrowing accounts and the counterparty accounts involved in the transactions.

21. Using these accounts, Defendants executed a series of self-directed transactions commonly referred to as "wash trades", through which value was systematically transferred from borrowing accounts containing protocol assets into accounts controlled by Defendants.

22. By repeatedly engaging in such transactions, Defendants caused the borrowing accounts to become insolvent while simultaneously transferring substantial value to wallets under their control.

23. As a result of Defendants' conduct, DeepBook incurred substantial losses and the affected margin accounts became incapable of repaying assets borrowed from the protocol's liquidity pools.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

24. The exploit was executed through five coordinated transaction blocks occurring between approximately 03:18:15 UTC and 04:23:03 UTC on May 9, 2026.

25. Through these transactions, Defendants extracted approximately 236,144.58 USDC and 5,608.49 SUI, representing a combined value of approximately $242,222.41 at the time of the exploit.

26. The total loss suffered by the protocol exceeded the value directly extracted by Defendants because the exploit generated substantial unrecoverable debt within the margin system.

27. As a direct and proximate result of Defendants' conduct, the protocol sustained losses totaling approximately 283,604 USDC.

28. To protect protocol participants and preserve the integrity of the DeepBook ecosystem, Plaintiff was required to provide a capital infusion sufficient to satisfy the deficit created by Defendants' actions and restore the protocol to solvency.

29. Plaintiff therefore sustained direct damages in an amount no less than 283,604 USDC, exclusive of additional damages, costs, expenses, prejudgment interest, and other relief recoverable under applicable law.

The Forensic Investigation and Tracing of the Stolen Assets

30. Immediately following discovery of the exploit, Plaintiff commenced an investigation into the theft and movement of the misappropriated assets. See attached Report as Exhibit 1.

31. As part of that investigation, Plaintiff retained blockchain forensic investigators to analyze the exploit, identify wallets involved in the attack, trace the movement of stolen assets, and determine the source and destination of funds associated with the exploit.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

32. Blockchain transactions are permanently recorded on distributed ledgers and create an immutable record of transfers between wallet addresses. As a result, digital assets can frequently be traced through successive transactions even when an actor attempts to conceal ownership through the use of multiple intermediary wallets.

33. Utilizing blockchain forensic techniques, investigators reconstructed the flow of assets associated with the exploit and identified multiple wallets used by Defendants to facilitate the theft, movement, concealment, and laundering of the stolen assets.

34. The investigation revealed that the exploit was not conducted through a single wallet or isolated transaction, but rather through a coordinated network of wallets operating in concert and under common control.

35. Investigators identified multiple wallets on the Sui blockchain that participated in the exploit and subsequently received, transferred, or controlled assets derived from the exploit.

36. The investigation further revealed that the wallets utilized by Defendants were funded and prepared in the days preceding the exploit through transactions originating from infrastructure associated with CoinEx.

37. Specifically, investigators identified a wallet commonly referred to as the CoinEx Omnibus Wallet bearing address: 0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb.

38. The CoinEx Omnibus Wallet is owned, operated, controlled, or maintained by CoinEx in connection with its cryptocurrency exchange business.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

39. Blockchain records reviewed during the investigation revealed transfers originating from the CoinEx Omnibus Wallet and directed to wallets later utilized by Defendants in connection with the exploit.

40. The investigation revealed that wallets utilized by Defendants in connection with the exploit received funding through a series of transactions occurring in the days immediately preceding the attack.

41. Investigators determined that a wallet utilized by Defendants in connection with the exploit received digital assets directly from the CoinEx Omnibus Wallet on multiple occasions prior to the exploit.

42. Investigators further determined that a second wallet utilized by Defendants received assets both from the first threat actor wallet and directly from the CoinEx Omnibus Wallet.

43. The investigation additionally identified transactions between a threat actor wallet and a CoinEx Hot Wallet associated with the operation of CoinEx's exchange platform.

44. Based upon the timing, sequence, and nature of these transactions, investigators concluded that the exploit wallets maintained operational connectivity with infrastructure controlled by or associated with CoinEx.

45. The investigation further revealed that an additional threat actor wallet was funded by another threat actor wallet shortly before multiple exploit transactions were executed, demonstrating coordination among the wallets involved in the attack.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

46. Collectively, the traced transactions established a continuous funding chain connecting the exploit wallets to CoinEx infrastructure and demonstrating that the wallets utilized during the exploit did not operate independently of one another.

47. Based upon the tracing analysis, Plaintiff is informed and believes that the individuals responsible for the exploit utilized one or more CoinEx accounts in connection with the planning, funding, preparation, execution, and subsequent concealment of the stolen assets.

48. Upon information and belief, CoinEx possesses records capable of identifying the individuals who controlled the wallets involved in the exploit and the subsequent movement of the stolen assets.

49. Such records include, but are not limited to, account registration information, customer identification records, Know Your Customer ("KYC") records, Anti-Money Laundering ("AML") records, login information, IP address information, device identifiers, transaction histories, withdrawal records, deposit records, and related account activity.

50. Following completion of the exploit, Defendants began transferring the stolen assets through a series of intermediary wallets in an effort to obscure the source and ownership of the funds.

51. The investigation determined that Defendants subsequently transferred a substantial portion of the stolen assets from the Sui blockchain to the Ethereum blockchain through a cross-chain bridge.

52. Through this process, assets originating from the exploit were transferred from the Sui blockchain and credited to Ethereum wallets controlled by Defendants.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

53. The investigation identified an Ethereum wallet that served as an aggregation point for assets transferred from the Sui blockchain following the exploit.

54. Investigators further identified a subsequent Ethereum wallet into which the stolen assets were consolidated after leaving the aggregation wallet.

