

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

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.

**CONSOLIDATED DEMAND FOR
ARBITRATION**

Claimants bring this Consolidated Arbitration Demand, pursuant to the arbitration provision contained in the Coinbase Wallet Terms of Service Agreement¹ (“Coinbase Wallet Terms”), alleging

¹ A true and correct copy of the Coinbase Terms of Service Agreement, containing the operative arbitration agreement is attached hereto as Exhibit 1. Coinbase Wallet Terms were updated in

violations of the Electronic Funds Transfer Act, 15 U.S.C. Section 1693 *et. seq.* (“EFTA”) and 12 C.F.R. Sections 1005-1005.20 (“Regulation E”), as well as other statutes and theories of liability as set forth herein, against Toshi Holdings Pte. Ltd. (“Toshi Holdings”), Coinbase, Inc., and Coinbase Global, Inc. (collectively, “Coinbase”).²

I. NATURE OF THE ACTION

1. This case is about a glaring security flaw in the Coinbase Wallet (the “Coinbase Wallet” or the “Wallet”), a non-custodial electronic wallet that Coinbase portrays as a safe, secure mechanism for users to store digital assets, like Bitcoin, Ethereum, and USDT (hereinafter, “crypto”). In fact, due to a compromised user interface that effectively lulls Wallet users into a false sense of security, the Wallet allows scammers to hijack customers’ Wallets and withdraw all of their crypto assets without authorization. Making matters worse, Coinbase had been repeatedly told about this security flaw for months, beginning in the early fall of 2021, but took no remedial steps to fix the security flaw or even warn customers about this major problem, despite warning customers about other security risks. Because of this, hundreds of Wallet users, many of whom stored their entire life savings (and more) in their Wallet, had their crypto stolen by thieves. This action will hold Coinbase accountable for this horrific security flaw that has devastated the lives of hundreds of people, all victims of this easily preventable scam.

2. Scams are nothing new in crypto. As relevant here, “liquidity mining pool scams” present themselves to customers in the form of decentralized applications (“dapps”) accessed through a browser on the Coinbase Wallet. Luring customers in through the promise of high yields earned in “liquidity mining pools,” scammers deploy malicious smart contracts, typically disguised as “voucher” purchases, “mining certificates,” or “node” connections. Once a user clicks on the contract to purchase a “voucher,” “mining certificate,” or “node,” the smart contract, in effect, plants a “Trojan Horse” in

September 2022, well after the Claimants here used their Wallets and had their crypto stolen. Accordingly, those new terms do not apply here.

² Prior to filing this arbitration demand, the parties entered into and extended an agreement to toll the statute of limitations period on any claims. The period from August 4, 2022 to October 14, 2022 would not be included in calculating any statute of limitations, if applicable.

the Wallet. Unbeknownst to the user, who think that they are spending *de minimus* funds to purchase a voucher, the smart contract allows the scammers, once sufficient crypto is loaded into the Wallet, to surreptitiously steal all of a customer's crypto through unauthorized transactions, effectively draining the Wallets of their assets.³ The scams succeed because Coinbase designed a flawed user interface that completely failed to warn its customers that the malicious smart contracts have the ability to access and *withdraw* (without the users' consent) unlimited amounts of users' crypto from their Wallets, both at the time the contract was entered into *and in the future*.⁴ Without adequate (or any) warnings, Coinbase's customers relied on the security assurances of Coinbase and unknowingly entered into these smart contracts that enabled these thefts to occur.

3. When these scams first started in the fall of 2021, customers immediately warned Coinbase's customer service about the security flaws in the Wallet.⁵ Customers even created YouTube videos about the Coinbase liquidity mining pool scams.⁶ And in its SEC filings, Coinbase confirmed that wallet security was a paramount concern and that malicious smart contracts posed a stark security threat. Nonetheless, Coinbase refused to take measures to: warn its customers about the scams,⁷ respond to the ongoing threat, take down or block the scam dapps that customers were warning

³ A "liquidity mining pool" is a process in which crypto holders lend assets to a decentralized exchange in return for rewards and interest. "Smart contracts" are programs stored on the blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

⁴ To be clear, the victims here were not fraudulently induced by a bad actor to make payments through the Wallet; instead, these were unauthorized transfers in which the user's Wallet was surreptitiously accessed by a "smart contract" allowed by the Coinbase Wallet and used to transfer crypto out of the Wallet without the user's consent.

⁵ See, e.g., Jeremy Merrill and Steven Zeitchik, *An ex-cop fell for Alice. Then he fell for her \$66 million crypto scam*, Washington Post, April 4, 2022, <https://www.washingtonpost.com/technology/2022/04/04/crypto-scams-coinbase-liquidity-mining/>.

⁶ See, e.g., <https://www.youtube.com/watch?v=W4-EEddpwx4;>
<https://www.youtube.com/watch?v=KiJIUd1-wZg;>
<https://www.youtube.com/watch?v=SfANI70UNno&t=226s>

⁷ See, e.g., Coinbase, *Around The Block Ep 8 - Crypto Security 101 with Coinbase's Mark Nesbitt*, <https://youtu.be/M4Q7kita0Nc>.

Coinbase about, change the design or user interface of its Wallet to fix the problem, or reimburse customers for their losses.

4. In fact, Coinbase did the opposite. When customers informed Coinbase about the thefts, Coinbase typically provided generic email responses that appear to have been crafted by “bots,” falsely stating that customers’ 12-word seed phrases had been compromised and that there was nothing Coinbase could do about the missing funds.⁸ Coinbase provided this generic response despite being repeatedly informed that the theft of the “seed phrases” had not occurred. Further, despite receiving numerous and repeated warnings as early as September 2021, Coinbase perplexingly stayed silent about the liquidity mining pool scams for six months, even while Coinbase Wallet’s terms and conditions continued to falsely reassure customers entrusting their financial lives to Coinbase that the seed phrase “is the *only* way to access the cryptocurrency associated” with the Wallet.⁹ For the most part, despite being told the specific URLs and names of the scam dapps, Coinbase did not even block or take down the malicious dapps, thereby leaving its own customers sitting ducks for fraudsters. When Coinbase finally addressed the issue in March 2022, its response was deficient and misleading. Coinbase released a purported public service announcement telling users that the scam was a crypto-wide problem targeting all non-custodial wallets, instead of a flaw specific to the Coinbase Wallet, and to bolster that contention, Coinbase tweeted out false, misleading Tweets that continued to tout the supposedly significant security features of the Wallet that would prevent thieves from stealing its customers’ crypto.

5. To date, while Coinbase has not fixed the security flaw in its Wallet or made its customers whole, Coinbase has demonstrated that the company had an ability to warn customers prior to entering into scam liquidity mining pools and block customers from accessing the scam liquidity

⁸ See, e.g., Scott Zamost et al., *Coinbase slammed for what users say is terrible customer service after hackers drain their accounts*, CNBC, August 24, 2021, <https://www.cnbc.com/2021/08/24/coinbase-slammed-for-terrible-customer-service-after-hackers-drain-user-accounts.html>.

⁹ See Exhibit 1; see also Coinbase Wallet Terms of Service (October 21, 2021) <https://web.archive.org/web/20220315215118/https://wallet.coinbase.com/terms-of-service>. The terms of service, dated October 21, 2021, claimed that the seed phrase was “the only way to access the cryptocurrency” in the Wallets, thereby giving new customers an undeserved and false sense of security.

mining pools. In that regard, shortly after counsel for the Claimants here sent Coinbase a draft complaint in late July 2022, Coinbase immediately installed warnings on the web page of many of the scam dapps that were stealing its customers' money. These warnings informed customers that the dapps were "dangerous" to the user. Of course, had Coinbase installed these warnings months earlier, when Coinbase first learned about these malicious liquidity pools, many of its customers' life savings would have been saved.

6. As a result of Coinbase's grossly negligent actions and incompetent response, Claimants and hundreds (if not thousands) of Coinbase Wallet customers have had their valuable crypto drained from their Wallets. This Firm alone represents nearly 100 Claimants who have lost more than \$21 million through the security flaws in Coinbase Wallet.

7. In the absence of adequate warnings from Coinbase, users flocked to social media to share information related to the Coinbase liquidity mining pool scams. A Facebook group dedicated to the Coinbase Wallet liquidity mining scam has nearly 300 members, and a Reddit sub-group on the same subject has more than 2,000 members.

8. The consequences of the thefts facilitated on Coinbase's platform have been devastating. The stolen funds were victims' life savings, retirement funds, children's educational funds, medical funds, and/or home down payments. Victims even borrowed funds from friends and family to fund the liquidity mining scams, and they are now plunged into debt because they must now pay back these funds. For Claimants and hundreds of other victims of this entirely foreseeable and preventable tragedy, their financial lives will never recover.

9. In response to that far-reaching damage, Coinbase has failed to take responsibility or make any assurances to customers that it intended to correct the problems. It has refused to reimburse Claimants or other customers for the drastic losses facilitated by Coinbase's security flaws and failed warnings—even as the Company's upper management enriched themselves through the sale of massive quantities of company stock.¹⁰ Instead, Coinbase has changed the terms and conditions for

¹⁰ Coinbase went public through a direct listing in the spring of 2021, and at its peak in November 2021, traded at more than \$340/share. As of July 22, 2022, Coinbase is trading at approximately \$72/share. Between April 2021 and July 2022, Coinbase insiders sold nearly \$6 billion worth of

the use of the Wallet product to make it even more onerous and difficult to hold Coinbase responsible for the security flaws in its Wallet.

10. In sum, Coinbase’s customers have suffered the preventable loss of millions of dollars. Coinbase’s Wallet has a major security flaw, and Coinbase’s management has made a calculated decision not to invest in competent customer service, not to adequately warn customers, and not to make damaged customers whole. Such malfeasance must end.

