Eric Rosen
Amos Friedland
Jordana Haviv
Constantine Economides
Kelvin Goode
Maya S. Jumper
FREEDMAN NORMAND FRIEDLAND LLP
99 Park Avenue, 19th Floor
New York, NY 10016
Tel.: (646) 350-0527
erosen@fnf.law
afriedland@fnf.law
jhaviv@fnf.law
ceconomides@fnf.law
kgoode@fnf.law
mjumper@fnf.law

Counsel for Claimants

THE AMERICAN ARBITRATION ASSOCIATION

COINBASE WALLET VICTIMS,

Claimants,

v.

TOSHI HOLDINGS PTE. LTD D/B/A COINBASE WALLET, COINBASE, INC., AND COINBASE GLOBAL, INC.

Respondents.

FIRST SUPPLEMENT TO THE CONSOLIDATED DEMAND FOR ARBITRATION

Case No. 01-22-0004-3719

This Supplement to the Consolidated Demand for Arbitration ("Consolidated Demand") fully incorporates by reference all allegations, facts, and claims asserted in the Consolidated Demand, filed on October 14, 2022 in this matter. This Supplement is intended to add additional Coinbase Wallet Victims as Claimants to the pending matter.

I. PARTIES

A. Claimants

1. Claimant Ignacio Garcia is a resident of California. Between March 2022 and April 2022 Mr. Garcia's crypto, valued at approximately $25,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Mr. Garcia's factual allegations is included below in Section II.A.

2. Claimant Joshua Hawkins is a resident of Texas. In or around November and December 2021, Mr. Hawkins's crypto, valued at approximately $86,970 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Mr. Hawkins's factual allegations is included below in Section II.A.

3. Claimant Dexter Casta is a resident of Minnesota. In or around May 2022, Mr. Casta's crypto, valued at approximately $678,476 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Casta's factual allegations is included below in Section II.A.

4. Claimant Chad Holmes is a resident of Utah. In or around June 2022, Mr. Holmes's crypto, valued at approximately $70,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Holmes's factual allegations is included below in Section II.A.

5. Claimant Nader Lobandi is a resident of Massachusetts. In or around April 2022, Mr. Lobandi's crypto, valued at approximately $92,640 USDT, was stolen from his Coinbase

Wallet in transactions that he did not authorize. A detailed description of Lobandi's factual allegations is included below in Section II.A.

6. Claimant John Doe 5 is a resident of Florida. In or around March 2022, John Doe 5's crypto, valued at approximately $3,718,480.68 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of John Doe 5's factual allegations is included below in Section II.A.

7. Claimant Craig Haskins is a resident of New Jersey. In or around June 30, 2022, Mr. Haskin's crypto, valued at approximately $209,588 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Haskin's factual allegations is included below in Section II.A.

8. Claimant Peter Tam is a resident of California. Between January and March 2022, Mr. Tam's crypto, valued at approximately $1,102,337 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Tam's factual allegations is included below in Section II.A.

9. Claimant James Burke is a resident of Massachusetts. In or around July 2022, Mr. Burke's crypto, valued at approximately $95,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Burke's factual allegations is included below in Section II.A.

10. Claimant Brian Rothaus is a resident of Pennsylvania. In or around September 2022, Mr. Rothaus's crypto, valued at approximately $247,456 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Rothaus's factual allegations is included below in Section II.A.

11. Claimant John Young is a resident of Georgia. In or around August 2022, Mr. Young's crypto, valued at approximately $277,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Young's factual allegations is included below in Section II.A.

II. FACTUAL ALLEGATIONS

A. Individual Claimant Narratives - Unauthorized Thefts from Claimants' Accounts and Coinbase's Deficient Responses to Reported Theft

12. A detailed account of each Claimant's respective experience as a victim of the Coinbase Wallet liquidity mining pool scams, including their individual monetary losses and other related harm suffered from the unauthorized transactions and thefts, is included below.[1]

a. Ignacio Garcia

13. On or around March 2, 2022, Claimant Ignacio Garcia ("Garcia") was contacted by an individual through Facebook. After befriending Garcia, the individual encouraged Garcia to join a liquidity mining pool through which Garcia could earn significant income. Having lulled Garcia into the prospect of significant returns on investment, the individual directed Garcia to deposit USDT into his Coinbase Wallet and open a link to a dapp called ETH-COIN ("eth-coin.cc") through his Coinbase Wallet browser. On or about March 5, 2022, Garcia followed these instructions and joined the mining pool through the dapp.

