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.

**SECOND SUPPLEMENT TO THE CONSOLIDATED DEMAND FOR ARBITRATION**

**Case No. 01-22-0004-3719**

This Second 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, as well as the first supplemental demand, filed on November 9, 2022 ("First Supplement"). This Second Supplement is intended to add additional Coinbase Wallet Victims as Claimants to the pending matter.

## I. PARTIES

### A. Claimants

1. Claimant Daniel Ryals is a resident of Maryland. In or around September 2022, Mr. Ryals's crypto, valued at approximately $356,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Mr. Ryals's factual allegations is included below in Section II.A.

2. Claimant Kyle Magnuson is a resident of Minnesota. Between February and March 2022, Mr. Magnuson's crypto, valued at approximately $50,011 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Mr. Magnuson's factual allegations is included below in Section II.A.

3. Claimant Gordon Shaylor is a resident of California. In or around December 2021 and August 2022, Mr. Shaylor's crypto, valued at approximately $1,200,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Mr. Shaylor's factual allegations is included below in Section II.A.

4. Claimant Jack Yao is a resident of California. Between June and July 2022, Mr. Yao's crypto, valued at approximately $310,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Yao's factual allegations is included below in Section II.A.

5. Claimant Tao Wang is a resident of California. Between June and July 2022, Mr. Wang's crypto, valued at approximately $658,744 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Mr. Wang's factual allegations is included below in Section II.A.

6. Claimant Keith Bolin is a resident of Florida. Between March and September 2022, Mr. Bolin's crypto, valued at approximately $237,149 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Mr. Bolin's factual allegations is included below in Section II.A.

7. Claimant Jun (Vicky) Huang is a resident of Hong Kong. In or around October 2022, Ms. Huang's crypto, valued at approximately $186,082 USDT, was stolen from her Coinbase Wallet in transactions that she did not authorize. A detailed description of Ms. Huang'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

8. 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. **Daniel Ryals**

9. On or around May 5, 2022, Claimant Daniel Ryals ("Ryals") was contacted by an individual through Telegram who introduced him to a dapp on Coinbase through which he was told he could earn significant income through a liquidity mining pool. Having lulled Ryals into the

[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.

prospect of significant returns on investment, the individual directed him to deposit USDT into his Coinbase Wallet and open a link to a dapp called CBBB ("cbbb.net/#/index") through his Coinbase Wallet browser. The individual assured Ryals that no one could access his Wallet without his 12-word security passphrase.

10. On or about June 16, 2022, Ryals followed these instructions and joined the mining pool through the dapp. Unbeknownst to Ryals, by following the directions provided by the scammer, Ryals entered into a malicious smart contract that would allow third-party scammers to gain access to withdraw assets from Ryals' Wallet without his consent.

11. During the process of joining the pool, Ryals received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet. Ryals never provided anyone with his 12-word security passphrase.

12. To fund the pool on the CBBB dapp, Ryals made 25 deposits into his Coinbase Wallet between June and August of 2022. The dapp reflected that Ryals was receiving the returns promised on his Wallet deposits. Based on this experience, Ryals decided to join a second liquidity mining pool after he was contacted by a second scammer who introduced him to a dapp called UForce ("uforce.top/index").

13. On or around August 15, 2022, Ryals joined the UForce mining pool by clicking a button that unknowingly entered him into another malicious smart contract. To fund the UForce pool, Ryals made 4 deposits into his Coinbase Wallet.

14. Between June 16 and September 22, 2022, scammers, through unauthorized transactions, stole all of the USDT in Ryals' Coinbase Wallet, totaling $356,000. These withdrawals were done without Ryals' permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

15. Immediately after realizing that his assets had been stolen through these fraudulent dapps, and that Coinbase's security assurances were false, Ryals contacted Coinbase's customer support to report the thefts (Case Nos. #13136984, #12948590). In response, Coinbase informed him that it would "flag[]" the malicious dapps to its security and investigation teams and that

Coinbase "cannot reimburse or credit [his] wallet." Coinbase then instructed Ryals to file a complaint with the FBI. In a subsequent response, Coinbase acknowledged that Ryals "did not consent to [the reported] transaction with the intent of actively compromising [his] funds."

16. As a result of the Coinbase Wallet scams, Ryals has lost a significant portion of his life savings, and incurred debt as a result of loans taken to fund the dapp deposit demands. These financial losses have resulted in significant emotional and mental distress to Ryals.