II. PARTIES

A. Claimants

11. Claimants are Coinbase Wallet customers who were victims of fraudulent liquidity mining pool scams which resulted in the unauthorized withdrawals of crypto from their respective Coinbase Wallets through Coinbase’s application or web-based platform.

12. Coinbase Wallet has a Terms of Service Agreement (the “Agreement”), or a substantially similar version, that contains a mandatory arbitration provision applicable to Coinbase Wallet customers residing in the United States and Canada. *See* Exhibit 1. California law governs Coinbase’s Terms of Service and any action related thereto. *Id.* The Terms of Service applicable here are dated October 21, 2021.¹¹

13. Claimant Ihab W. Francis is a resident of New York. In or around January 2022, Francis’s crypto, valued at approximately \$662,883.48 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Francis’s factual allegations is included below in Section III.G.

14. Claimant Shakeeb Khan is a resident of Massachusetts. In or around February 2022, Khan’s crypto, valued at approximately \$58,000 USDT, was stolen from his Coinbase Wallet in a

shares. During that same time period, no executive purchased a single share outside of the options granted in the executives’ contracts.

¹¹ *See* Exhibit 1; *see supra* note 9.

transaction that he did not authorize. A detailed description of Khan’s factual allegations is included below in Section III.G.

15. Claimant Ich Cong Tran is a resident of California. In or around November 2021, Tran’s crypto, valued at approximately \$58,734 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Tran’s factual allegations is included below in Section III.G.

16. Claimant Autumn Pavao is a resident of California. In or around January 2022, Pavao’s crypto, valued at approximately \$72,283.00 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Pavao’s factual allegations is included below in Section III.G.

17. Claimant Johannes Masehi is a resident of California. In or around November 2021, Masehi’s crypto, valued at approximately \$43,959 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Masehi’s factual allegations is included below in Section III.G.

18. Claimant Leonard Waki is a resident of California. In or around December 2021, Waki’s crypto, valued at approximately \$312,125 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Waki’s factual allegations is included below in Section III.G.

19. Claimant Jon Leathers is a resident of Washington. In or around December 2021, Leathers’ crypto, valued at approximately \$54,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Leathers’ factual allegations is included below in Section III.G.

20. Claimant Lawrence Bateman is a resident of Arizona. In or around December 2021, Bateman’s crypto, valued at approximately \$104,088 USDT, was stolen from his Coinbase Wallet in

a transaction that he did not authorize. A detailed description of Bateman's factual allegations is included below in Section III.G.

21. Claimant Kyle Thome is a resident of Michigan. In or around January 2022, Thome's crypto, valued at approximately \$66,034 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Thome's factual allegations is included below in Section III.G.

22. Claimant Jane Doe 1 is a resident of Massachusetts. In or around March 2022, Jane Doe 1's crypto, valued at approximately \$167,383.74 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Jane Doe 1's factual allegations is included below in Section III.G.¹²

23. Claimant Jeffrey Yeager is a resident of Michigan. In or around March 2022, Yeager's crypto, valued at approximately \$519,505.43 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Yeager's factual allegations is included below in Section III.G.

24. Claimant Thomas Daly is a resident of California. In or around January 2022, Daly's crypto, valued at approximately \$43,115.12 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Daly's factual allegations is included below in Section III.G.

25. Claimant Gabriel Rockman is a resident of Maryland. In or around December 2021, Rockman's crypto, valued at approximately \$35,045.78 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Rockman's factual allegations is included below in Section III.G.

26. Claimant Maurits van Westenbrugge is a resident of Florida. In or around February 2022, van Westenbrugge's crypto, valued at approximately \$47,127.74 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of van Westenbrugge's factual allegations is included below in Section III.G.

¹² The true names of the "Jane" or "John" Doe Claimants will be provided to the arbitrator and the Defendants.

27. Claimant Chao Tian is a resident of California. In or around October 2021, Tian's crypto, valued at approximately \$102,070 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Tian's factual allegations is included below in Section III.G.

28. Claimant Filip Lorinc is a resident of Texas. In or around January 2022, Lorinc's crypto, valued at approximately \$70,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Lorinc's factual allegations is included below in Section III.G.

29. Claimant John Doe 1 is a resident of California. In or around December 2021, John Doe 1's crypto, valued at approximately \$509,828.39 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of John Doe 1's factual allegations is included below in Section III.G.

30. Claimant Raymond Leung is a resident of British Columbia. In or around December 2021, Leung's crypto, valued at approximately \$109,631.82 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Leung's factual allegations is included below in Section III.G.

31. Claimant Christian Kelly is a resident of Pennsylvania. In or around February 2022, Kelly's crypto, valued at approximately \$107,841.02 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Kelly's factual allegations is included below in Section III.G.

32. Claimant Daniel Chang is a resident of California. In or around March 2022, Chang's crypto, valued at approximately \$289,916 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Chang's factual allegations is included below in Section III.G.

33. Claimant Raphael Elbaz is a resident of New York. In or around January 2022, Elbaz's crypto, valued at approximately \$300,934 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Elbaz's factual allegations is included below in Section III.G.

34. Claimant Jun Zhai is a resident of Washington. In or around March 2022, Mr. Zhai's crypto, valued at approximately \$71,075 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Mr. Zhai's factual allegations is included below in Section III.G.

35. Claimant Leandro Paparelli is a resident of Texas. In or around October 2021, Paparelli's crypto, valued at approximately \$200,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Paparelli's factual allegations is included below in Section III.G.

36. Claimant Grigore Rosca is a resident of Massachusetts. In or around December 2021, Rosca's crypto, valued at approximately \$88,400 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Rosca's factual allegations is included below in Section III.G.

37. Claimant Wai Chan is a resident of California. In or around November 2021, Chan's crypto, valued at approximately \$223,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Chan's factual allegations is included below in Section III.G.

38. Claimant Jane Doe 2 is a resident of California. In or around February 2022, Jane Doe 2's crypto, valued at approximately \$741,170.21 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Jane Doe 2's factual allegations is included below in Section III.G.

39. Claimant Dominic Chow is a resident of Massachusetts. In or around March 2022, Chow's crypto, valued at approximately \$280,914 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Chow's factual allegations is included below in Section III.G.

40. Claimant Sabiha Goriawala is a resident of Ontario, Canada. In or around February 2022, Goriawala's crypto, valued at approximately \$54,974 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Goriawala's factual allegations is included below in Section III.G.

41. Claimant Manash Sharma is a resident of California. In or around March 2022, Sharma's crypto, valued at approximately \$116,544.60 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Sharma's factual allegations is included below in Section III.G.

42. Claimant Chengguo Dong is a resident of California. In or around November 2021, Dong's crypto, valued at approximately \$994,165 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Dong's factual allegations is included below in Section III.G.

43. Claimant James Moskwa is a resident of Rhode Island. In or around January 2022, Moskwa's crypto, valued at approximately \$1,354,603 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Moskwa's factual allegations is included below in Section III.G.

44. Claimant Anh Nguyen is a resident of California. In or around October 2021, Nguyen's crypto, valued at approximately \$222,946 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Nguyen's factual allegations is included below in Section III.G.

45. Claimant Canh Thai is a resident of Texas. In or around November 2021, Thai's crypto, valued at approximately \$1,199,294.64 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Thai's factual allegations is included below in Section III.G.

46. Claimant Eva Fengel is a resident of Georgia. In or around November 2021, Fengel's crypto, valued at approximately \$53,482.73 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Fengel's factual allegations is included below in Section III.G.

47. Claimant Nicholas Chicoine is a resident of California. In or around November 2021, Chicoine's crypto, valued at approximately \$302,597.15 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Chicoine's factual allegations is included below in Section III.G.

48. Claimant Zhangting Song is a resident of California. In or around December 2021, Song's crypto, valued at approximately \$34,082.07 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Song's factual allegations is included below in Section III.G.

49. Claimant Xiaoli Yuan is a resident of California. In or around December 2021, Yuan's crypto, valued at approximately \$49,028.43 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Yuan's factual allegations is included below in Section III.G.

50. Claimant Richard Slavant is a resident of Louisiana. In or around November 2021, Slavant's crypto, valued at approximately \$52,380.02 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Slavant's factual allegations is included below in Section III.G.

51. Claimant Dong Dong Li is a resident of Washington. In or around April 2022, Li's crypto, valued at approximately \$132,702.88 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Li's factual allegations is included below in Section III.G.

52. Claimant Trevor Lau is a resident of Ontario. In or around February 2022, Lau's crypto, valued at approximately \$250,327.96 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Lau's factual allegations is included below in Section III.G.

53. Claimant Troy Gochenour is a resident of Ohio. In or around November 2021, Gochenour's crypto, valued at approximately \$25,800 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Gochenour's factual allegations is included below in Section III.G.

54. Claimant Ethan Dang is a resident of Nevada. In or around November 2021, Dang's crypto, valued at approximately \$438,756.23 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Dang's factual allegations is included below in Section III.G.

55. Claimant Yao Li is a resident of California. In or around January 2022, Li's crypto, valued at approximately \$80,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Li's factual allegations is included below in Section III.G.

56. Claimant Dalton Green is a resident of Colorado. In or around December 2021, Green's crypto, valued at approximately \$71,143.35 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Green's factual allegations is included below in Section III.G.

57. Claimant Phuong Thanh is a resident of California. In or around January 2022, Thanh's crypto, valued at approximately \$225,000 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Thanh's factual allegations is included below in Section III.G.

58. Claimant Kelly Schmittel is a resident of Arizona. In or around May 2022, Schmittel's crypto, valued at approximately \$233,000.21 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Schmittel's factual allegations is included below in Section III.G.

59. Claimant John Doe 2 is a resident of California. In or around April 2022, John Doe 2's crypto, valued at approximately \$102,800 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of John Doe 2's factual allegations is included below in Section III.G.

60. Claimant Richard Wisinszky is a resident of Florida. In or around January 2022, Wisinszky's crypto, valued at approximately \$78,246 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Wisinszky's factual allegations is included below in Section III.G.