55. Upon information and belief, the latter wallet presently serves as a repository for assets traceable to the exploit.

56. Blockchain forensic analysis successfully traced the stolen assets from the exploit wallets on the Sui blockchain, through the cross-chain transfer process, into the aggregation wallet, and ultimately into the final destination wallet controlled by Defendants.

57. As of the date of the forensic investigation, assets derived from the exploit remained identifiable on public blockchains and capable of being traced to wallets controlled by Defendants.

58. The investigation established a continuous tracing path from the exploit transactions, through the intermediary wallets utilized by Defendants, and ultimately to wallets containing assets derived from the theft.

59. Despite Defendants' efforts to conceal their identities and the movement of the stolen assets through multiple wallets and blockchain networks, investigators successfully reconstructed the path of the stolen assets and identified infrastructure capable of revealing the identities of the individuals responsible for the exploit.

60. The movement and retention of the stolen assets were conducted without authorization, without legal justification, and in derogation of Plaintiff's rights in and to those assets.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

Plaintiff's Damages

61. As a direct and proximate result of Defendants' conduct, the DeepBook Protocol suffered substantial losses and incurred a significant deficit within its margin lending system.
62. The exploit rendered certain borrowing accounts insolvent and created unrecoverable debt within the protocol's liquidity pools.
63. In order to protect users of the DeepBook Protocol and preserve the integrity and stability of the ecosystem, Plaintiff undertook immediate remedial measures following discovery of the exploit.
64. As part of those remedial efforts, Plaintiff provided a capital infusion sufficient to eliminate the deficit created by Defendants' conduct and restore the affected liquidity pools to solvency.
65. Plaintiff funded and satisfied the losses caused by Defendants' actions and thereby absorbed the economic harm resulting from the exploit.
66. As a result, Plaintiff suffered direct damages in an amount no less than 283,604 USDC, representing the deficit created by Defendants' misconduct and subsequently funded by Plaintiff.
67. In addition to the capital infusion required to restore the protocol, Plaintiff incurred and continues to incur substantial costs associated with investigating the exploit, tracing the stolen assets, identifying the responsible parties, securing evidence, mitigating damages, and pursuing recovery of the stolen property.
68. Defendants have refused and continue to refuse to return the stolen assets or otherwise compensate Plaintiff for the losses caused by their conduct.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

69. As a direct and proximate result of Defendants' actions, Plaintiff has suffered damages in an amount to be proven at trial, together with all other relief permitted under law and equity.

COUNT I
CONVERSION
(Against All Defendants)

70. Plaintiff realleges and incorporates by reference paragraphs 1 through 69 as though fully set forth herein.

71. Plaintiff owned, possessed, controlled, or otherwise had an immediate right to possess the digital assets and funds described in this Complaint, including the assets wrongfully obtained through the exploitation of the DeepBook Protocol.

72. The digital assets at issue constitute specific and identifiable property capable of ownership, possession, tracing, recovery, and return.

73. Through the exploit described above, Defendants intentionally and wrongfully exercised dominion and control over Plaintiff's property.

74. Defendants knowingly manipulated the DeepBook Margin Protocol, caused assets to be transferred from protocol-controlled accounts, and appropriated those assets for their own use and benefit.

75. Defendants exercised unauthorized dominion and control over Plaintiff's property in a manner inconsistent with Plaintiff's ownership rights.

76. Following the exploit, Defendants transferred, concealed, laundered, retained, and otherwise exercised control over the stolen assets and proceeds derived therefrom.

77. The stolen assets were transferred through multiple intermediary wallets, bridged across blockchain networks, and consolidated into wallets controlled by Defendants.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

78. Despite Defendants' efforts to conceal the stolen assets, Plaintiff's investigation successfully traced the assets and established a continuous tracing path connecting the exploit to wallets controlled by Defendants.
79. Upon information and belief, assets derived from the exploit remain identifiable and traceable to wallets controlled by Defendants.
80. CoinEx possesses information, records, and account data identifying the individuals and accounts that received, controlled, transferred, or otherwise exercised dominion over the stolen assets.
81. By wrongfully obtaining, possessing, transferring, concealing, retaining, and exercising control over Plaintiff's property, Defendants committed conversion under Florida law.
82. As a direct and proximate result of Defendants' conversion, Plaintiff suffered damages including, but not limited to, the loss of approximately 283,604 USDC, investigative expenses, mitigation costs, and other damages in an amount to be proven at trial.
83. Defendants' conduct was willful, intentional, malicious, and undertaken with knowledge that the assets belonged to Plaintiff or were obtained through unauthorized means.

WHEREFORE, Plaintiff, SUI FOUNDATION, LTD. d/b/a DEEPBOOK, respectfully requests that this Court enter judgment in its favor and against Defendants DOE NOS. 1–25, award compensatory damages in an amount to be proven at trial, together with prejudgment interest, taxable costs, and all other relief available under law and equity, and grant such further relief as this Court deems just and proper.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

COUNT II
UNJUST ENRICHMENT AND IMPOSITION OF CONSTRUCTIVE TRUST
(Against all Defendants)

94. Plaintiff realleges and incorporates by reference paragraphs 1 through 69 as though fully set forth herein.

95. Through the exploit described above, the Doe Defendants obtained and retained digital assets belonging to Plaintiff without authorization, legal justification, or compensation.

96. The Doe Defendants knowingly accepted, received, possessed, transferred, and retained the benefits derived from the stolen assets.

97. The assets obtained by the Doe Defendants were derived directly from the exploitation of the DeepBook Protocol and from property rightfully belonging to Plaintiff.

98. As a result of the exploit, the Doe Defendants received substantial benefits, including digital assets having a value of no less than approximately 283,604 USDC.

99. The Doe Defendants appreciated, accepted, and voluntarily retained those benefits.

100. It would be inequitable, unjust, and contrary to principles of equity and good conscience for the Doe Defendants to retain the benefits obtained through the exploit.