14. During the process of joining the pool, Garcia received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

15. To fund the pool, Garcia deposited a total of 25,000 USDT into his Coinbase Wallet between March and April of 2022.

[1] The Individual Claimant Narratives included herein are abbreviated factual recitations. These narratives incorporate by reference and necessarily include the allegations contained in the Consolidated Demand, filed on October 14, 2022.

16. Between March 20 and April 14, 2022, scammers, through unauthorized transactions, stole all of the USDT in Garcia's Coinbase Wallet, totaling $25,000. These withdrawals were done without Garcia's permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

17. Immediately after realizing that his assets had been stolen through the fraudulent dapp, Garcia contacted Coinbase's customer support to report the theft (Case No. #10890741). In response, Coinbase accused Garcia of disclosing his security seed phrase to the scammers, denied liability or fault, and informed Garcia that "Coinbase Wallet is a user-controlled and non-custodial product" and since Coinbase does not have access to customers' seed phrases, Coinbase "cannot help recover any Coinbase Wallet or transfer funds on [his] behalf." Coinbase then instructed Garcia to file a complaint with the FBI. Garcia informed Coinbase that he already filed a complaint with the FBI and needed assistance from Coinbase to investigate the unauthorized transactions. On information and belief, following Mr. Garcia's complaint, Coinbase has now flagged and restricted access to the fraudulent ETH-COIN dapp on its platform.

18. As a result of the Coinbase Wallet scams, Garcia has lost his life savings, which has caused major hardship for him and his family. These financial losses have resulted in significant emotional and mental distress.

b. Joshua Hawkins

19. On or around August 17, 2021, a woman contacted Claimant Joshua Hawkins ("Hawkins") through Facebook. After befriending Hawkins, the woman encouraged Hawkins to join a liquidity mining pool and to deposit his entire life savings to his Coinbase Wallet. Under the guidance of this woman, Hawkins deposited USDT to his Coinbase Wallet and opened a link to the dapp COINBASE U2e (https://www.coinbaseu2e.com/?d=TSASHA) through his Coinbase Wallet browser.

20. During the process of joining the pool, Hawkins received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

21. To fund the pool, Hawkins deposited a total of 86,970 USDT into his Coinbase Wallet.

22. In or around November 2021, scammers, through unauthorized transactions, stole all of the USDT in Hawkins's Coinbase Wallet, amounting to approximately $86,970. These withdrawals were done without Hawkins's permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

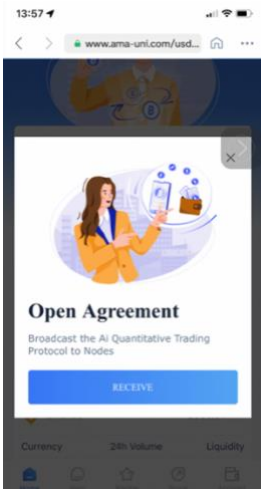
23. Hawkins contacted Coinbase's customer support after realizing his Coinbase Wallet was drained (Case No. #13621439). In response, Coinbase informed Hawkins that it would "take longer to respond" to his reported theft given the high number of request it was receiving and dissuaded him from submitting additional inquires. At no point did Coinbase provide Hawkins with a substantive response to his inquiry or offer guidance on how to recover his assets.

24. Hawkins has lost his entire life savings, has gone into substantial debt from loans undertaken due to the trust he placed in Coinbase Wallet, and has suffered significant mental anguish and suicidal ideations as a result of the financial impact of the unauthorized transactions.

c. Dexter Casta

25. On or around May 3, 2022, Claimant Dexter Casta ("Casta") was contacted by a woman named Lisa through a social dating app. After befriending Casta, Lisa encouraged Casta to join a liquidity mining pool from which she insisted Casta would be able to earn significant income. Lisa directed Casta to deposit USDT into his Coinbase Wallet.