61. Claimant Bryce Richmond is a resident of California. In or around February 2022, Richmond's crypto, valued at approximately \$258,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Richmond's factual allegations is included below in Section III.G.

62. Claimant Eric Wong is a resident of California. In or around February 2022, Wong's crypto, valued at approximately \$92,445 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Wong's factual allegations is included below in Section III.G.

63. Claimant Henry Chen is a resident of California. In or around March 2022, Chen's crypto, valued at approximately \$121,516 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Chen's factual allegations is included below in Section III.G.

64. Claimant Kathleen Warren is a resident of Oregon. In or around January 2022, Warren's crypto, valued at approximately \$111,051.93 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Warren's factual allegations is included below in Section III.G.

65. Claimant Christopher Elkins is a resident of Oklahoma. In or around January 2022, Elkins' crypto, valued at approximately \$132,309 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Elkins' factual allegations is included below in Section III.G.

66. Claimant Akshay Raghavendra is a resident of California. In or around February 2022, Raghavendra's crypto, valued at approximately \$243,559.82 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Raghavendra's factual allegations is included below in Section III.G.

67. Claimant Jeffrey Osbun is a resident of California. In or around November 2021, Osbun's crypto, valued at approximately \$76,468.49 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Osbun's factual allegations is included below in Section III.G.

68. Claimant Sergey Demenko is a resident of Washington. In or around October 2021, Demenko's crypto, valued at approximately \$75,251 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Demenko's factual allegations is included below in Section III.G.

69. Claimant Douglas Herring is a resident of Oregon. In or around January 2022, Herring's crypto, valued at approximately \$610,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Herring's factual allegations is included below in Section III.G.

70. Claimant Deepak Soneji is a resident of California. In or around April 2022, Soneji's crypto, valued at approximately \$607,592.78 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Soneji's factual allegations is included below in Section III.G.

71. Claimant Eisi Mollanji is a resident of Ontario, Canada. In or around April 2022, Mollanji's crypto, valued at approximately \$100,471 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Mollanji's factual allegations is included below in Section III.G.

72. Claimant Robert Willis is a resident of Arizona. In or around February 2022, Willis's crypto, valued at approximately \$270,009.07 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Willis's factual allegations is included below in Section III.G.

73. Claimant Dr. Stephen Parker is a resident of South Carolina. In or around March 2022, Parker's crypto, valued at approximately \$163,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Parker's factual allegations is included below in Section III.G.

74. Claimant Sachin Garg is a resident of California. In or around December 2021, Garg's crypto, valued at approximately \$100,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Garg's factual allegations is included below in Section III.G.

75. Claimant Timothy Magnus is a resident of Washington. In or around December 2021, Magnus' crypto, valued at approximately \$30,517.13 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Magnus' factual allegations is included below in Section III.G.

76. Claimant Sudang Tjin is a resident of Georgia. In or around January 2022, Tjin’s crypto, valued at approximately \$48,520 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Tjin’s factual allegations is included below in Section III.G.

77. Claimant Jane Doe 3 is a resident of California. In or around February 2022, Jane Doe 3’s crypto, valued at approximately \$335,218.49 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Jane Doe 3’s factual allegations is included below in Section III.G.

78. Claimant Dieu Thai is a resident of Texas. In or around November 2021, Thai’s crypto, valued at approximately \$218,185.87 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Thai’s factual allegations is included below in Section III.G.

79. Claimant Anna Yuan is a resident of California. In or around January 2022, Yuan’s crypto, valued at approximately \$102,500 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Yuan’s factual allegations is included below in Section III.G.

80. Claimant Erin Finegold is a resident of California. In or around December 2021, Finegold’s crypto, valued at approximately \$303,487.47 USDT, was stolen from her Coinbase Wallet in a transaction that she did not authorize. A detailed description of Finegold’s factual allegations is included below in Section III.G.

81. Claimant John Doe 3 is a resident of Virginia. In or around June 2022, John Doe 3’s crypto, valued at approximately \$678,243.64 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of John Doe 3’s factual allegations is included below in Section III.G.

82. Claimant Joseph (“Bill”) Beakey is a resident of Florida. In or around July 2022, Beakey’s crypto, valued at approximately \$1,149,225 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Beakey’s factual allegations is included below in Section III.G.

83. Claimant Michael Gibson is a resident of South Carolina. In or around January 2022, Gibson's crypto, valued at approximately \$271,758.08 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Gibson's factual allegations is included below in Section III.G.

84. Claimant Terrence Smith is a resident of California. In or around July 2022, Smith's crypto, valued at approximately \$51,100.00 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Smith's factual allegations is included below in Section III.G.

85. Claimant Mike Liadov is a resident of Massachusetts. In or around August 2022, Liadov's crypto, valued at approximately \$120,000 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Liadov's factual allegations is included below in Section III.G.

86. Claimant Jad Ghandour is a resident of Florida. In or around November 2021, Ghandour's crypto, valued at approximately \$196,629.71 USDT, was stolen from his Coinbase Wallet in transactions he did not authorize. A detailed description of Ghandour's factual allegations is included below in Section III.G.

87. Claimant Jian Jing Shen is a resident of California. In or around July 2022, Shen's crypto, valued at approximately \$182,889.08 USDT, was stolen from her Coinbase Wallet in transactions she did not authorize. A detailed description of Shen's factual allegations is included below in Section III.G.

88. Claimant Curtis Cecil is a resident of North Carolina. In or around August 2022, Cecil's crypto, valued at approximately \$60,712.66 USDT, was stolen from his Coinbase Wallet in transactions he did not authorize. A detailed description of Cecil's factual allegations is included below in Section III.G.

89. Claimant John Doe 4 is a resident of North Carolina. In or around August 2022, John Doe 4's crypto, valued at approximately \$282,554.01 USDT, was stolen from his Coinbase Wallet in transactions he did not authorize. A detailed description of John Doe 4's factual allegations is included below in Section III.G.

90. Claimant James Buchan is a citizen of the United Kingdom. In March 2022, Mr. Buchan's crypto, valued at approximately \$87,105.98 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Buchan's factual allegations is included below in Section III.G.

91. Claimant Ali Comert is a citizen of Turkey. In March 2022, Mr. Comert's crypto, valued at approximately \$89,000 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Comert's factual allegations transfers is included below in Section III.G.

92. Claimant David Evdokimow is a citizen of Bulgaria. In November 2021, Mr. Evdokimow's crypto, valued at approximately \$492,449 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Evdokimow's factual allegations is included below in Section III.G.

93. Claimant Amine Fennane is a citizen of France. Between April 2022 and May 2022, Mr. Fennane's crypto, valued at approximately \$160,307 USDT, was stolen from his Coinbase Wallet in transactions that he did not authorize. A detailed description of Fennane's factual allegations is included below in Section III.G.

94. Claimant Vitaly Geyman is a United States citizen. In July 2022, Mr. Geyman's crypto, valued at approximately \$249,000 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Geryman's factual allegations is included below in Section III.G.

95. Claimant Shai Granovski is a citizen of Israel and Canada. Between November 2021 and December 2021, Mr. Granovski's crypto, valued at approximately \$517,477 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. At the time the crypto was stolen from him, Mr. Granovski was living in and located in Moscow, Russia. A detailed description of Granovski's factual allegations is included below in Section III.G.

96. Claimant Chris Haeusser is a citizen of Germany. In November 2021, Mr. Haeusser's crypto, valued at approximately \$52,000 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Haeusser's factual allegations is included below in Section III.G.

97. Claimant Jianling Hao is a citizen of Belgium. Between March 2022 and April 2022, Ms. Hao's crypto, valued at approximately \$80,000 USDT, was stolen from her Coinbase Wallet through transactions that she did not authorize. A detailed description of Hao's factual allegations is included below in Section III.G.

98. Claimant E. Kong is a citizen of Singapore. In January 2022, Mr. Kong's crypto, valued at approximately \$40,398 USDT, was stolen from his Coinbase Wallet in an unauthorized transaction. An additional amount of approximately \$520,000 USDT, was stolen from Mr. Kong due to transfers from his bank account to scammers' bank accounts *after* the initial USDT was taken from his Coinbase Wallet. A detailed description of Kong's factual allegations is included below in Section III.G.

99. Claimant Alicia Lau (Lau Pui Mei) is a citizen of Malaysia and a permanent resident of Singapore. Between October 2021 and December 2021, Ms. Lau's crypto, valued at approximately \$205,744 USDT, was stolen from her Coinbase Wallet through transactions that she did not authorize. A detailed description of Lau's factual allegations is included below in Section III.G.

100. Claimant Richard Mokry is a citizen of the Czech Republic. In July 2022, Mr. Mokry's crypto, valued at approximately \$26,201.80 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Mokry's factual allegations is included below in Section III.G.

101. Claimant Morten Nilsen is a citizen of Norway. In August 2022, Mr. Nilsen's crypto, valued at approximately \$155,888 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Nilsen's factual allegations transfers is included below in Section III.G.

102. Claimant Abdul-Azeez Oladapo is a citizen of the United Kingdom. In February 2022, Mr. Oladapo's crypto, valued at approximately \$108,000 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Oladapo's factual allegations is included below in Section III.G.

103. Claimant Mahmoud Osman is a Sudanese passport holder who is based in Malaysia. In October 2021, Mr. Osman's crypto, valued at approximately \$12,175 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Osman's factual allegations is included below in Section III.G.

104. Claimant Jane Doe 4 is a United States citizen. Between December 2021 and March 2022, Jane Doe 4's crypto, valued at approximately \$314,626 USDT, was stolen from her Coinbase Wallet through transactions that she did not authorize. A detailed description of Jane Doe 4's factual allegations is included below in Section III.G.