101. Plaintiff has suffered damages as a direct result of the Doe Defendants' retention of assets and proceeds derived from the exploit.

102. Plaintiff's investigation has successfully traced the stolen assets through multiple wallets and blockchain networks and has identified wallets presently containing assets derived from the exploit.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

103. Upon information and belief, assets traceable to the exploit remain identifiable and under the possession, custody, or control of the Doe Defendants.

104. Because the stolen assets and their proceeds remain identifiable and traceable, equity requires the imposition of a constructive trust over such assets and any proceeds, substitutions, derivatives, or property acquired therefrom.

105. The Doe Defendants should not be permitted to benefit from their wrongful conduct or retain property obtained through the exploitation of the DeepBook Protocol.

106. Plaintiff has no adequate remedy at law to recover the specific assets and proceeds presently traceable to the exploit.

WHEREFORE, Plaintiff, SUI FOUNDATION, LTD. d/b/a DEEPBOOK, respectfully requests that this Court enter judgment in its favor and against the Doe Defendants, order restitution of all benefits wrongfully obtained, impose a constructive trust over all assets traceable to the exploit and any proceeds derived therefrom, award prejudgment interest, costs, and grant such further legal and equitable relief as the Court deems just and proper.

COUNT III
DECLARATORY JUDGMENT
(Against All Defendants)

107. Plaintiff realleges and incorporates by reference paragraphs 1 through 106 as though fully set forth herein.

108. This is an action for declaratory relief pursuant to Chapter 86, Florida Statutes.

109. A bona fide, actual, present, and practical need exists for a judicial declaration regarding the rights, interests, and obligations of the parties arising from the theft, transfer,

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

laundering, and retention of digital assets wrongfully obtained through the exploitation of the DeepBook Protocol.

110. Plaintiff contends that the digital assets and proceeds derived from the exploit belong to Plaintiff and that Plaintiff's ownership interest in such assets is superior to any interest claimed by Defendants.

111. Upon information and belief, the Doe Defendants claim or purport to claim ownership, possession, custody, or control of assets traceable to the exploit.

112. Plaintiff's investigation has identified specific wallets containing assets derived from the exploit and has established a continuous tracing path connecting those assets to the wrongful conduct alleged herein.

113. CoinEx possesses information and records capable of identifying the individuals and accounts that controlled the wallets involved in the exploit and the subsequent movement of the stolen assets.

114. An actual controversy presently exists regarding the ownership, possession, control, and disposition of the assets derived from the exploit.

115. Plaintiff contends that all assets traceable to the exploit, together with any proceeds, substitutions, derivatives, or property acquired therefrom, rightfully belong to Plaintiff and should be returned to Plaintiff.

116. Defendants' interests are adverse, antagonistic, and directly contrary to Plaintiff's ownership rights.

Xander Law Group, P.A.
25 SE 2nd Ave Suite 808, Miami, FL 33131 | (305) 767-2001 | matt@xanderlaw.com

117. The declaration sought herein relates to a present and existing controversy involving specific and identifiable digital assets that have been traced through blockchain forensic analysis.

118. The parties' respective rights cannot be determined without judicial intervention.

119. A declaratory judgment is necessary to determine the ownership and possessory rights associated with the stolen assets and to resolve the parties' competing claims thereto.

120. Without such a declaration, Plaintiff will continue to suffer irreparable harm, including the continued deprivation of its property and uncertainty regarding its rights in assets traceable to the exploit.

WHEREFORE, Plaintiff, SUI FOUNDATION, LTD. d/b/a DEEPBOOK, respectfully requests that this Court enter a declaratory judgment determining that: (a) Plaintiff possesses the superior ownership interest in all assets traceable to the exploit described herein; (b) the Doe Defendants possess no lawful ownership interest in such assets; (c) any assets, proceeds, substitutions, or derivative property traceable to the exploit are subject to Plaintiff's superior rights; and (d) Plaintiff is entitled to recover such assets and proceeds, together with such other and further relief as the Court deems just and proper.

Respectfully submitted,

By: */s/Jose Teurbe-Tolon*___

XANDER LAW GROUP, P.A.
25 S.E. 2nd Avenue, Suite 808
Miami, Florida 33131
Telephone: (305) 767-2001
service@xanderlaw.com
jose@xanderlaw.com
Counsels for Plaintiff

Introduction

DeepBook is a decentralized Central Limit Order Book (CLOB) natively deployed on the Sui blockchain. Engineered as an institutional-grade matching engine, it serves as the foundational liquidity layer for the Sui ecosystem. Unlike traditional Automated Market Makers (AMMs), DeepBook's architecture supports high-frequency, on-chain execution of complex financial instruments including: spot trading, margin facilities, and leveraged positions, characterized by sub-second settlement finality.

On May 9, 2026 at approximately 03:18:15 UTC, a sophisticated threat actor executed a coordinated exploit targeting the DeepBook Margin Protocol. The perpetrator utilized five interconnected transactions to extract assets with an aggregate approximate fair market value of $242,222 USD. The total protocol loss was finalized at 283,604 USDC. Following a rapid forensic assessment, the Sui Foundation provided a full capital injection to cover the deficit. Due to this immediate indemnification, all depositor liabilities were met in full, and no individual liquidity providers or retail users experienced a loss of principal as a result of the incident.

Blockchain forensic analysis has traced the funding source of the exploit to the CoinEx Omnibus Wallet (0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb). This address is attributed to CoinEx (COINEX TECHNOLOGY LIMITED), a centralized digital asset exchange headquartered in Seychelles. As CoinEx enforces mandatory Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures, identifiable information regarding the actor associated with this wallet is presumed to be on record with the exchange.