**b. Kyle Magnuson**

17. On or around January 21, 2022, a woman contacted a friend of Claimant Kyle Magnuson ("Magnuson") through Twitter and introduced him to a liquidity mining pool on Coinbase. Based on his friend's assurances, Magnuson decided to join the pool as well. After befriending Magnuson's friend, the woman introduced Magnuson to a female friend of hers who encouraged him to to increase his investments in the liquidity mining pool.

18. On or around February 6, 2022, following the instructions the woman provided to his friend, Magnuson opened the provided link to a dapp called 4moreusdt (https://4moreusdt.com/bnb/index.html) and deposited funds into his Coinbase Wallet to fund the pool. Once on the dapp, Magnuson unknowingly purchased a "voucher" which allowed third-party scammers to access his Wallet through a malicious smart contract. At all relevant times, Magnuson, having relied on Coinbase's security assurances, believed that his Wallet could only be assessed using his secure 12-word security passphrase.

19. During the process of joining the pool, Magnuson received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet. Magnuson never gave his 12-word security passphrase to anyone else.

20. To fund the pool, Magnuson made 20 deposits of USDT into his Coinbase Wallet. Initially, Magnuson saw returns on the deposits made to his Coinbase Wallet and believed that the dapp was legitimate, so he continued to deposit additional funds. Further, scammers working as customer service representatives on the dapp repeatedly assured Magnuson that his funds were

securely held in his Coinbase Wallet, even telling him at one point that "if this wasn't legit why would Coinbase allow this app to be attached to their Wallet."

21. Between February and March 2022, scammers, through unauthorized transactions, stole all of the USDT in Magnuson's Coinbase Wallet, amounting to approximately $50,011. These withdrawals were done without Magnuson's permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

22. Magnuson contacted Coinbase's customer support after realizing his Coinbase Wallet was drained and that the dapp scammers had no intention of returning his funds (Case No. #13863249). In response, Coinbase informed Magnuson that it was "flagging th[e] malicious dapp" and acknowledged that Magnuson "did not consent to this Approval transaction," but refused to reimburse or credit his Wallet. At no point did Coinbase provide Magnuson with any assistance in recovering his stolen assets.

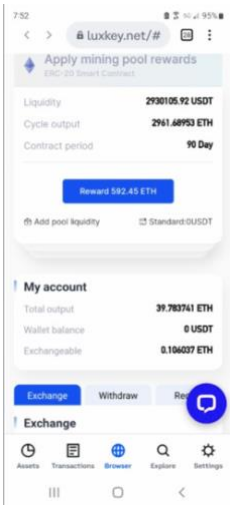
23. Magnuson has lost his entire life savings, has gone into substantial debt from loans undertaken due to the trust he placed in Coinbase Wallet, and has suffered significant mental anguish as a result of the financial impact of the unauthorized transactions.

**c. Gordon Shaylor**

24. On or around December 17, 2021, Claimant Gordan Shaylor ("Shaylor") was contacted by a woman named Sa Li through Facebook. After befriending Shaylor, Sa Li began communicating with him on WhatsApp and encouraged Shaylor to join a liquidity mining pool, which she assured Shaylor was a safe investment opportunity.

25. To join the pool, Sa Li directed Shaylor to open a Coinbase Wallet account and deposit USDT into his Coinbase Wallet.

26. Shaylor was then instructed to open the link for Luxkey.net through his Coinbase Wallet browser. Shaylor was instructed to purchase a "node," which unbeknownst to him, provided scammers unfettered access to his Coinbase Wallet.

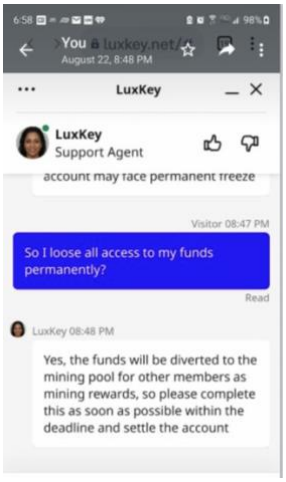



27. To fund the pool, Shaylor made multiple deposits of USDT into his Coinbase Wallet over the course of nine months. The fraudulent dapp reflected that Shaylor was receiving significant returns of interest on his deposits so Shaylor continued to head to encouragement of Sa Li to deposit more and more money into his Wallet.

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

29. At all relevant times, Shaylor believed that his funds were securely held in his Coinbase Wallet and could not be accessed or withdrawn without his unique 12-word recovery phrase. Shaylor never authorized the withdrawal of his crypto from his Coinbase Wallet and never provided anyone else with his unique 12-word recovery phrase.