26. Lisa then directed Casta to open the link for AMMUNI (https://www.ama-uni.com/usdc?d=TEASHW) through his Coinbase Wallet browser. Casta was instructed to purchase a "node," which unbeknownst to him, provided scammers unfettered access to his Coinbase Wallet.



27. During the process of joining the pool, Casta received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

28. To fund the pool, Casta made 15 deposits of USDT, totaling 678,476 USDT, into his Coinbase Wallet.

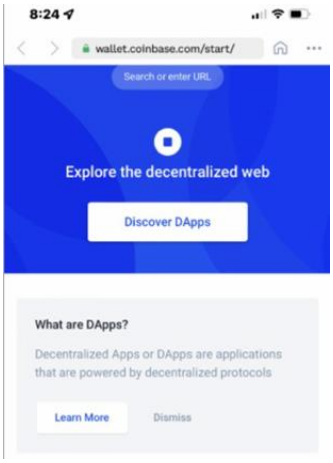
29. Between May 2022 and June 2022, scammers, through unauthorized transactions, stole all of the USDT in Casta's Coinbase Wallet, amounting to approximately $678,476. These withdrawals were done without Casta's permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

30. Casta immediately contacted Coinbase's customer support several times after realizing his Coinbase Wallet was drained (Case No. #12338467). Coinbase's initial generic response was entirely unhelpful and not tailored to the fraudulent scam Casta had reported. In a subsequent response, Coinbase advised Casta to "cease engagement" with the fraudulent dapp and to contact law enforcement. Coinbase denied any liability or fault and informed Casta there was no way to recover his funds.

31. As a result of the fraud scam facilitated through Coinbase's platform, Casta lost his life savings, and has incurred substantial debt from loans taken during the process. He also experienced significant anxiety and emotion distress due to the financial loss.

d. Craig Haskins

32. On or around May 9, 2022, Claimant Craig Haskins ("Haskins") was contacted by an individual named Nari on Twitter who introduced him to a liquidity mining pool through dapps on Coinbase.



33. After befriending Haskins, Nari told him he would be able to earn significant income though a dapp on Coinbase Wallet's platform called DEX-CEX.

34. On or around May 10, 2022, Haskins deposited USDT into his Coinbase Wallet, and as directed, open the link for DEX-CEX dapp through his Coinbase Wallet browser to join the mining pool.

35. During the process of joining the pool, Haskins received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

36. To fund the pool, Haskin deposited a total of 209,588 USDT into his Coinbase Wallet.

37. On or around June 30, 2022, scammers, through an unauthorized transaction, stole all of the USDT in Haskin's Coinbase Wallet, totaling $209,588. This withdrawal was done without his permission or consent and without any notification, warning, or substantive response from Coinbase.

38. Upon realizing that his assets had been stolen through the dapp, Haskins contacted Coinbase's customer support to report the theft and flag the fraudulent dapp (Case No. #12370493). In response, Coinbase denied liability or fault and, without providing any assistance to Haskins to recover his funds, closed his complaint file.

39. Haskins has lost a substantial portion of his life savings and suffered significant mental and emotion distress as result of the unauthorized transaction.

e. Chad Holmes

40. On or around June 3, 2022, Claimant Chad Holmes ("Holmes") was introduced to a liquidity mining pool by two individuals named Moe and Katherine who held themselves out to be Fidelity and Coinhub representatives who worked in collaboration with Coinbase. The individuals informed Holmes that "Coinbase was one of the largest safest cryptocurrency platforms in the world" and directed Holmes to download Coinbase Wallet and deposit USDT into his Wallet.

41. Holmes was then instructed to open the link provided by the individuals for a dapp called app.fidelityquantitative.fun.com through his Coinbase Wallet browser in order to join the mining pool. On or around June 6, 2022, Holmes followed these instructions, joined the pool, and began depositing USDT into his Wallet to fund the pool.