Exploit Overview

DeepBook Margin operates as a leveraged extension of the DeepBook Core protocol, utilizing a creditor-debtor relationship between two primary entities: the Margin Pool and the Margin Manager. The Margin Pool acts as a decentralized vault where liquidity providers deposit assets to earn interest, effectively serving as the lender for the ecosystem. In contrast, the Margin Manager is a specialized borrower account held by an individual user. To maintain the system's integrity, every Margin Manager is required to maintain a "risk ratio"—a minimum amount of collateral relative to their debt. If an account's value drops below this safety threshold, the protocol is designed to trigger a liquidation to protect the lender's capital.

The security breach occurred because the protocol failed to verify account solvency during active trading. While the system correctly checked that a borrower was solvent when they first took out a loan, it only applied a "price check" during the actual trading process. This price check ensured that individual trades stayed within 5% of market value but failed to re-evaluate whether the user's total account still held enough collateral to cover their debt after the trade was finished. This created a critical blind spot: the protocol was effectively checking the validity of the transaction price while ignoring the resulting insolvency of the borrower's account.

EXHIBIT 1

The attacker exploited this oversight by controlling both sides of the transaction. By using a Margin Manager (the borrower) to trade against a separate personal account (the counterparty), the attacker executed a series of wash trades. These trades were priced just close enough to market rates to pass the protocol's price filters, yet they were intentionally structured to be economically disastrous for the borrowing account. Through this method, the attacker systematically transferred borrowed funds into their personal account. Because the protocol never re-calculated the borrower's risk ratio during these trades, the attacker was able to drain the account until it was entirely underwater.

This coordinated maneuver generated "bad debt" within the lending pools, as the borrowing accounts no longer possessed the assets required to repay the Vault. The theft was carried out across five distinct transaction blocks over approximately 65 minutes (from 03:18:15 UTC to 04:23:03 UTC). Although the protocol was paused roughly three hours after the initial exploit, the lending pool had already incurred a significant capital deficit. To prevent this deficit from impacting the public, the Sui Foundation provided a full capital injection to cover the loss, ensuring that all protocol depositors remained whole and did not suffer a loss of principal.

It is important to note that the total financial impact on the protocol exceeded the amount of cash physically extracted by the attacker. While the perpetrator walked away with approximately $242,222 USD, the total loss to the protocol, and the subsequent payout by the Sui Foundation, was 283,604 USDC. This $41,382 discrepancy represents the inherent costs of the exploit, including the accumulation of unpaid interest on the $1.1 million in borrowed funds and the protocol's internal liquidation penalties (calculated as a percentage of the debt). Essentially, the Foundation's capital injection did not merely replace the stolen assets; it covered the entire "bad debt" left behind by the insolvent accounts to ensure the lending pool was restored to a fully solvent state.

Analyst Note: A more in-depth explanation of the exploit can be found at Appendix A: Exploit Technical Deep Dive

Exploit Transactions on Sui

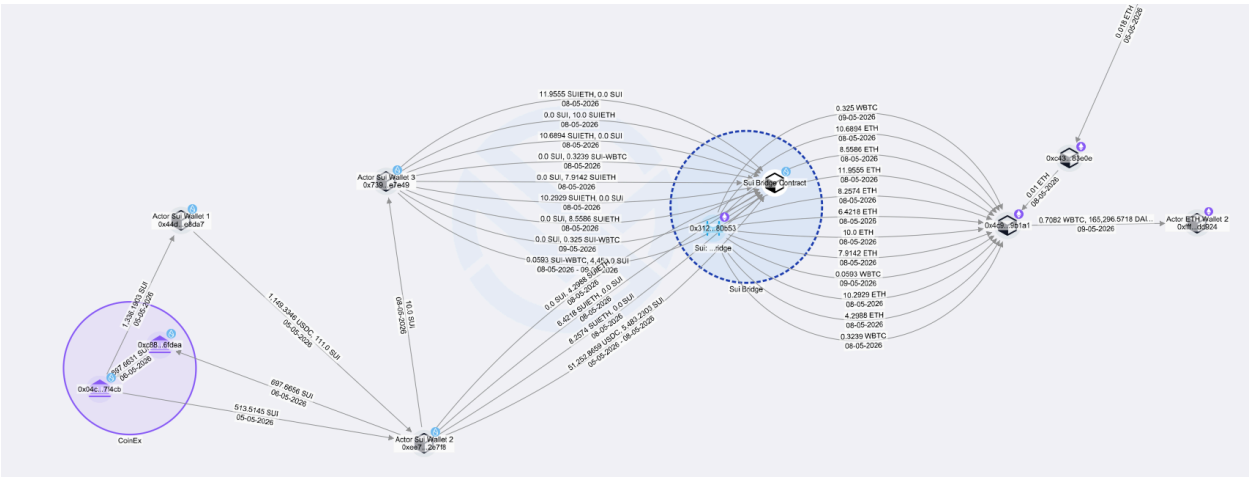
The following five transactions constitute the documented on-chain exploit, all occurring on May 9, 2026. The "Externally Extracted" column details the attacker's net balance changes, representing the USDC and SUI removed from the exploited margin managers via the aforementioned wash-trading mechanism.

Time UTC	Sui Transaction Digest	Externally Extracted

3:18:15	FgoNpxyducURr7B8vzHB3uixDj8SSHVG5jvYb3GAzJD5	44,309.62 USDC + 1,097.61 SUI
3:40:04	Bk9WsjM4BhhVKmVVgZoRHyaBGGsYAYX3AhGhhpqBQAZQ	44,070.72 USDC + 1,246.98 SUI
3:44:38	BYuPXAowtKktt9RHuWaXGqiEgyFvxe8sNbrJX73t4Lt8	103,167.43 USDC + 1,562.14 SUI
3:53:43	Frr1fnbrPVfjS5jrLaTETHBDnKznNFyHz2zPCHy1hSxK	18,354.24 USDC + 954.92 SUI
4:23:03	BWxFxA4F5YmKYLyiLTAXspQAopVzyzH4okVkJhjAFCmY	26,242.57 USDC + 746.85 SUI

The aggregate volume of assets externally extracted across the attacker's balance changes totaled 236,144.58 USDC and 5,608.49 SUI. Based on the spot prices at the time of each transaction, the total direct external extraction is valued at $242,222.41 USD.