30. After Shaylor's attempt to withdraw his funds from Wallet, on or around August 2022, scammers, through an unauthorized transaction, stole all of the USDT in Shaylor's Coinbase Wallet, amounting to approximately $1,200,000. This withdrawal was done without Shaylor's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.




31. Shaylor contacted Coinbase's customer support numerous times after realizing his Coinbase Wallet was drained and that the fraudulent dapp had no intention of returning his funds (Case Nos. #12881296, #13198763, #13199065, #1353091). Coinbase's initial generic response was entirely unhelpful and not tailored to Shaylor's complaint details. In a subsequent response, Coinbase advised Shaylor that "he may be interacting with a malicious third party/decentralized app (dApp) as what [he was] describing is not a common industry standard within cryptocurrency trading protocol." Coinbase denied any liability for Shaylor's loss and advised him "to be sure that you trust the dApp you're interacting with" to avoid further loss. Coinbase offered Shaylor no assistance in recovering his funds.

32. As a result of the fraud scam facilitated through Coinbase's platform, Shaylor lost all of his life savings at age 60, 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. Jack Yao**

33. On or around May 30, 2022, Claimant Jack Yao ("Yao") was introduced to a liquidity mining pool investment opportunity by his friend, Claimant Tao Wang ("Wang"), who had been contacted by a woman named Li Zhu on WeChat.

34. After communicating with his friend about the investment pool, Yao agreed to join the pool as well. Based on the assurances from his friend and the reputation of Coinbase, Yao believed that the investment opportunity was legitimate. Yao also understood the Coinbase Wallet app required iPhone FaceID authentication to authorize any transaction through the app.

35. On or around May 30, 2022, Yao deposited USDT into his Coinbase Wallet, and opened the provided link for a dapp called Coinbase Farm (coinbase-farmab.com) through his Coinbase Wallet browser to join the mining pool. Relying on Coinbase's App Lock setting, which informs users that authentication is required for every transaction, Yao believed that his crypto was securely held in his Coinbase Wallet and could not be accessed or withdrawn without his unique 12-word recovery phrase and iPhone FaceID authentication.

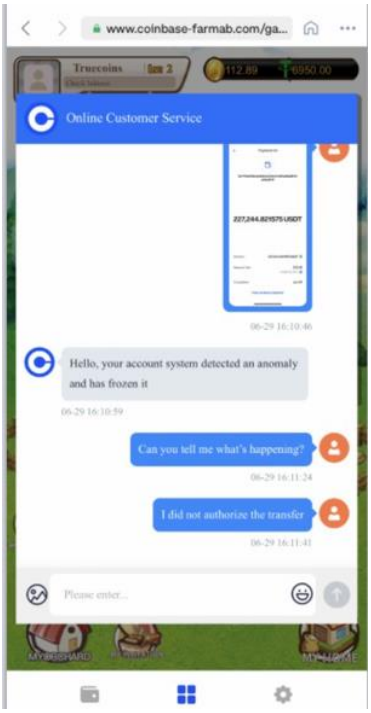
36. During the process of joining the pool, Yao received no warnings from Coinbase stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

37. To fund the pool, Yao made 6 deposits of USDT into his Coinbase Wallet. Immediately, after depositing the initial funds into his Coinbase Wallet, Jack was able to see his crypto through his Coinbase Wallet account and believed that the investment pool was operating as promised.

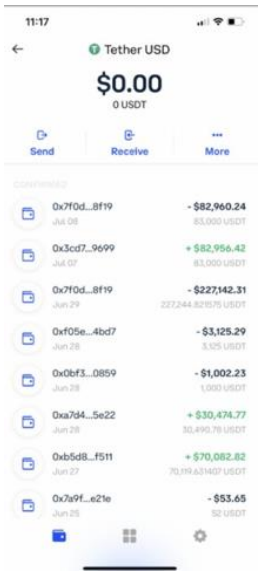
38. On or around June 28, 2022, Yao received an invitation from the dapp to join a "special event" which would require him to send money from his Coinbase Wallet directly to a separate wallet address. Yao declined to participate.

39. The following day, scammers from the dapp drained Yao's entire Wallet. Yao promptly contacted his friend who informed him that his Wallet had also been drained. Yao immediately contacted the dapp's customer service representative about the unauthorized withdrawal and he was informed that his account had been "frozen" and his crypto "transferred to a custodian account because they detected abnormal activit[y]."

40. The dapp representative instructed Yao that he would have to deposit additional funds into his Wallet in order to unfreeze his account. On or around July 7, 2022, Yao, desperate to retrieve his crypto, complied with the demand and deposited additional funds into his Wallet. Hours later, Yao's Wallet was drained again by the fraudulent dapp and the representative stopped responding to Yao's messages.