42. During the process of joining the pool, Holmes received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

43. To fund the pool, Holmes deposited a total of 70,000 USDT into his Coinbase Wallet.

44. On or around June 8, 2022, scammers, through an unauthorized transaction, stole all of the USDT in Holmes's Coinbase Wallet, totaling approximately $70,000. This withdrawal was done without his permission or consent and without any notification, warning, or substantive response from Coinbase.

45. Holmes promptly contacted Coinbase's customer support on multiple occasions after realizing his Coinbase Wallet had been drained to report the theft and the fraudulent dapp (Case Nos. # 12846016, 12805010, 12596991, 12395573). In response, Coinbase requested additional information regarding the fraudulent transaction, including the transaction hash of the unauthorized transactions. After Holmes provided the requested information, Coinbase still failed to provide any meaningful assistance to Holmes and locked his account without further notice.

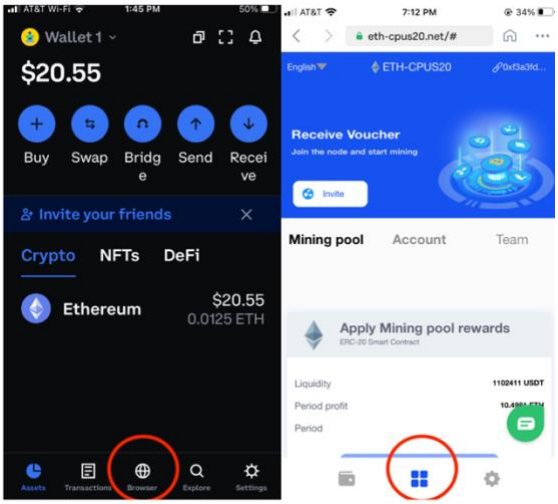
46. Holmes has been financially devasted by the loss of his assets. He has suffered significant mental and emotional distress as a result of the scammers' unauthorized use of his Wallet.

f. Peter Tam

47. On or around January 2022, a person going by the name of Sugar Chan, contacted Claimant Peter Tam ("Tam") through a social media app called LINE. After befriending Tam, the individual encouraged Tam to join a liquidity mining pool under the prospect of earning significant income. Tam was then directed to deposit USDT into his Coinbase Wallet and open the link for a dapp called ETH-CPUS (eth-cpus20.net/#) through his Coinbase Wallet browser. Tam then clicked a button to join the mining pool, which unknowingly gave scammers access to his Coinbase Wallet without his security passphrase.

48. During the process of joining the pool, Tam received no warnings stating that he was engaging with a third-party entity outside independent of Coinbase and giving any third parties access to withdraw crypto from his Coinbase Wallet. Further, the "four square" symbol in the

Wallet application made it appear that the dapps were internal applications within Coinbase Wallet (see image on right).



49. There was no warning that the users were leaving the Wallet protocols. Several months after the fraudulent withdrawal, Coinbase changed its dapp symbol from the Coinbase "four square" symbol to a globe to inform users that they were leaving the Coinbase application (see image on left).

50. To fund the pool, Tam made four deposits of USDT into his Coinbase Wallet between January and March of 2022.

51. In or around March 2022, the scammers, through unauthorized transactions, stole all of the USDT in Tam's Coinbase Wallet, amounting to approximately $1,102,337.42. These withdrawals were done without his permission or consent and without any notification, warning, or substantive response from Coinbase.

52. Tam promptly contacted Coinbase's customer support on March 13, 2022 after realizing that his Coinbase Wallet had been drained (Case No. #11448982). In response, Coinbase informed him that they did not "handle queries or complaints regarding the Wallet" and denied liability or fault for the unauthorized transactions. Tam continued to reach out to Coinbase customer support, providing pictures and details of the fraudulent withdrawals. On March 17, Coinbase finally responded and acknowledged that Tam had fallen victim to a scam. Tam filed a

formal complaint with Coinbase on April 20, 2022. After reviewing his complaint, Coinbase maintained its position that it would not reimburse Tam for his "alleged losses."