On-Chain Investigation



DeepBook exploit public trace graph [1]

Threat Actor Wallets (Sui)

[1] Merkle: https://tracker.app.merklescience.com/shared/graph/052E386133A04EBD.

Label	Sui Address	Attribution
CoinEx Omnibus Wallet	0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb	CoinEx Omnibus
CoinEx Hot Wallet	0xc880e710b4c0dc2634e8191c152d7fcd59588e09fe81c270b707b7b79d86fdea	CoinEx Address Used by Threat Actor
Actor Sui Wallet 1	0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7	Threat Actor
Actor Sui Wallet 2	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	Threat Actor
Actor Sui Wallet 3	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	Threat Actor

Threat Actor Wallets (Ethereum) and Related Wallets

Label	Ethereum Address	Attribution
Actor Ethereum Wallet 1	0x4c9a14620ed8516238f0d6b9745d637d1609b1a1	Aggregated all Sui-Ethereum bridged stolen value
Gas Funder of Actor Ethereum Wallet 1	0xc4393c1b8463f18ae4e16ce39bde1ece55883e0e	Pre-positioned operator gas; funded the laundering intermediate
Actor Ethereum Wallet 2	0xfff00112e3fdA3d5C1CCA51bB05Df11822AdD924	Final resting wallet; as of May 12, currently holds 6.7 ETH + 0.7082 WBTC + 165,296.57 DAI
Sui-Ethereum Bridge	0x312e67b47a2a29ae200184949093d92369f80b53	Legitimate Sui-Ethereum bridge contract; NOT actor-controlled

Wormhole Receiver	0xa8969f3f8d97b3ed89d4e2ec19b6b0cfd504b212	Received Wormhole-bridged operator gas from Solana

Source of Funds

This section details the on-chain forensic investigation, utilizing backward tracing to establish a link between the exploit transactions and their point of origin. By identifying the most recent operational inflows for each participating wallet and tracing them to the preceding sender, we have established a clear funding chain originating from a CoinEx-attributed wallet. The following chronology moves in reverse-temporal order (from the exploit back to the initial funding).

Step 1: Exploit transactions (May 9, 2026, 03:18 to 04:23 UTC)

The five exploit transactions were executed by two distinct addresses. Actor Sui Wallet 2 executed the initial transaction at 03:18:15 UTC. Actor Sui Wallet 3 executed the remaining four transactions between 03:40:04 and 04:23:03 UTC.

Step 2: Trace Actor Sui Wallet 3 funding (back to 03:35:33 UTC on May 9)

Actor Sui Wallet 3 was funded approximately 17 minutes after the first exploit transaction and five minutes prior to its own first exploit. The funds originated from Actor Sui Wallet 2:

- Timestamp: 2026-05-09 03:35:33 UTC
- Transaction digest: Caxc4sTyy32Va3qDzVspLoAnrEEjYoGmXtczUshyuSWy
- From: 0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8
- To: 0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49
- Amount: 10.0 SUI

Step 3: CoinEx Hot Wallet Interaction (May 6, 2026)

On-chain data from May 6 identifies a clear deposit sequence, confirming active operational connectivity between Actor Sui Wallet 2 and a specific user account on CoinEx. This sequence follows the standard architecture of a centralized exchange deposit:

- **Actor Sui Wallet 2 to CoinEx Hot Wallet**
  - Timestamp: 2026-05-06 16:00:10.322 UTC
  - Transaction digest: 3Ynfq2exREaQepb6WqvbpUGy2iw3uDVfTDor3oXR8DSq
  - From: 0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8
  - To: 0xc880e710b4c0dc2634e8191c152d7fcd59588e09fe81c270b707b7b79d86fdea
  - Amount: 697.67 SUI
- **CoinEx Hot Wallet to CoinEx Omnibus Wallet**

    - Timestamp: 2026-05-06 16:01:48.554 UTC
    - Transaction digest: 7GDAziYLXcVPaDDMFAd97tnkp8eqQFqCrrDwW2vtK9M6
    - From: 0xc880e710b4c0dc2634e8191c152d7fcd59588e09fe81c270b707b7b79d86fdea
    - To: 0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb
    - Amount: 697.66 SUI

Step 4: Trace Actor Sui Wallet 2 funding (back to May 5, 2026 evening)

Actor Sui Wallet 2 received operational USDC and SUI through three transactions approximately four days prior to the exploit:

- **Inflow 3a, USDC from Actor Sui Wallet 1**
    - Timestamp: 2026-05-05 17:37:55.866 UTC
    - Transaction digest: B3Fxu7Ffh4YjHEGD8fXJY5ef8xZaj7LwEFrRM1XCktLx
    - From: 0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7
    - To: 0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8
    - Amount: 1,149.33 USDC

- **Inflow 3b, SUI from Actor Sui Wallet 1**
    - Timestamp: 2026-05-05 17:38:15.913 UTC
    - Transaction digest: DybBfPnd4ctrLPhJtrwhMfhytPsWnX5fz4YgAYH3Eipn
    - From: 0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7
    - To: 0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8
    - Amount: 111.0 SUI