105. Claimant Ivo van Reenen is a citizen of the Netherlands. In December 2021, Mr. Reenen's crypto, valued at approximately \$83,689 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Reenen's factual allegations is included below in Section III.G.

106. Claimant Miha Soršak is a citizen of Slovenia. In April 2022, Mr. Soršak's crypto, valued at approximately \$110,346 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Soršak's factual allegations is included below in Section III.G.

107. Claimant Paul Wilkinson is a citizen of the United Kingdom. In December 2021, Mr. Wilkinson's crypto, valued at approximately \$70,699 USDT, was stolen from his Coinbase Wallet in a transaction that he did not authorize. A detailed description of Wilkinson's factual allegations is included below in Section III.G.

108. Claimant Edmund Yeo is a citizen of Singapore. Between December 2021 and January 2022, Mr. Yeo’s crypto, valued at approximately \$346,652 USDT, was stolen from his Coinbase Wallet through transactions that he did not authorize. A detailed description of Yeo’s factual allegations is included below in Section III.G.

B. Respondents

109. Respondent Toshi Holdings Pte. Ltd. is a Singapore private limited company and wholly owned subsidiary of Coinbase Global, Inc. Toshi Holdings makes the crypto access device known as the Coinbase Wallet.

110. Respondent Coinbase, Inc. is a Delaware company and wholly owned subsidiary of Coinbase Global, Inc. Coinbase, Inc. has its principal place of business in San Francisco, California, maintains its executive offices in San Francisco, California, is registered with the Secretary of State of California, and has an agent for service of process in California.

111. Respondent Coinbase Global, Inc. is a publicly traded Delaware company. Coinbase Global, Inc. has its principal place of business in San Francisco, California, maintains its executive offices in San Francisco, California, is registered with the Secretary of State of California, and has an agent for service of process in California. In Coinbase’s S-1 statement of registration, filed with the SEC on or about March 17, 2021, Coinbase’s CEO described Coinbase as a “company with an ambitious vision: to create more economic freedom for every person and business.”

112. As stated in Coinbase Global, Inc.’s May 11, 2022 Form 10-Q, Coinbase Global, Inc., and Coinbase, Inc, are operationally the same company—the companies are referred to by Coinbase Global, Inc. collectively as “the ‘Company’” which “operates globally and is a leading provider of end-to-end financial infrastructure and technology for the cryptoeconomy” and “offers retail users the primary financial account for the cryptoeconomy, institutions a state of the art marketplace with a deep pool of liquidity for transacting in crypto assets, and ecosystem partners technology and services that enable them to build crypto-based applications and securely accept crypto assets as payment.” Given the corporations’ expressly stated activities, Coinbase Global, Inc., Coinbase Inc. and Toshi Holdings,

which makes the Coinbase Wallet, are a single enterprise financial institution for purposes of liability for Claimants' claims.

III. FACTUAL ALLEGATIONS

A. The Coinbase Wallet

113. Centralized finance ("CeFi") describes the type of finance in which banks and brokerages retain custody of customers' assets. Similarly, in the world of crypto, centralized exchanges like Binance and Coinbase, Inc. take custody over their customers' crypto. Decentralized finance ("DeFi"), in contrast, involves banking and financial services based on peer-to-peer payments through blockchain technology. Effectively, DeFi transactions, executed through automatic smart contracts on the blockchain, allow consumers to sidestep financial middlemen such as banks and brokers.

114. To access and participate in DeFi, consumers typically use a non-custodial electronic wallet account to store crypto and interact with DeFi programs and applications. A non-custodial wallet means that the wallet itself does not have custody over consumers' assets; rather, the wallet serves as an interface or access device that allows consumers to access self-custodied assets while also allowing third-party application integrations in the DeFi space. In other words, non-custodial wallets exist to help owners of crypto access those assets on blockchains and then use those assets—including, for example, withdrawing the assets or employing the assets in a DeFi application. Non-custodial wallets are made by numerous companies, including MetaMask, Binance (Trust Wallet), and Coinomi. Coinbase, a leading US-based crypto-asset exchange, also has its own non-custodial wallet called the Coinbase Wallet.¹³

115. Coinbase, Inc. has both an exchange, which hosts customers' assets in hosted wallets (Coinbase.com), and a DeFi platform, which is Coinbase Wallet (a non-custodial wallet). With its

¹³ Generally, crypto wallets are categorized by who has custody of the wallet's private key. A private key or seed phrase is a set of randomized numbers and letters assigned to the consumer's wallet that grants access to spend, trade, or do other things with the crypto contained therein. A crypto wallet is considered a custodial wallet when a service, like a crypto exchange such as Coinbase, controls the private key to the consumer's wallet and directly holds a person's crypto in their custody. A crypto wallet is considered non-custodial when the consumer has control of their private key.

exchange, Coinbase directly holds consumers' crypto in a hosted wallet controlled by Coinbase. With Coinbase Wallet, Coinbase indirectly holds the consumers' crypto in a non-custodial wallet account. Each system has its own benefits. With a non-custodial Wallet account, for example, it is difficult to exchange fiat currency for crypto, which can be done with a hosted wallet.¹⁴ Conversely, as Coinbase explains on its website,¹⁵ consumers generally set up a non-custodial wallet, which allows "full control of the security of [the consumer's] crypto," to "access more advanced crypto activities like yield farming, staking, lending, borrowing, and more." Those types of activities generally cannot be done with a hosted wallet. To maximize their options, therefore, some Coinbase users have both a hosted and non-hosted wallet. In fact, Coinbase promotional videos encourage Coinbase users to link their custodial account to their Wallet.¹⁶

116. Toshi Holdings, a subsidiary of Coinbase, developed the Coinbase Wallet in April 2017. On August 15, 2018, Coinbase, Inc. acquired the Wallet and announced that "Toshi is becoming Coinbase wallet!"¹⁷ In the announcement, Coinbase touted the Wallet's security, telling consumers that "as part of our effort to be the most trusted brand in the space, we also set out to provide best-in-class secure storage. With Coinbase Wallet, your private keys are secured using your device's Secure Enclave and biometric authentication technology."¹⁸ Even today, Coinbase touts its non-custodial

¹⁴ Coinbase, *Tutorials*, <https://www.coinbase.com/wallet/tutorials>, last accessed on October 7, 2022.

¹⁵ Coinbase, *How to set up a crypto wallet*, <https://www.coinbase.com/learn/tips-and-tutorials/how-to-set-up-a-crypto-wallet#:~:text=A%20self%20custody%20wallet%2C%20like,to%20keep%20your%20crypto%20safe>, last accessed on October 7, 2022.

¹⁶ See, e.g., Coinbase, *Tutorial: Getting started with Coinbase Wallet*, December 20, 2021, <https://youtu.be/CZDgLG6jpgw>.

¹⁷ On August 15, 2018, through Coinbase Inc.'s official twitter account, Coinbase, Inc. made the announcement that the Toshi Wallet is now the Coinbase Wallet. Coinbase Inc.'s tweet contained a link to an August 15, 2018, blog post by Coinbase Inc.'s engineer Siddharth Coelho-Prabhu. See Coinbase Blog, *Goodbye Toshi, Hello Coinbase Wallet – the easiest and most secure crypto wallet and browser*, August 15, 2018, <https://web.archive.org/web/20211105014830/https://blog.coinbase.com/goodbye-toshi-hello-coinbase-wallet-the-easiest-and-most-secure-crypto-wallet-and-browser-4ba6e52e4913?gi=310a3de9c8b7>, last accessed on October 7, 2022; see also <https://twitter.com/coinbase/status/1029792777675005952>.

¹⁸ *Id.*

Wallet as having “Industry-leading security” that provides “more ways to keep [customers’] crypto safe and secure.”¹⁹ In fact, the Coinbase Wallet Twitter account boldly proclaims that the Coinbase Wallet is the “easiest and most secure crypto wallet and dapp browser.”²⁰

117. According to Coinbase, Inc.’s official Twitter account, the change in name from Toshi to Coinbase was “part of a larger effort to invest in products that will define the future of the decentralized web and make the future accessible to anyone.” Coinbase viewed the Wallet as customers’ “home-base for browsing the decentralized web and exploring its possibilities,” which includes storage of digital assets.²¹

118. With Coinbase Wallet, as advertised on Coinbase’s website, customers can manage ETH and ERC-20 tokens, receive airdrops, buy and store NFTs, send payments to anyone globally, access decentralized exchanges to purchase tokens, and use third-party dapps that “enable everything from taking out a loan or lending to others on the blockchain to earning crypto by answering questions, performing services, or completing tasks.”

119. To buy or sell cryptocurrencies with fiat currencies, users of the Coinbase exchange can also link their Coinbase.com account to their Coinbase Wallet. Then, users can electronically purchase or transfer funds directly through their Coinbase.com wallet account to the Coinbase Wallet.²²

120. On April 6, 2022, Coinbase posted on YouTube a recorded video interview with its Director of Engineering Chintan Turakhia.²³ During the interview, Turakhia said, in sum and substance, that customers come to Coinbase because the Coinbase brand “exudes trust” and users could be sure that Coinbase complies with all “regulatory and compliance” issues.

¹⁹ See Coinbase, *Coinbase Wallet*, <https://www.coinbase.com/wallet>, last accessed on October 7, 2022.

²⁰ See <https://twitter.com/CoinbaseWallet>.

²¹ See <https://twitter.com/coinbase/status/1029792780720074752>.

²² Coinbase, *Coinbase Wallet FAQ*, <https://wallet.coinbase.com/faq/>, last accessed on October 7, 2022.

²³ See Coinbase, *Around The Block Ep 20 – The Present & Future of Crypto Self Custody w/ Chintan Turakhia*, April 6, 2022, <https://youtu.be/ypB9rUy6hpo>.