53. As a result of this scam facilitated on Coinbase's platform, Tam has suffered a devastating financial loss, and significant mental and emotional harm.

g. Nader Lobandi (User 1)

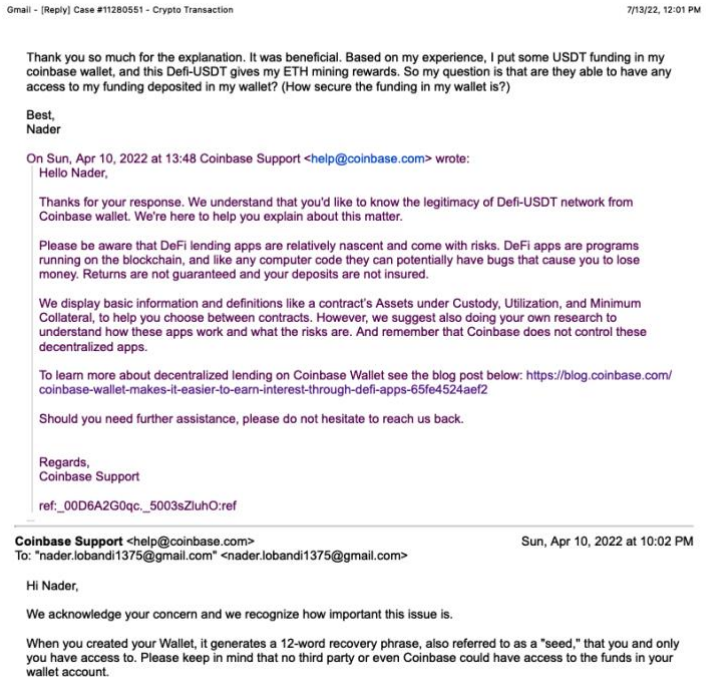
54. On or around March of 2022, a person going by the name of Aimee contacted Claimant Nader Lobandi ("Lobandi") through social media. Lobandi is referred to as User 1 in the October 14, 2022 Consolidated Demand (the allegations are incorporated herein). After befriending Lobandi, Aimee encouraged him to join a liquidity mining pool from which she insisted he would be able to earn significant income. She directed Lobandi to deposit USDT into his Coinbase Wallet to contribute to the pool. Aimee then directed Lobandi to open the link she provided him for a dapp called DEFI-ETH-USDT (defi-eth-usdt.com/home) through his Coinbase Wallet browser. Aimee directed him to click a button to "join the node" and start participating in the mining pool. Unbeknownst to Lobandi, this action allowed scammers to access and initiate transfers from his Wallet without his consent or authorization.

55. During the process of joining the pool, Lobandi received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet. Lobandi never gave anyone access to his security passphrase.

56. After joining the pool, Lobandi made approximately 5 deposits of USDT into his Coinbase Wallet. Lobandi withdrew all the funds out of his Coinbase wallet on or around April 10th, being suspicious of the legitimacy of the dapp and the security of the funds within his Coinbase Wallet.

57. On or around April 10, 2022, Lobandi contacted Coinbase customer support to inquire about the legitimacy of the DEFI-ETH-USDT dapp, specifically asking whether the dapp is "able to have any access to my funding deposited in my wallet." In response, Coinbase customer support informed Lobandi that "no third party or even Coinbase could have access to the funds in

your wallet account." With this misinformation, Lobandi transferred all the funds back into his Coinbase wallet in two deposits of USDT.



Gmail - [Reply] Case #11280551 - Crypto Transaction 7/13/22, 12:01 PM

Thank you so much for the explanation. It was beneficial. Based on my experience, I put some USDT funding in my coinbase wallet, and this Defi-USDT gives my ETH mining rewards. So my question is that are they able to have any access to my funding deposited in my wallet? (How secure the funding in my wallet is?)

Best,
Nader

On Sun, Apr 10, 2022 at 13:48 Coinbase Support <help@coinbase.com> wrote:

Hello Nader,

Thanks for your response. We understand that you'd like to know the legitimacy of Defi-USDT network from Coinbase wallet. We're here to help you explain about this matter.

Please be aware that DeFi lending apps are relatively nascent and come with risks. DeFi apps are programs running on the blockchain, and like any computer code they can potentially have bugs that cause you to lose money. Returns are not guaranteed and your deposits are not insured.