- **Inflow 3c, SUI direct from CoinEx Omnibus Wallet (parallel path)**
    - Timestamp: 2026-05-05 20:58:11.567 UTC
    - Transaction digest: RZe7A3Z4hzMwFo2x3hdvCRUsPbaFdwUR7KGr53yKtuM
    - From: 0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb
    - To: 0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8
    - Amount: 513.51 SUI

Step 5: Trace Actor Sui Wallet 1 funding (back to May 5, 2026 afternoon)

Actor Sui Wallet 1 was funded directly by the CoinEx Omnibus Wallet (0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb) in two transactions on May 5:

- **Inflow 4a**
  - Timestamp: 2026-05-05 16:00:07.464 UTC
  - Transaction digest: ByH2gTNz7yAAJP2LsGPY5FPF7ob2mGSPwrgLSuteJcZN
  - From: 0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb
  - To: 0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7
  - Amount: 35.65 SUI
- **Inflow 4b**
  - Timestamp: 2026-05-05 17:10:06.125 UTC
  - Transaction digest: H96FPUb6pJ5r24Xf4yvM8Q15qQcGanjxdhk458JV2hx6
  - From: 0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb
  - To: 0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7
  - Amount: 1,300.54 SUI

Combined, the CoinEx Omnibus Wallet moved 1,336.19 SUI to Actor Sui Wallet 1 across these two transactions.

Destination of Funds

Following the exploit, the threat actor initiated a multi-chain migration to move the stolen assets from the Sui blockchain to Ethereum. The actor utilized the Sui-Ethereum Bridge, where each "burn", or destruction of SUI, on the Sui network produced a corresponding release of funds on the Ethereum mainnet. These assets were initially credited to Actor Ethereum Wallet 1 (0x4c9a14620ed8516238f0d6b9745d637d1609b1a1), where the bridged value was aggregated before being consolidated into a terminal repository, Actor Ethereum Wallet 2 (0xfff00112e3fdA3d5C1CCA51bB05Df11822AdD924). This final transfer was completed across six transactions on May 9, 2026, and the funds currently remain unspent at this destination as of May 12, 2026.

Forensic analysis of the operational funding for these Ethereum accounts reveals a sophisticated layering strategy designed to obfuscate the perpetrator's trail. Actor Ethereum Wallet 1 was provisioned with gas by an intermediary address (0xc4393C1B8463f18AE4E16ce39Bde1Ece55883E0E), which had received its funding from a Solana-based address (2Xp7cm3jimiLh5AKXLFCFxQUbGL49dd4KQaX3bhj3adR) via the Wormhole bridge.

Transaction Map

This section provides a detailed map of all value transfers associated with the exploit, as visualized in the MerkleScience forensic graph. The data below includes full sender/receiver addresses, transaction digests, asset types, amounts, and timestamps.

Actor Sui Infrastructure Setup (Sui Network)

Between May 5 and May 6, 2026, the threat actor established the necessary on-chain infrastructure, utilizing the CoinEx Omnibus wallet to provision multiple operational addresses.

Time UTC	From	To	Asset/Amount	Tx Digest
2026-05-05 16:00:07	0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb	0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7	35.65 SUI	ByH2gTNz7yAAJP2LsGPY5FPF7ob2mGSPwrgLSuteJcZN
2026-05-05 17:10:06	0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb	0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7	1,300.54 SUI	H96FPUb6pJ5r24Xf4yvM8Q15qQcGanjxdhk458JV2hx6
2026-05-05 17:37:55	0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	1,149.33 USDC	B3Fxu7Ffh4YjHEGD8fXJY5ef8xZaj7LwEFrRM1XCktLx
2026-05-05 17:38:15	0x44d5293f2b4c2eedf16a873aa2f6a016e44e4dade6db7c9ed926a8d3ad4e8da7	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	111.0 SUI	DybBfPnd4ctrLPhJtrwhMfhytPsWnX5fz4YgAYH3Eipn
2026-05-05 20:58:11	0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	513.51 SUI	RZe7A3Z4hzMwFo2x3hdvCRUsPbaFdwUR7KGr53yKtuM
2026-05-06 16:00:10	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	0xc880e710b4c0dc2634e8191c152d7fcd59588e09fe81c270b707b7b79d86fdea	697.67 SUI	3Ynfq2exREaQepb6WqvbpUGy2iw3uDVfTDor3oXR8DSq
2026-05-06 16:01:48	0xc880e710b4c0dc2634e8191c152d7fcd59588e09fe81c270b707b7b79d86fdea	0x04c4cc8077b6717b3fd0b40bcd254c958119ed02474ac59d2f9a6b331617f4cb	697.66 SUI	7GDAziYLXcVPaDDMFAd97tnkp8eqQFqCrrDwW2vtK9M6
2026-05-09 3:35:33	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	10.0 SUI	Caxc4sTyy32Va3qDzVspLoAnrEEjYoGmXtczUshyuSWy

Cross-Chain Migration (Sui-to-Ethereum Bridge)

Following the exploit on May 9, 2026, the actor bridged the stolen assets to Ethereum. Each Sui-side burn corresponds to an Ethereum-side release credited to Actor Ethereum Wallet 1 (0x4c9a14620ed8516238f0d6b9745d637d1609b1a1).