121. Finally, all transfers between a user’s Coinbase.com and Coinbase Wallet account are completed electronically on-chain and require confirmation on the Coinbase network before being processed. Moreover, all transfers from Coinbase.com to Coinbase Wallet are subject to any restrictions outlined in Coinbase’s Terms. Coinbase Wallet users can also transfer or receive funds to or from other crypto wallets or exchanges directly through their Coinbase Wallet. Coinbase charges a fee on all transfers.²⁴

B. The Coinbase Wallet Setup

122. To create a Coinbase Wallet, a consumer just needs to either download the Coinbase Wallet application onto their smartphone or download the Coinbase Wallet browser extension to their web browser. Once downloaded, the user will then create an account by completing the following steps: create a new wallet; accept the terms of service; choose a username; select between having a private or public account; choose whether the account should have either biometric or passcode security; and pick a “recovery phrase” or “seed” phrase that customers can use to access their wallet.

123. Coinbase touts the seed phrase as being an important security component of the Wallet: “Coinbase Wallet is a user-controlled, non-custodial product. **The app generates a 12-word recovery phrase which is what gives you, and only you, access to your account to move received funds.**”²⁵ (emphasis added). Claimants relied on those representations in downloading and installing the Wallet. Further, the Coinbase Wallet website touted that: the Coinbase Wallet allowed users to “safely store” their crypto; users could “[e]xplore the decentralized web with confidence” and “[u]se DeFi liquidity pools to supply or borrow crypto; and, the Wallet allowed users to take advantage of “industry-leading security” to keep “crypto safe and secure”.²⁶

²⁴ As Coinbase provides in its February 25, 2022, 10-K: “Coinbase Wallet, a separately managed retail software product, allows users to self-custody crypto assets and NFTs in one place and interact with the cryptoeconomy and Web3, including an expanded set of approximately 5,500 crypto assets and decentralized applications. A fee is charged for select activities executed in the self-hosted wallet.”

²⁵ See <https://wallet.coinbase.com/faq/> (last accessed on October 13, 2022); see also Exhibit 1 [“Your Recovery Phrase is the only way to access the cryptocurrency associated with your Account.”]

²⁶ See <https://www.coinbase.com/wallet> (last visited, October 13, 2022).

124. Coinbase took no steps to prevent beginner or average crypto users from downloading and using the Wallet, linking their Coinbase.com account to their Wallet, or limiting the amount of crypto that could be loaded by beginner or average users into their Wallet. As Turakhia explained in the video discussed above, the Wallet set-up simply asked whether the user wanted to create a Wallet or download an already existing wallet.²⁷ The video also discussed, repeatedly and at length, the need to safeguard a user’s “seed phrase” or private key to prevent scammers from stealing assets. But the video did not mention that thieves could also steal crypto by convincing users to engage in a transaction that would later allow unlimited access to all the funds in the Wallet. To the contrary, the video walked the viewer through entering into a transaction with a third-party website that was validated with a transaction, but which allowed the third-party website access to only see what was in the Wallet but not take the assets.

125. Once a consumer’s Coinbase Wallet account is complete, Coinbase recommends that, if the consumer has a Coinbase.com account, “the first thing you would want to do is link it to your Coinbase Wallet so you can transfer your crypto,” and if you do not have a Coinbase.com account, you can “still transfer your crypto from other exchanges or wallets by sending the crypto to your Coinbase Wallet account.”²⁸

C. Coinbase Wallet’s Terms of Service

126. Coinbase asks users of Coinbase Wallet to acknowledge Coinbase Wallet’s Terms, Exhibit 1. For example, when downloading the application onto smartphones, users are asked to review the Wallet’s “Privacy Policy and Terms of Service.”

127. The Terms make clear that the Coinbase Wallet has been developed by “Toshi Holdings Pte. Ltd.,” which is a “wholly owned subsidiary of Coinbase Global, Inc.”²⁹ The terms purport to only bind “Toshi Holdings.”

²⁷ See supra note 24.

²⁸ See Coinbase, *Tutorial: Getting Started with Coinbase Wallet*, <https://youtu.be/CZDgLG6jpgw>.

²⁹ See Exhibit 1, see supra note 9. Coinbase’s revised terms of service, dated September 19, 2022 and posted on the Coinbase website, are not applicable to the Claimants.

128. Coinbase Wallet also makes the following relevant disclosures through its Terms of Service.³⁰

The Wallet Application enables users to (i) self custody digital assets; (ii) access a digital asset browser and link to decentralized applications and decentralized exchanges (‘dapp(s)’); (iii) view addresses and information that are part of digital assets networks and broadcast transactions .

* * *

You’re responsible for all activities that occur under your Account, or are otherwise referable to your Account credentials, whether or not you know about them.

* * *

TO THE MAXIMUM EXTENT NOT PROHIBITED BY LAW, TOSHI HOLDINGS SHALL NOT BE LIABLE FOR DAMAGES OF ANY TYPE, WHETHER DIRECT OR INDIRECT, ARISING OUT OF OR IN ANY WAY RELATED TO YOUR USE OR INABILITY TO USE THE SERVICES, INCLUDING BUT NOT LIMITED TO DAMAGES ALLEGEDLY ARISING FROM THE COMPROMISE OR LOSS OF YOUR LOGIN CREDENTIALS OR FUNDS, OR LOSS OF OR INABILITY TO RESTORE ACCESS FROM YOUR BACKUP PHRASE, OR FOR MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, DEFECTS AND/OR ERRORS IN THE TRANSMISSION OF TRANSACTIONS OR MESSAGES TO THE ETHEREUM NETWORK, OR THE FAILURE OF ANY MESSAGE TO SEND OR BE RECEIVED BY THE INTENDED RECIPIENT IN THE INTENDED FORM, OR FOR DIMINUTION OF VALUE OF ETHER OR ANY OTHER DIGITAL TOKEN OR DIGITAL ASSET ON THE ETHEREUM NETWORK.

TOSHI HOLDINGS SHALL NOT BE LIABLE UNDER ANY CIRCUMSTANCES FOR DAMAGES ARISING OUT OF OR IN ANY WAY RELATED TO SOFTWARE, PRODUCTS, SERVICES, AND/OR INFORMATION OFFERED OR PROVIDED BY THIRD-PARTIES AND ACCESSED THROUGH THE APP, SITE OR SERVICES.³¹

³⁰ *Id.*

³¹ The Terms of Service also state: “When using a dapp or other Third-Party Materials, you understand that you are at no time transferring your assets to us. We provide access to Third Party Materials only as a convenience, do not have control over their content, do not warrant or endorse, and are not responsible for the availability or legitimacy of, the content, products or services on or accessible from those Third-Party Materials (including any related websites, resources or links displayed therein). We make no warranties or representations, express or implied, about such linked Third-Party Materials, the third parties they are owned and operated by, the information contained on them or the suitability of their products or services. You acknowledge sole responsibility for and assume all risk arising from

129. The terms and conditions further provide that the “Terms and any action related thereto” are “governed by the laws of the state of California in the United States, without regard to its conflict of laws provisions. . . .”.

130. Finally, the terms and conditions provide users with the assurance that only by obtaining a user’s “Recovery Phrase” can a thief or hacker access the Wallet. Specifically, the terms state that: “You are solely responsible for the retention and security of your twelve word recovery phrase (“Recovery Phrase”). Your Recovery Phrase is **the only way** to access the cryptocurrency associated with your Account. Anyone that has access to your Recovery Phrase can access your cryptocurrency. If you lose your Recovery Phrase, you will not be able to access your cryptocurrency.” Customers relied on this term and condition of the contract in downloading, installing and using the Wallet.³²

D. Coinbase Wallet and Liquidity Mining with dApps

131. Centralized exchanges such as Coinbase and Binance act as “market makers” for trades out of their customer’s deposits. This centralized market-maker system is similar to how large brokerage firms trade stocks.

132. DeFi exchanges, however, trade differently. They execute protocols, built into their networks, known as Automated Market Makers (AMM). Smart contracts built into DeFi networks determine the price of a pair of cryptocurrencies being exchanged and execute the trade. However, because there is no centralized pool of assets to draw from, the exchanges rely on crowdsourced liquidity pools to provide the capital required to complete the trade.

133. To create a liquidity pool, investors use a blockchain-based smart contract to commit (*i.e.*, lend) both pairs of cryptocurrencies to the pool. In exchange for lending that crypto to the pool, the lenders get a reward based on a percentage of the trading fees associated with the DeFi protocol.

your use of any third-party websites, applications, or resources.” The Terms of Service do not disclose that a dapp can remove crypto from a user’s Wallet without obtaining the Recovery Phrase.

³² This representation is repeated in multiple places on the Coinbase website. *See, e.g.*, Coinbase, *How to link my Coinbase Wallet to my Coinbase.com account*, <https://web.archive.org/web/20211021093142/https://help.coinbase.com/en/coinbase/trading-and-funding/buying-selling-or-converting-crypto/link-my-coinbase-wallet-to-my-coinbase-account>, last accessed on October 7, 2022.

The “mining” part comes from the fact that investors typically earn liquidity pool tokens (“LP Token”), which represent the investor’s share of the total liquidity pool.

134. In sum, an investor contributes crypto into the DeFi liquidity pool. In exchange, the investor gets LP Tokens, which entitles the holder to a percentage of trading fees from each transaction within that liquidity pool. The number of LP Tokens (and the concomitant percentage of trading fees) depends on the amount of crypto the investor lent to the liquidity pool—*i.e.*, investors who invest more ultimately receive a higher percentage of the trading fees. Additionally, these LP tokens can be traded or sold. And, as an incentive to keep assets in the pool, the LP Tokens themselves can be staked back into the pool, with additional rewards received in additional tokens.

135. Critically, a non-custodial wallet, such as the Coinbase Wallet, is needed to interact with these DeFi protocols and liquidity pools.