We display basic information and definitions like a contract's Assets under Custody, Utilization, and Minimum Collateral, to help you choose between contracts. However, we suggest also doing your own research to understand how these apps work and what the risks are. And remember that Coinbase does not control these decentralized apps.

To learn more about decentralized lending on Coinbase Wallet see the blog post below: https://blog.coinbase.com/coinbase-wallet-makes-it-easier-to-earn-interest-through-defi-apps-65fe4524aef2

Should you need further assistance, please do not hesitate to reach us back.

Regards,
Coinbase Support

ref:_00D6A2G0qc._5003sZluhO:ref

Coinbase Support <help@coinbase.com> Sun, Apr 10, 2022 at 10:02 PM
To: "nader.lobandi1375@gmail.com" <nader.lobandi1375@gmail.com>

Hi Nader,

We acknowledge your concern and we recognize how important this issue is.

When you created your Wallet, it generates a 12-word recovery phrase, also referred to as a "seed," that you and only you have access to. Please keep in mind that no third party or even Coinbase could have access to the funds in your wallet account.

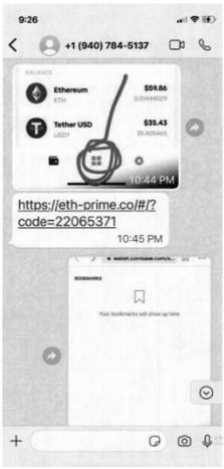
58. Despite Coinbase's assurances, on or around April 12, 2022, scammers, through unauthorized transactions, stole all of the USDT from Lobandi's Coinbase Wallet, amounting to approximately $92,640 USDT. These withdrawals were done without Lobandi's permission or consent. They were also done without any notification, or warning from Coinbase.

59. After the fraudulent withdrawal, Lobandi contacted Coinbase's customer support to report that his Coinbase Wallet was drained (Case No. #11280551). Coinbase denied liability or fault and informed him that "there is no way to recover [his] funds."

60. Lobandi lost a significant portion of his life savings, and suffered emotional and mental distress as a result of the loss caused by these unauthorized transactions. Due to the mental distress Lobandi experienced soon after the incident, he was hospitalized for two weeks for severe anxiety and depression. His studies as a PhD student have suffered and he continues to take antidepressant medications as a treatment of the traumatic experience.

h. John Doe 5

61. On or around November 11, 2021, Claimant John Doe 5 met a woman through a social media website. After befriending John Doe 5, the woman encouraged John Doe 5 to join a liquidity mining pool through a dapp called ETH-PRIME from which she insisted John Doe 5 would be able to earn significant income. She directed John Doe 5 to deposit USDT into his Coinbase Wallet and open the link she provided for ETH-PRIME (https://eth-prime.co/#/?) through his Coinbase Wallet browser.



62. John Doe 5 followed these instructions and joined the dapp to begin participating in the mining pool. The woman even offered to provide John Doe 5 with funds to purchase the mining certificate to join the pool.

63. At all times, John Doe 5 believed that his assets were securely stored in his Coinbase Wallet, and inaccessible to third parties without his unique seed passphrase. Unbeknownst to John Doe 5, the purchase of the mining certificate provided scammers access to withdraw John Doe 5's assets without his authorization or consent.

64. During the process of joining the pool, John Doe 5 received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

65. Between December 2021 and March 2022, John Doe 5 made 18 deposits of USDT, totaling approximately 3,718,480 USDT, into his Coinbase Wallet to fund the pool.

66. In or around January of 2022, John Doe 5 received a message from the dapp customer representative indicating that his account was "restricted" and he would need to contribute more USDT to his Wallet to meet the contribution threshold. Believing that he had been communicating with a Coinbase affiliate and that Coinbase, rather than the fraudulent dapp, had restricted his account, John Doe 5 attempted to contact Coinbase customer support over a dozen times by phone and email to inquire about the account "restriction" and other activity concerning his Coinbase Wallet.