Time UTC	From	To	Asset/Amount	Tx Digest
May 09, 2026 03:23:28	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	0x000000000000000000000000000000000000000000000000000000000000000b	4.29884463 SUIETH	EbjfgpBkpNDSDzb7AiXnZ5s9PqyQ9jwK9h2qySFLwCsv
May 09, 2026 03:28:12	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	0x000000000000000000000000000000000000000000000000000000000000000b	6.4218155 SUIETH	8ouPrBgNzfQhJWXUo6ykwZGTtqXTTBhGPpidJd5w1pNd
May 09, 2026 03:29:38	0xee7c1a66286ac5c194072801935ffcc3e10c3f514b298549a4d06b6a3d82e7f8	0x000000000000000000000000000000000000000000000000000000000000000b	8.25744951 SUIETH	DyVskHtDgJUMpoF3dVsjp17agAQz1XpAcmguyozgP8m6
May 09, 2026 03:41:25	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	8.55856455 SUIETH	9WdiErRjfBFWSvWoXSJk7X5zcXDvBMbyykh6FhXTWhkC
May 09, 2026 03:46:26	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	10.68941167 SUIETH	FPp56oz4Y8zcCxpnk4Po7e4vdEZijhSPo816Gr1xVNhN
May 09, 2026 03:42:40	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	10.29285866 SUIETH	BV9bzhULvsGdRyjfWQKwkXQRxWWMJzsp5FHYiVDdYhuN

May 09, 2026 03:47:34	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	11.95547806 SUIETH	5AiaRT4kGFHwhvfGWTYe3TyLD88wmwqtuewBgRNRExHG
May 09, 2026 03:49:30	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	10 SUIETH	DHoMnPocm8rxrgs5UqF71PVTeHb4gShsDgdRdf2No7Mg
May 09, 2026 03:52:16	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	0.32393617 SUIWBTC	diBt8Z94KgRgHGhW6KgyaZV3ereJLb8CoFjmqyYdfwm
May 09, 2026 03:55:54	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	7.91424524 SUIETH	3BbCmHCvpfutjtWMo1N3cpyjdAMiTXZn39wJH4RcpTq6
May 09, 2026 04:25:11	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	0.32498789 SUIWBTC	JCGciueh9Lsn1fDpsUm71JudguwPErn8Hb6RbVUbiWCj
May 09, 2026 05:12:43	0x73904852f5edc15bbbbe641fd436301cae02c6e229e9d781ada2a6d3788e7e49	0x000000000000000000000000000000000000000000000000000000000000000b	0.05929862 SUIWBTC	BdaNun7SKajFA19fWUNYWxVCJBpyqNWoKiG2U73B6zWE

Bridge-in transactions

Time UTC	From	To	Asset/Amount	Ethereum Tx Hash
2026-05-09 3:26:11	0xc4393C1B8463f18AE4E16ce39Bde1Ece55883E0E	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0.01 ETH (gas)	0xe087ac5ec6ff7bc10dd829bcbbc4bce9507938d8bc0c40c258064b0657c2532b

2026-05-09 3:26:59	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	4.2988 ETH	0xbeea858e5edfc0b15bcf54b99e76b5c60b75e2f97548f0bb7fb379d0183a4114
2026-05-09 3:28:47	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	6.4218 ETH	0x4e046a8384c01d14b90f97c8fedb51c03eeb19c9adff7e952cef97f490efab8e
2026-05-09 3:29:59	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	8.2574 ETH	0xaed4808d8082aec575d60c9cb05d807b9bf910f828b0fbff888f7ee1cf12ab75
2026-05-09 3:41:47	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	8.5586 ETH	0x464998708e7947caeddc664446883b77e34152b914bdaae8d82a8f9de2d94fee
2026-05-09 3:42:59	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	10.2929 ETH	0xda99d6b1952bfc4a5509c1cd4a3e9d2035b1f5870ee7f70f932af517ccd9fd73
2026-05-09 3:46:47	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	10.6894 ETH	0xbf7313d55e63a265d291fb52412cdc5bad60c024a3e4666a1402df22846925b9
2026-05-09 3:47:59	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	11.9555 ETH	0x7480dea566727365daec36b1e3604e21e5474b8796a8f703f69badee9ea4bf2d
2026-05-09 3:52:11	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	10.0 ETH	0x4dabfe912cb2c952a9a93ebe3579cbf2b5640b51c89a4a0e64202366f10f2cc2
2026-05-09 3:52:59	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0.3239 WBTC	0x20ed996e6ef18676bd625b8f870c2e8da7188f50f607769b272b82cdcf50f498

2026-05-09 3:56:23	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	7.9142 ETH	0x9636c21d7df08f49af8ade6dc7f39de50018db18af4457c6ef64bd4a352431e9
2026-05-09 4:25:35	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0.325 WBTC	0xb4ba865cdca94ecc88e0a7bd5064964b4974c7df7c4c31661fd73f2986dec526
2026-05-09 5:12:59	0x312e67b47A2A29AE200184949093D92369F80B53	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0.0593 WBTC	0x35025ae45082eed0a96c98b1701550d97612e5f5e3208729ea9b8a5d75284121

Bridge-out transactions

Bridged Funds Consolidation (Ethereum)

On May 9, 2026, the bridged value was aggregated at Actor Ethereum Wallet 1 (0x4c9a14620ed8516238f0d6b9745d637d1609b1a1) and then forwarded to the final resting wallet, Actor Ethereum Wallet 2 (0xfff00112e3fdA3d5C1CCA51bB05Df11822AdD924) in six separate transactions.

Time UTC	From	To	Asset/Amount	Ethereum Tx Hash
2026-05-09 5:03:11	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0xFFF00112e3fdA3d5C1CCA51bB05Df11822AdD924	1.0 ETH	0x6ec8ef8bccf6fbd59130bca38f45bf3f07eb328e4c6cd7f84453c40e67f8bd7e
2026-05-09 5:07:11	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0xFFF00112e3fdA3d5C1CCA51bB05Df11822AdD924	5,000 DAI	0xfdc204bebffef0233157162ccb483895d94a0b5efcf4d0fc2dbe992c4301157b
2026-05-09 5:08:47	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0xFFF00112e3fdA3d5C1CCA51bB05Df11822AdD924	0.64892 WBTC	0xafde0e5146f986197c9760ee6a94429a65acfb068b7289e687ca82b771c95682
2026-05-09 5:11:11	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0xFFF00112e3fdA3d5C1CCA51bB05Df11822AdD924	160,296.57 DAI	0x0afc5c0dc9ed0c5acfa85cd7fb76fae92a9e3d45ff023b7f9c00c5978a3616b5