136. In addition to lending cryptocurrencies to pools, the Coinbase Wallet also allows consumers to trade on decentralized exchanges (DEX) such as Uniswap. To trade on a DEX, consumers use the DEX feature that is built into the Coinbase Wallet. To use this feature, consumers would select the “convert” option in their Coinbase Wallet, select the coin and the amount they want to trade, and then review the transaction. The Coinbase Wallet would then display the fees associated with the conversion, as well as a network fee and a Coinbase fee.³³ If the consumer then wants to execute the trade, they will agree to pay the fees and then execute the trade through the Coinbase Wallet by selecting the convert button.

E. Security Flaws in the Coinbase Wallet Allow Scammers to Steal Consumers’ Crypto.

137. Although there are numerous legitimate liquidity mining pools, scammers have also created fake crypto liquidity mining pools to steal customers’ funds. As relevant here, the fake liquidity pools drain customers’ Wallets by relying on Coinbase’s porous security features.

138. Although individual experiences varied, most victims are contacted by scammers on social media, such as WhatsApp, Facebook, Twitter, or online dating sites. From there, the scammer

³³ The Wallet is highly lucrative for Coinbase. Customers are told that the “Coinbase Wallet charges a fee on all conversions,” meaning any exchange of one crypto-asset for another. *See supra* note 34.

induces their target, who may be unfamiliar with DeFi and crypto, to download the Coinbase Wallet. The scammers typically steer users directly to the Coinbase Wallet, as opposed to other non-custodial wallets. Once the Wallet is downloaded, the scammer then directs the victim to a fake liquidity mining pool that the user can access with their Coinbase Wallet browser. If the target already has a Coinbase Wallet, scammers direct users to the fraudulent dapp website through the Coinbase Wallet browser. The Wallet is typically funded by victims through transfers from Coinbase.com or other centralized exchanges.

139. The most important component of the scam is when the victim is told to purchase a “voucher,” “mining” or “node” certificate. This “voucher,” which is actually a malicious smart contract, gives the scammers complete access to the entire funds in the victim’s wallets *in perpetuum*. Typically, this voucher is initiated with a “receive” button, meaning that the victim believes he or she will actually receive some type of voucher or contract which will allow them to participate in a liquidity pool. But clicking on the “receive” button actually allows the scammers to electronically transfer unlimited amounts of crypto from the victim’s wallet to the wallet of their choosing at any time, even if the victim does not provide any further consents and without authorization by the Victim. The smart contract, in effect, acts as a Trojan Horse within a user’s Wallet, permitting the scammer to control and send crypto out of that Wallet without the need for *any* additional approvals or activities by the user. In effect, the smart contract grants the scammers unauthorized “approved spender” permission, which allows the smart contract to spend all the USDT in a Wallet without authorization by the Wallet owner.

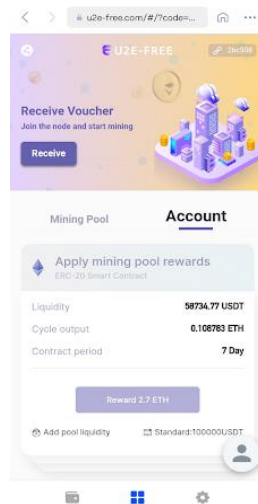


Showing 1 of 1 approved contracts found

Filter by: Filter

Txn Hash	Last Updated (UTC)	Assets	Approved Spender	Allowance
0x5d3b2697712f9b591f7...	2021-11-09 04:27:11	Tether USD	0x7e72b68d841ca...	Unlimited USDT

Revoke

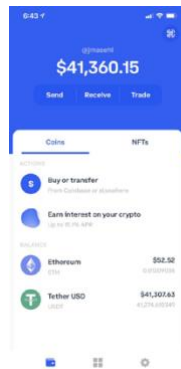


140. An analysis of the code in a malicious dapp and the Coinbase Wallet indicates that Coinbase incorporated a major flaw into the Wallet.³⁴ Effectively, the malicious dapps are created so that they, using a smart contract, request approval to spend unlimited USDT by transferring the USDT from the user's Wallet to an external address. But the dapp cannot simply take funds from a Wallet without the permission from the Wallet; rather, to do so, the spending transaction must be signed by the Wallet application, which has access to the private key stored in the user's device storage. In that regard, all transactions must have a signature "generated when the sender's private key signs the transaction and confirms the sender has authorized the transaction." Thus, when the malicious dapp interacts with the Coinbase Wallet to get approval and confirm the transaction, it is the code of the Coinbase Wallet that governs and provides permission for the spending transaction to take place. But instead of warning users that the Wallet's code is granting the dapp unlimited spend access to all the USDT in the wallet currently and all USDT added to it in the future, as the malicious dapp is asking, the Wallet provides no notification at all that this going on behind the scenes, leading users to believe that they are simply confirming a transaction to purchase a voucher. Had the Wallet simply informed users as to what the dapp was actually asking to do, instead of hiding it from the users, none of this would likely have happened.

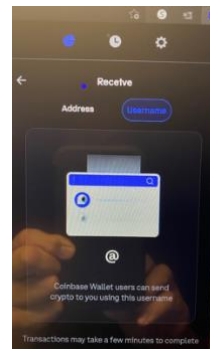
³⁴ As explained by Mr. Ich Tran at: <https://coinbase-wallet-not-secure.blogspot.com/2022/01/inside-scammers-dapp.html>

141. Once the smart contract is (unknowingly) entered into—*i.e.*, the victim has received and clicked on the voucher—the victim is then instructed to load USDT (Tether) into their Wallet. At first, most victims will load only a small amount of USDT onto their Wallets. The USDT will remain in their Wallets, although it will purportedly be pledged to the pool. Victims are typically told that the USDT will remain in their wallet throughout their participation in the mining pool. The victim’s mining pool account will then appear to be accumulating interest each day, which the victim can withdraw back into his or her wallet. This interest is meant to convince the victim that the mining pool is legitimate. Relying on that legitimacy, the victim will load more and more USDT into their Wallet. When the scammers believe that the victim will not load any additional USDT, the scammers—having already activated the smart contract “voucher” or “node” allowing unlimited access to the victim’s wallet—drain the wallet of all funds.

142. Coinbase Wallet can be accessed two ways, and these scams work with either type of access. *First*, there is a Coinbase Wallet Extension for web browsers. *Second*, there is a Coinbase Wallet smart-phone application.

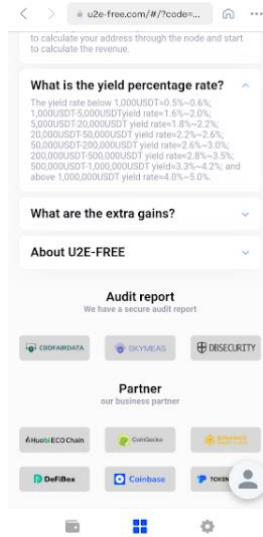


(Coinbase Application)

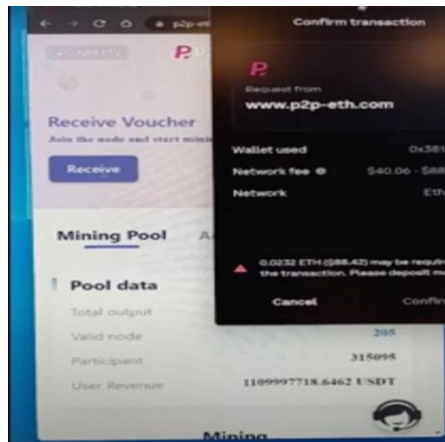


(Coinbase Browser)

143. When users of the browser extension click “receive” on the voucher or node (which surreptitiously commences the scam), the Coinbase Wallet asks the victim to “Confirm the transaction,” which is typically styled as a request from the mining pool. As shown below, the browser extension also provides the user with the wallet’s address, provides the network or gas fee, notes the Network used (Ethereum), and displays the amount of ETH required for that particular transaction (the Network Fee):



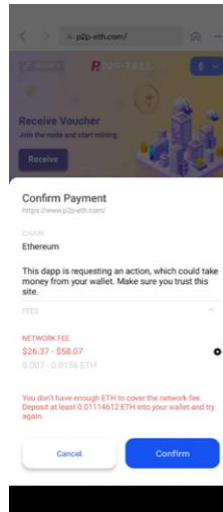
144. **At no point** does the Wallet inform the victim that he or she is giving the dapp access to the entirety of the Wallet for funds that will be deposited at a later date.³⁵ Consequently, most victims, who are using the browser extension as intended believe that they are simply confirming a transaction to purchase a voucher. They do not know that they are giving a dapp unlimited access to the USDT and future USDT deposits in their Wallet.



145. The mobile application does not remedy the issue. The mobile app does have a “Confirm Payment” button that tells the user that the “dapp is requesting an action, which could take money from your wallet. Make sure you trust this site.” The mobile app also lists the network or gas

³⁵ https://www.youtube.com/watch?time_continue=5&v=N7TySE9AdB4&feature=emb_logo.

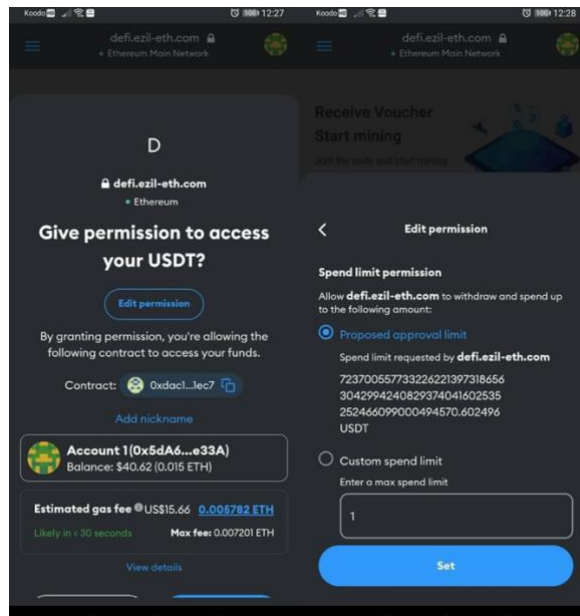
fee and states that the user must have sufficient funds to cover the network fee (usually a *de minimus* amount):



146. But those statements are woefully deficient. Most victims would understand that the “confirm payment” would be confirming payment for the voucher *at the time of the transaction*. There is no warning or other indication that the consent could permit the dapp to have unlimited access to the funds in a user’s wallet going forward. Indeed, the term “confirm payment” or “confirm transaction” necessarily indicates a single payment or single transaction. And when the user is told that the dapp is requesting “an action,” they reasonably believe that they are consenting to engage in a single “action” or purchase. Further, there is no clear notification for a user to confirm if they have or have not given their Wallet permission to engage in future transactions. Nor is there an indication of how much money the dapp is being allowed to access or of the duration of the access. Indeed, each Claimant believed that they were granting one-time access to purchase a voucher or node to join a mining pool. None of the Claimants believed that they were giving a dapp wholesale permission to access all of the funds in their wallet forever.