67. In response, Coinbase customer service representatives sent John Doe 5 through numerous account verification hurdles and repeatedly assured him that Coinbase was investigating his case. Even after being alerted to the fraudulent activity on his account, Coinbase failed to inform John Doe 5 that he was not communicating with a Coinbase representative, and failed to implement any security measures to protect his assets or flag unusual activity on the account. During the pendency of Coinbase's investigation, scammers continued to access John Doe 5's Wallet without his authorization.

68. Between December 2021 to March 2022, scammers, through unauthorized transactions, stole all of the USDT in John Doe 5's Coinbase Wallet, amounting to approximately $3,718,480. These withdrawals were done without John Doe 5's permission or consent. They were also done without any notification, warning, or substantive response from Coinbase. John Doe 5 did not receive a response to his inquiries from Coinbase until late March 2022, weeks after his Wallet had already been drained by scammers through the fraudulent dapp.

69. John Doe 5 contacted Coinbase's customer support again after learning that his Coinbase Wallet was drained (Consolidated Case No. #09807487). Coinbase denied liability or responsibility for the fraudulent activity and directed John Doe 5 to contact law enforcement to report the unauthorized transactions.

70. The financial loss caused by the Coinbase scam has been devastating for John Doe 5. John Doe 5, age 83, depleted his savings in the process and took out multiple loans to fund his Wallet in response to demands for additional deposits that he believed were required by Coinbase. As a result of his grave financial loss, he has suffered significant mental and emotional distress and anxiety concerning potential tax liability.

i. James Burke

71. On or around May 25, 2022, a person going by the name of Lena, contacted Claimant James Burke ("Burke") through a social dating website. After befriending Burke, Lena encouraged him to join a liquidity mining pool from which she insisted he would be able to earn significant income. Lena directed Burke to deposit USDT into his Coinbase Wallet and open the link she provided to a dapp called https://rep-eth.com/erc/#/?code=E10004. On or around June 10, 2022, Burke did as he was instructed and clicked a button in his Coinbase Wallet browser to join the mining pool.

72. During the process of joining the pool, Burke received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

73. To fund the pool, Burke deposited a total of 95,000 USDT into his Coinbase Wallet.

74. Between June and July 25, 2022, the scammers, through unauthorized transactions, stole all of the USDT in Burke's Coinbase Wallet, amounting to approximately $95,000. These withdrawals were done without Burke's permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

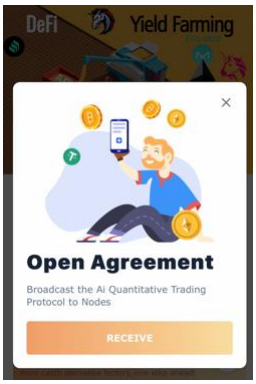
75. Burke contacted Coinbase's customer support after realizing his Coinbase Wallet had been accessed and drained without his authorization (Case No. #12462628). In response, Coinbase denied liability or fault and informed they his "seed phrase [was] [] compromised" and "Coinbase cannot recover the funds."

76. Burke has lost his life savings and suffered significant emotional and mental distress as a result of the unauthorized transactions.

j. Brian Rothaus

77. On or around April 11, 2022, a woman contacted Claimant Brian Rothaus ("Rothaus") through Facebook under the guise of seeking golf advice from Rothaus – an avid golfer. After chatting with Rothaus, the woman told him about her investments in cryptocurrency and asked Rothaus to participate in a liquidity mining pool. The woman directed Rothaus to create a Coinbase Wallet account and deposit USDT into his Coinbase Wallet. The woman told Rothaus that he could easily transfer the funds from his Wallet back to his personal account.

78. The woman then directed Rothaus to open the link for a dapp called Farmyieldpro (https://yield-farming.pro) through his Coinbase Wallet browser. Rothaus was immediately suspicious of the third-party interface and contacted Coinbase to inquire about the legitimacy of the dapp browser. Coinbase informed Rothaus that there was no way for anyone to access his Wallet assets without his security passphrase.



79. Rothaus made one deposit of 247,456.34 USDT into his Coinbase Wallet on or around October 26, 2022. On or around October 27, 2022, after numerous attempts to exit out of the dapp to return to the Coinbase home page interface on the Coinbase Wallet app, Rothaus clicked a button to "receive" a node on the dapp, which unknowingly entered him into a malicious smart contract.