41. On or around June 29 and July 9, 2022, scammers, through unauthorized transactions, stole all of the USDT in Yao's Coinbase Wallet, totaling $310,000. These withdrawals were done without his permission or consent and without any notification, warning, or substantive response from Coinbase.



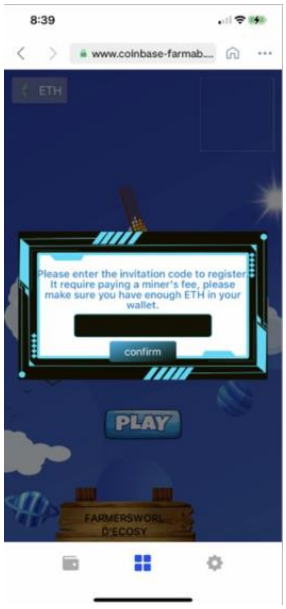

42. Upon realizing that his assets had been stolen through the dapp, Yao promptly contacted Coinbase's customer support to report the theft and flag the fraudulent dapp (Case No. #12478787). In response, Coinbase informed Yao that it could not recover his funds and advised him to contact law enforcement to report the theft.

43. Yao has lost his entire life savings and suffered significant mental and emotion distress as result of the unauthorized transactions.

**e. Tao Wang**

44. On or around May 10, 2022, Claimant Tao Wang ("Wang") was introduced to a liquidity mining pool by a woman named Li Zhu on WeChat. After multiple conversations with Wang, Li shared her interests in cryptocurrency and introduced Wang to what she described as an "internal test project" that Coinbase was offering by personal invitation through a dapp called Coinbase Farm (https://www.coinbase-farmab.com/).

45. Li then provided Wang with an invitation code to the dapp and directed Wang to participate in the investment opportunity. Wang accessed the dapp through his Coinbase Wallet browser and began depositing funds into his Wallet to fund the investment.




46. Initially, the investment opportunity worked as Li had described and Wang was receiving returns into his Coinbase Wallet account. Based on this experience and his reliance on the reputation of Coinbase, Wang shared the opportunity with Claimant Yao and others.

47. To fund the pool, Wang made 10 deposits of USDT into his Coinbase Wallet.

48. During the process of joining the pool, Wang never received any warnings from Coinbase stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

49. Between June 9 and July 28, 2022, scammers, through unauthorized transactions, stole all of the USDT in Wang's Coinbase Wallet, totaling approximately $658,744. These withdrawals were done without his permission or consent and without any notification, warning, or substantive response from Coinbase.

50. Wang 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. # 12360453, 1236076, 12437722, 12650004). In response, Coinbase requested additional information regarding the fraudulent dapp, which Wang provided. Weeks later, Coinbase informed Wang that it could not recover his funds and advised him to contact law enforcement to report the theft. After further outreach from Wang, Coinbase finally stated that they would "flag[] this malicious dapp to [Coinbase's] security and investigation teams." Coinbase failed to provide Want with any meaningful assistance to retrieve his stolen assets. Two months after Wang's report and Coinbase's "flag" of the dapp, Wang noticed that the dapp was still accessible on the Coinbase Wallet platform.

51. Wang has been financially devasted by the loss of his assets, comprised of his life savings. He has suffered significant mental and emotional distress as a result of the scammers' unauthorized use of his Wallet.

**k. Keith Bolin**

52. On or around April 1, 2022, an individual contacted Claimant Keith Bolin ("Bolin") through Facebook. After befriending Bolin, the individual encouraged Bolin to join a liquidity mining pool with the prospect of earning significant income on his investments. The individual provided Bolin with step-by-step instructions and directed him to use his Coinbase Wallet app and deposit USDT into his Coinbase Wallet. Once on the Coinbase Wallet app, the individual directed

Bolin to open a link to a dapp called UPLANAMM through his Coinbase Wallet browser in order to join the mining pool.

53. On or around May 1, 2022, Bolin followed the instructions provided and clicked a button to participate in the pool, which unknowingly entered him into a malicious smart contract.

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

55. To fund the pool, Bolin made multiple deposits of USDT and ETH into his Coinbase Wallet between March and September of 2022. After months of participation in the mining pool, during which Bolin believed his crypto was securely held in his Wallet, Bolin attempted to transfer some of his crypto to his bank account. The dapp flagged Bolin's account and informed him that he could not transfer his funds due to a smart contract which required that he keep his money in his Wallet for a certain period of time. After multiple communications with the dapp's customer service representative, the dapp told Bolin that it needed to "verify" his account before it released his funds. Bolin continued to demand the return of his assets for weeks. No funds were ever returned to Bolin and the dapp representative stopped responding to his messages.