147. These glaring flaws are why scammers pointed victims towards Coinbase Wallet instead of other non-custodial wallets like MetaMask. Other non-custodial wallets have far more effective security features. First, when a MetaMask user purchases a voucher, the MetaMask wallet will ask the user: “Give this site permission to access your USDT?” and then re-affirms that “By granting this permission, you’re allowing this site to access your funds.” This warning indicates to the wallet owner that the dapp is not just engaging in a single transaction or payment for a voucher, but is

instead attempting to access all the USDT in a user’s wallet. Second, the MetaMask wallet has an “edit permission” button that sensibly allows the user to limit the amount of funds that can be withdrawn by the particular dapp. Third, the wallet’s “edit permissions” features tell the user how much USDT the dapp is attempting to access. As seen below, the authorized amount (“spend limit”) of USDT is an astronomical number (higher than 1,000,000,000,000⁵), which will inform the user that the dapp is most likely a scam.



148. All of the Claimants’ experiences with Coinbase Wallet largely paralleled the events outlined above. Each Claimant made attempts to report these events to Coinbase and suffered enormous damages that Coinbase could and should have prevented. As elaborated below, moreover, Coinbase’s customer service—in response to Claimants’ requests for help after these devastating and preventable scams—was woefully deficient.

F. Coinbase’s Outsourced Customer Service Provided an Incompetent Response to the Liquidity Pool Scams, Thereby Allowing the Scams to Continue for Many Months After They Became Known, Resulting in Millions of Dollars in Preventable Losses to Many Users.

149. Coinbase was first alerted to the security flaws in its Wallet in approximately October 2021. But Coinbase failed to take any remedial action. In fact, Coinbase customer service did not even

recognize the problem. Coinbase even published so-called “security” videos about risks to the Wallet without even mentioning the liquidity pool scams, even though Coinbase had been warned about the scams months earlier.³⁶

150. In fact, Coinbase did nothing until March 24, 2022—approximately *six months* later—when it posted a “Security PSA” related to “security threats” that were purportedly “not only to Coinbase but to the crypto ecosystem as a whole.”³⁷ The PSA stated that “recently,” Coinbase “security teams have uncovered ongoing mining pools scams targeting users of self-custody wallets.” Coinbase estimated that these scams “have resulted in the theft of over \$50 million in crypto assets from a variety of non-custodial wallet applications.” Despite the fact that the scammers directed consumers to use Coinbase Wallet, Coinbase claimed that “[t]hese scams target those using any decentralized wallet browser (e.g., Coinbase Wallet, Metamask, Trust, etc.)” Coinbase’s “PSA” did contain an important admission, however. Coinbase stated, in explaining the scam, that “Victims are contacted via social media and/or other messaging services by scammers claiming to offer an attractive crypto investment opportunity *to stake USDT (Tether) in their wallet* for a guaranteed return.” Thus, Coinbase recognizes that the victims of these scams did not expect the crypto to ever leave their wallet, thereby conceding that the transfers were “unauthorized” for the purposes of liability under EFTA.

151. Thus, with at least six months of direct knowledge of Coinbase’s failures vis-à-vis these scams, Coinbase attempted to deflect from its own culpability. In addition to falsely framing its own failures as a problem with all decentralized wallets, Coinbase lied to consumers about having “recently” discovered the “security threats,” even though the problems had been brought to Coinbase’s attention more than six months earlier. Making matters worse, given that Coinbase, once apprised of this potential lawsuit, quickly installed warnings on many of the dapp websites, it is apparent that Coinbase could have easily prevented many of the thefts at issue here (in fact, customers repeatedly gave the scam site URLs to Coinbase), but instead chose not to protect their users.

³⁶ See supra note 7.

³⁷ See Coinbase, *Security PSA: Mining Pool Scams Targeting Self-Custody Wallets*, <https://blog.coinbase.com/security-psa-mining-pool-scams-targeting-self-custody-wallets-543ffe698724>, last accessed on October 7, 2022.

152. When Claimants and other Coinbase Wallet users saw that their funds had been stolen, typically, their first step was to contact Coinbase for help. Coinbase, however, did not offer live customer support, and customers typically had to either call, send an email to support@coinbase.com or fill out a form in the Coinbase Help Center. Given the superficial and often nonsensical responses Coinbase repeatedly provided to its defrauded customers, Coinbase appeared to use automated “bots” to respond to customer complaints—even complaints that Coinbase’s securities flaws had triggered the loss of life-changing sums.

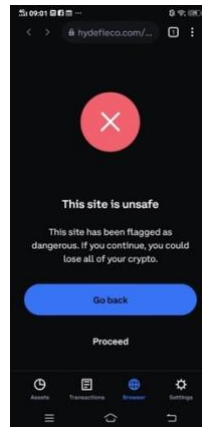
153. Making matters worse, Coinbase’s failure to invest in competent and responsive customer service appears to be a calculated decision that Coinbase intentionally undertook to rapidly grow the company. As Coinbase admitted to investors in its 2022 Q1 Form 10-Q filed with the SEC on May 10, 2022, Coinbase’s outsourced “customer service” would result in “increased operational risks” for Coinbase. Coinbase then deliberately chose to go ahead with this form of customer service in order to increase its customers, thereby putting profit over security.

“We rely on third parties in connection with many aspects of our business, including payment processors, banks, and payment gateways to process transactions; cloud computing services and data centers that provide facilities, infrastructure, website functionality and access, components, and services, including databases and data center facilities and cloud computing; as well as **third parties that provide outsourced customer service**, compliance support and product development functions, which are critical to our operations. **Because we rely on third parties to provide these services and to facilitate certain of our business activities, we face increased operational risks.** We do not directly manage the operation of any of these third parties, including their data center facilities that we use.”³⁸

154. The results of Coinbase’s calculated business decision, designed to increase customers without the ability to adequately supervise, assist, and integrate those customers, were catastrophic.

³⁸ See SEC, 2022 10-Q Coinbase Global, Inc., March 31, 2022, <https://web.archive.org/web/20220512124440/https://d18rn0p25nwr6d.cloudfront.net/CIK-0001679788/89c60d81-41a2-4a3c-86fb-b4067ab1016c.pdf>, p. 80, last accessed on October 7, 2022. These same warnings, after months of complaints to Coinbase’s customer service about the security flaws in the Coinbase Wallet, were included in Coinbase’s 2021 10-K annual report, filed on February 25, 2022.

155. Finally, many of these thefts were easily preventable had Coinbase bothered to employ even a minimally competent customer service team. In that regard, after counsel for Claimants in this action sent a draft complaint to Coinbase in late July 2022, Coinbase took immediate action. Coinbase was able to post warnings, such as the one above, on many of the scammer dapps. This simple warning, had it been posted earlier (which it easily could have given that customers were telling Coinbase how their crypto had been stolen), would have prevented many of the thefts at issue here from occurring.



Example 1: November 2021 (Ich Tran)

156. One user's interaction with Coinbase, Claimant Ich Tran, as set forth in a public blog entry detailed below, is typical of Coinbase's woefully insufficient responses, which failed to acknowledge the major security issues present in Coinbase Wallet.³⁹ In fact, Coinbase's responses appear to be generic, computer-generated messages that Coinbase created, and which falsely blame users for the loss of their seed security phrases, which did not happen. In short, Coinbase asks users to entrust significant financial assets to Coinbase's custody and software, but Coinbase refuses to even provide minimal customer service to enable customers to retain their assets and protect themselves from scammers.

157. Tran first wrote to Coinbase on approximately November 18, 2021, explaining that all his money, nearly \$60,000 USDT, was transferred out of his Wallet without his permission that same day. Tran provided an etherscan link to the transaction. Tran explained that he had never shared his

³⁹ See *DApp Phishing Scam in Coinbase Wallet*, December 23, 2021, <https://coinbase-wallet-not-secure.blogspot.com/2021/12/my-experience-contacting-coinbase.html>.

“Recovery Phase” with anyone, and he asked how a “dApp can take all my money without my permission?” He even provided Coinbase with a URL link to the dapp – u2e-free.com.

158. Coinbase provided a generic response, stating: “If you did not authorize any outgoing transactions from your Coinbase Wallet, it means that your recovery phrase has been compromised.” The response went on to state that: “Because your Coinbase Wallet is a user-controlled and non-custodial product, which means that only you have full control/access to your wallet (including the recovery phrase), we cannot provide any further details about how it was compromised nor can we help recover funds.” Coinbase explained that the transaction could neither be cancelled or reversed, and recommended that the user create a “new Coinbase Wallet” to hold any remaining funds.