80. Later that same day, scammers stole all of the USDT in Rothaus's Coinbase Wallet, totaling approximately $247,456. This withdrawal was done without his permission or consent and without any notification, warning, or substantive response from Coinbase.

81. Rothaus never disclosed his seed phrase to anyone and received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

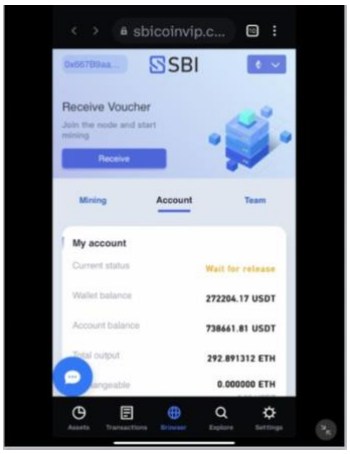
82. Rothaus contacted Coinbase's customer support several times by phone and email after realizing his Coinbase Wallet had been drained (Case Nos. #339704436, #13533814). In response, Coinbase restricted his Wallet account and sent Rothaus a list of follow-up questions, many of which he had already answered. Coinbase never provided Rothaus with any guidance on how to recover his assets. To date, the dapp is still accessible on Coinbase Wallet's platform.

83. Rothaus has lost his IRA savings as a result of this scam and suffered substantial emotional and mental distress due to the financial loss.

k. John Young

84. On or around June 7, 2022, a person going by the name of Emily Smith contacted Claimant John Young ("Young") through Tinder. After befriending Young, Emily encouraged Young to join a liquidity mining pool from which she insisted he would be able to earn significant

income. Emily provided Young with step-by-step instructions and directed Young to download the Coinbase Wallet app and deposit USDT into his Coinbase Wallet. Once on the Coinbase Wallet app, Emily directed Young to open a link to a dapp called SBI COIN VIP (sbicoinvip.com) through his Coinbase Wallet browser in order to join the mining pool. On or around June 21, 2022, Young followed Emily's instructions and clicked a button to participate in the pool, which unknowingly entered him into a malicious smart contract.



85. During the process of joining the pool, Young received no warnings stating that he was exiting Coinbase's internal platform, or was giving any third parties access to withdraw crypto from his Coinbase Wallet by using the external dapp.

86. To fund the pool, Young made six deposits of USDT into his Coinbase Wallet between June and August 2022.

87. On or around September 21, 2022, scammers, through an unauthorized transaction, stole all of the USDT in Young's Coinbase Wallet, totaling $277,000. This withdrawal was done without Young's permission or consent.

88. Young contacted Coinbase's customer support several times after realizing that his Coinbase Wallet had been accessed without his consent and drained (Case Nos. #13340849, 13139490, 13156885, 12929072, 12942368, 12959833, 12930037, 12920332, 12870696, 12870361, 12869759, 12867721, 12814417, 12870361, 12869759, 12814398, 12814370,

12624735, 12423421). Young filed a formal complaint with Coinbase regarding the unauthorized transactions. In response, Coinbase informed Young that it would need 20 days to investigate his complaint. On or around August 2, 2022, Coinbase informed Young that it was closing his case, although no findings were provided to Young from Coinbase's investigation and no guidance was provided to assist him in recovering his assets.

89. Young, a retiree and single dad, has lost his entire life savings as a result of the Coinbase scam and incurred substantial debt during the process. Young suffered significant emotional and mental anguish due to the impact the financial loss has had on his ability to provide for his family and repay money that was loaned to him.

Dated: November 9, 2022

Respectfully submitted,

/s/ Eric S. Rosen

Eric Rosen
Amos Friedland
Jordana Haviv
Constantine Economides
Kelvin Goode
Maya S. Jumper
FREEDMAN NORMAND FRIEDLAND LLP
99 Park Avenue, 1910
New York, NY 10016
Tel.: (646) 350-0527
erosen@fnf.law
afriedland@fnf.law
jhaviv@fnf.law
ceconomides@fnf.law
kgoode@fnf.law
mjumper@fnf.law

Counsel for Claimants