56. In or around October of 2022, scammers, through unauthorized transactions, stole all of the crypto in Bolin's Coinbase Wallet, totaling $264,197.69. These withdrawals were done without Bolin's permission or consent.

57. Bolin contacted Coinbase's customer support by phone and email after realizing that his Coinbase Wallet had been accessed without his consent and drained (Case Nos. # 13348266, 13183163). In response, Coinbase sent Bolin nonsensical responses providing general guidance with troubleshooting tips and browser extension use.

58. Bolin has lost his life savings as a result of the Coinbase scam and incurred substantial debt during the process. Bolin 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.

**k. Jun (Vicky) Huang**

59. On or around September 6, 2022, a man named Jason contacted Claimant Jun (Vicky) Huang ("Huang") through WhatsApp. After befriending Huang, Jason began to tell her about his interest in cryptocurrency and introduced her to a crypto investment opportunity using Coinbase Wallet.

60. On or around September 12, 2022, Jason provided Huang with step-by-step instructions to download the Coinbase Wallet app and deposit USDT into her Coinbase Wallet.


61. Once on the Coinbase Wallet app, the individual directed Huang to open a link to a dapp called "GOE" (https://goe-defi.me/#/) through the Coinbase Wallet browser in order to join the mining pool.

62. Huang researched the URL that Jason provided to see assess its legitimacy and found no warnings of fraudulent activity connected with the dapp URL. Based on this information, Jason's assurances, and the reputation of the Coinbase platform, Huang decided to participate in the pool.

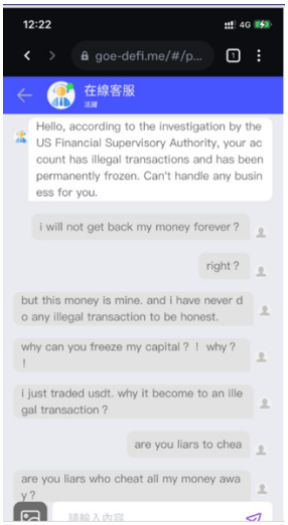
63. Huang then followed Jason's instructions and clicked a button to participate in the pool. Unbeknownst to Huang, these actions entered her into a malicious smart contract with scammers operating the dapp on Coinbase's platform. Jason even agreed to send her ETH to pay the mining node fee on the dapp.

64. During the process of joining the pool, Huang received no warnings from Coinbase stating that she was exiting the internal platform, or that she was giving any third parties access to withdraw crypto from her Coinbase Wallet by using the external dapp. At all times, Huang believed that her funds were secure in her Coinbase Wallet account.

65. To fund the pool, made 10 deposits of USDT into her Coinbase Wallet between September and October 2022. Over the course of her participation, Huang believed that her assets were securely held in her Coinbase Wallet and could not be accessed without her security passphrase, which she had not revealed to anyone.

66. On October 1, 2022, Huang received a notification from the dapp informing her that her account had been frozen due to "illegal activity" and she would need to make an additional deposit of funds into her Coinbase Wallet to unfreeze and retrieve her funds.

67. Once Huang made the additional deposit, a customer representative of the dapp informed her that her account would be "permanently frozen" due to an "investigation by the US Financial Supervisory Authority" revealing "illegal transactions" on her account. Shortly thereafter, the dapp representative stopped responding to Huang's messages requesting the return of her funds.



68. After freezing Huang's account, in or around October of 2022, scammers, through an unauthorized transaction, stole all of the USDT in Huang's Coinbase Wallet, totaling $186,082. This withdrawal was done without her permission or consent.

69. Huang contacted Coinbase's customer support several times after realizing that she had fallen victim to a scam on Coinbase Wallet's platform (Case No. #13683345). In response, Coinbase informed her that she had signed a transaction which gave a "malicious third party access to the funds held inside your Coinbase Wallet" but that Coinbase cannot revert or recover her stolen funds. Huang replied to Coinbase's response stating that "you are a company that advertises that the wallet you provided is very secure. How can you allow unauthorized transactions to happen without any notification to me?" Coinbase responded by accusing Huang of disclosing her security seed phrase (which she had not done) and informed her that customers are "solely responsible for their wallets' security."

70. Huang has lost her entire life savings as a result of the Coinbase scam and finds herself in significant debt due to loans taken out to fund the pool. Huang suffered significant emotional and mental anguish due to the impact the financial loss has had on her family's life.

Dated: January 20, 2023

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*