2026-05-09 5:11:47	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0xFFF00112e3fdA3d5C1CCA51bB05Df11822AdD924	5.7 ETH	0x9742ded2d8595ee610313d664ec76df724db6bac8e4a43057b533e0a2c80e214
2026-05-09 5:13:35	0x4C9A14620eD8516238f0d6b9745d637d1609B1A1	0xFFF00112e3fdA3d5C1CCA51bB05Df11822AdD924	0.05929 WBTC	0xd45ab19523539940a245139a811a5ee22b7ee010a950c6ed26836b8357417938

The total value consolidated at the resting wallet (0xFFF00112e3fdA3d5C1CCA51bB05Df11822AdD924) consists of approximately 6.7 ETH, 0.708 WBTC, and 165,296.57 DAI. On-chain data confirms that these funds remain dormant in Actor Ethereum Wallet 2 as of May 12, 2026.

Appendix A: Exploit Technical Deep Dive

How DeepBook Margin Works

DeepBook Margin is a secondary layer built upon the DeepBook Core, designed to facilitate borrow-funded leverage. The protocol's architecture relies on two distinct components to manage credit and risk:

1. The Margin Pool functions as a single-asset lending market (e.g., USDC or SUI). Liquidity providers supply assets to the pool in exchange for supplier shares, which represent a pro-rata claim on the underlying capital. These shares accrue yield as the pool’s exchange rate appreciates via interest paid by borrowers. The protocol monitors the pool's total supply, aggregate debt, vault balance, and utilization rate, maintaining a configurable borrowing cap to ensure liquidity.

2. The Margin Manager serves as a segregated borrower account for each user. It houses both the user’s posted collateral and any liabilities drawn from the margin pools. All trading activity on DeepBook is executed through this entity. To maintain solvency, the Margin Manager must sustain a risk ratio, the value of assets relative to debt, above a predefined liquidation threshold. If the ratio falls below this floor, the account becomes eligible for liquidation.

   The relationship between these two entities is strictly creditor-debtor: the margin pool acts as the lender, while the margin manager acts as the borrower. Consequently, if a margin manager is drained or compromised, it generates "bad debt" within the

corresponding margin pool. In such an event, the outstanding supplier shares represent a total claim that exceeds the pool's actual underlying assets, resulting in a capital deficit.

Technical Exploit Mechanism

The technical vulnerability stemmed from the inconsistent application of two safety invariants that should ideally govern every balance-changing operation: per-order price validity and post-state account solvency. While both invariants were correctly enforced on the borrow path, the trade path only enforced price validity.

Borrow Path:
When a user borrows from a pool, the assets are deposited into the margin manager and the system immediately verifies the manager's risk ratio. A borrow transaction only executes successfully if the manager remains solvent in the post-borrow state.

Trade Path:
When a margin manager placed an order, the system verified that the order price fell within a 5% tolerance band of the oracle price. However, following the fill, after balances had shifted, the system failed to recompute the manager's risk ratio. Consequently, while per-fill price validity was strictly enforced, post-fill account health was not.

These two invariants are orthogonal. The 5% guard is a defense against oracle manipulation for a single fill; it does not account for cumulative equity loss across multiple trades, nor does it protect against an adversarial counterparty filling at a price that is technically valid but economically unfavorable to the margin manager.

Exploit Mechanism:
The attacker controlled both sides of the order book. The first account, a margin manager (Account A), held borrowed USDC. A second, non-margin balance manager (Account B), also controlled by the attacker, acted as the counterparty. Account A placed orders within the 5% band that were intentionally unfavorable to itself; Account B filled these orders. Each trade successfully transferred value from Account A to Account B at oracle-valid prices. Account A's borrowed assets were systematically bled into Account B, causing Account A's risk ratio to degrade below the liquidation threshold without detection. This process, repeated across five Programmable Transaction Blocks (PTBs), left the affected margin managers insolvent and created bad debt within the USDC margin pool.

The conceptual error was treating per-order price validity as a sufficient proxy for post-trade account health. The necessary invariant, that every path materially changing a margin manager's balance must enforce post-change solvency, was present in the borrow path but absent in the trade path.

The DeepBook protocol was paused at 06:40 UTC, approximately 3 hours and 22 minutes after the initial exploit transaction. Total exposure across all five attack transactions was approximately 65 minutes (from 03:18:15 UTC to 04:23:03 UTC).

Analysis of Financial Discrepancy and Protocol Loss:
The total financial impact on the protocol exceeded the net value successfully extracted by the attacker. While the perpetrator's external balance changes totaled approximately $242,222 USD, the aggregate "bad debt" generated within the protocol, and subsequently indemnified by the Sui Foundation, was 283,604 USDC.

This discrepancy of $41,382 represents the difference between the attacker's realized profit and the protocol's total loss, which was compounded by several factors:

- Unpaid Borrowing Interest: During the 65-minute attack and the subsequent three-hour exposure window before the protocol was paused, the $1.1 million in borrowed USDC continued to accrue interest. This increased the total liability of the insolvent Margin Managers.

- Liquidation Penalties: The protocol enforces a 5% liquidation penalty (comprising a 2% liquidator reward and a 3% pool reward). When the attacker's trades pushed the Margin Managers below a 1.0 risk ratio, these protocol-level penalties were automatically applied to the accounts' remaining balances.

The Sui Foundation's capital injection was calculated to cover the entirety of this bad debt. This ensured that the Margin Pool was restored to a 1:1 asset-to-share ratio, completely insulating liquidity providers from the costs of the interest deficit and protocol penalties.