159. Tran responded shortly thereafter (November 18, 2021 at 9:46 p.m.), “So you cannot help answer whether a dApp in Coinbase Wallet can take my recovery phrase somehow?” Tran warned: “It might be a security issue in the Coinbase Wallet app.” To this, Tran received another generic email stating “Coinbase Wallet is a user-controlled and non-custodial product which means that you-and only you-have access to your seed phrase and the ability to move your funds.” Coinbase remarked, “Coinbase will never have access to you or to any of our customers’ seed phrases. For this reason, we cannot help recover any Coinbase Wallet or transfer funds on your behalf. We understand that this may cause some difficulty, but we cannot reimburse or credit your Coinbase Wallet whether you lose access or not.”

160. Tran responded to Coinbase’s reply with a series of screenshots documenting the unauthorized transactions, and Tran explained that he was “really confident that I am keeping the Recovery Phrase safe.” Tran again warned Coinbase about the dapp, and also, again, stated “I believe that there is a security vulnerability in the Coinbase Wallet app where that dApp exploited and gained access to our wallets to take money from us.” Tran asked the Coinbase representative to escalate the issue. No effective response was received from Coinbase.

161. On November 20, 2021, Tran wrote to Coinbase again, stating that he was “not satisfied with [Coinbase’s] response because it did not help me. I have not heard of any other response so I would believe that you have closed the case.” Tran told Coinbase that he was “planning to publish” what he “found to help other users from getting their Wallet drained even though their recovery phrase

is not compromised.” Once again, Coinbase provided a generic robotic response, stating that “Coinbase Wallet is a user-controlled and non-custodial product which means that you-and only you-have access to your seed phrase and the ability to move your funds. Coinbase will never have access to you or any of our customers’ seed phrases. For this reason, we cannot help recover any Coinbase Wallet or transfer funds on your behalf. We understand that this may cause some difficulty, but we cannot reimburse or credit your Coinbase Wallet whether you lose access or not.”

162. This pattern continued. On November 25, 2021, Coinbase, yet again, wrote to Tran: “If you did not authorize any outgoing transactions from your Coinbase Wallet, it means that your recovery phrase has been compromised.”

163. On February 3, 2022, Tran filed a formal complaint with Coinbase regarding the theft of the crypto from his wallet (#10048013), which he had repeatedly told Coinbase had not occurred due to a compromise of his “12 word recovery phrase.” Despite this, Coinbase, yet again wrote to Tran: "Coinbase Wallet is a user-controlled, non-custodial product, this means that the 12 word recovery phrase gives you, and only you, access to recover your account. According to the Coinbase Wallet Terms of Service, the user is "solely responsible for the retention and security of [their] twelve word recovery phrase" and Coinbase "does not store and is not responsible in any way for the security of [their] Recovery Phrase".

164. In addition, the scam dapp that Tran used was still up and running weeks after it was reported to Coinbase.

Example 2: April 2022

165. A second example is from a Wallet User (User 1) who had approximately \$92,000 stolen from him through the liquidity mining scam on or about April 12, 2022. Two days earlier, User 1 had asked Coinbase customer support to confirm the security of a dapp liquidity mining pool. User 1 asked if the network was “legitimate.” Coinbase customer service responded that User 1 should do his own research to “understand how these apps work and what the risks are. And remember that Coinbase does not control these decentralized apps.” To this, User 1 asked whether the liquidity pool would be “able to have any access to my funding deposited in my wallet? (How secure the funding in my wallet is?)”. Coinbase responded that User 1 created a 12-word seed phrase when he created his

wallet; and that “no third party or even Coinbase could have access to the funds in your wallet account. Because your wallet is user-controlled and non-custodial product, meaning that only you have full control/access.”

166. Two days later, User 1’s wallet was drained of all USDT in a transaction that User 1 did not authorize. User 1 wrote back to Coinbase noting that Coinbase had just said that “as long as I secured my seed, my wallet would be safe. I am certain that I have not exposed my 12-word recovery phrase to any third parties. That being said, I believe this is a security issue with the Coinbase wallet where someone was able to breach my account, as I have other standalone wallets, like MetaMask, and this issue is not occurring with those.” To this, Coinbase responded that “Coinbase Wallet is a user-controlled and non-custodial product which means that you – and only you – have access to your seed phrase and the ability to move your funds.” Because of this, Coinbase could not “help recover any Coinbase Wallet or transfer funds on your behalf.”

167. User 1, however, remained adamant that his “seed was not exposed to any third parties.” User 1 noted that the issue “has also happened to my friends and many other Coinbase users, who were also joined in this network through dapp of the Coinbase wallet. It is impossible that all of our seeds were exposed at the same time.” User 1 explained that the “security issue” with the Wallet most likely arose through the “initial transaction” where User 1 paid “\$9.15” to join the pool. User 1 explained that this was “clearly a security bug of the Coinbase wallet and is unrelated to the seed exposure.” User 1 further noted that there was another similar scam project that he was aware of, and “it can be opened both via Metamask and Coinbase wallet. But it won’t give any gains on the Metamask wallet, and only works with the Coinbase wallet. Taking all this into account, we are certain that there is a security bug in the Coinbase wallet that needs to be resolved as soon as possible.”

168. Later that day (April 12, 2022), Coinbase wrote back and acknowledged that User 1’s “seed phrase was not compromised.” Coinbase noted that the: “unauthorized activity you reported appears to have resulted from a signed transaction that approved a malicious third party to transfer funds from your Wallet on Mar-24-2022 09:50:16 PM.” However, Coinbase wrote: “Please note Coinbase Wallet and Standalone Wallet Extension are user-controlled and non-custodial products. At no point has Coinbase ever had access to your Wallet or the funds held inside. It’s the customer’s

responsibility to review the details of the dapp they interact with and understand the risk when interacting with it.”

169. User 1 responded with one final email:

Thanks for your email. You should know that I was suspicious about smart contract safety from days before this fraud happened. I even contacted Coinbase support days before the unauthorized transaction regarding my safety concerns. In the email, the Coinbase support team confirmed that the only way anyone can have access to my wallet is only through the seed password, which turned out to be misleading and false information. Coinbase support must have let me know of the threat when I provided the information and inquired about the safety of the smart contract known as Defi-USDT. Now that I have lost the funds, it is too late to inform me that I had to revoke this access hidden underneath a totally normal-looking transaction. This access was completely hidden, and was granted without my consent or knowledge. There were no alert notifications from the Coinbase wallet of such an obvious threat. I have attached a screenshot of my correspondence with Coinbase support as a reference. With all these known, I demand a meeting with a person from Coinbase that can resolve my issue immediately. I don't think an email thread would serve the purpose. It is a serious matter, and I have enough information and pieces of evidence showing that Coinbase is already aware of this nationwide scam, still not trying to eliminate this security bug nor accepting the responsibility for that.

170. Thus, although Coinbase was made well-aware of the scam and the security issues with its Wallet beginning in at least October 2021 by dozens if not hundreds of people, Coinbase did nothing to fix the security problem or even warn users about the scams. No warnings took place for approximately six months, and even then, Coinbase attempted to pass this off as a widespread crypto wallet problem, rather than a problem specific to the Coinbase Wallet. Instead, Coinbase's incompetent customer service provided generic responses to customers' important queries. These responses, provided in an endless loop of automated and unhelpful emails, stated only that Coinbase was denying fault and liability and told Claimants that Coinbase could not cancel or reverse the transactions. Due to Coinbase's incompetence and unprepared customer service, who could not even escalate a major security flaw to Coinbase's developers, dozens, if not hundreds, of additional people lost millions of dollars. Some of these people had their entire life savings wiped out in catastrophic thefts.

171. In spite of this, at approximately the same time as User 1 had all his funds stolen from him due to the Wallet’s security flaws, Coinbase Wallet’s Twitter account, on April 6, 2022, published a self-aggrandizing Tweet (falsely) touting the Wallet’s security:



172. The experiences of Tran and Users 1 exemplify the deficient responses of Coinbase’s customer service in response to reports made by Claimants and other Coinbase Wallet users in their attempts to receive meaningful assistance from Coinbase following the devastating realization that they were victims of a financial scam facilitated on Coinbase’s platform.

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

173. A detailed account of each Claimant’s respective experience as a victim of 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.⁴⁰

a. Ihab William Francis

174. On or about September 18, 2021, Claimant Ihab William Francis (“Francis”) was contacted by an individual on LinkedIn who described himself as a cryptocurrency investor offering to explain to Francis how he had successfully made money in the cryptocurrency market. The individual offered Francis a “time-limited opportunity” to earn interest in an investment mining pool

⁴⁰ Because there are so many Victims included in this Arbitration Demand, the narratives are abbreviated.

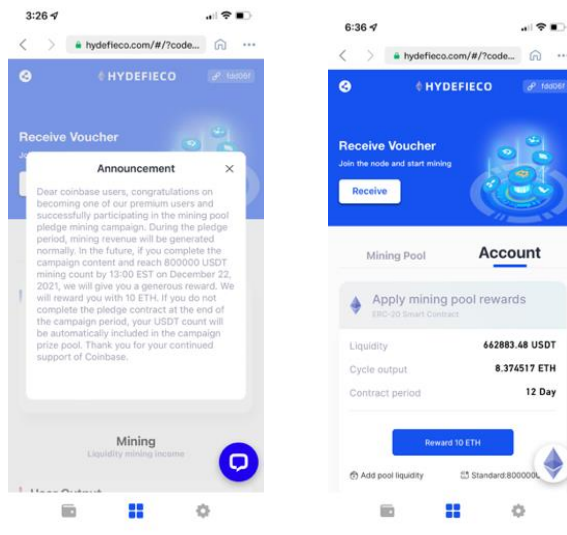
through a cryptocurrency transaction on Coinbase using a DeFi platform called “HYDEFIECO.com.” The individual told Francis that Coinbase was “the most trusted cryptocurrency application out there” and then directed him to create a Coinbase Wallet account to complete the transaction. Francis downloaded the Coinbase Wallet application and opened the link for HYDEFIECO.com using the Wallet’s browser as instructed believing that the exchange was a legitimate transaction involving crypto assets held in his Coinbase Wallet. Unbeknownst to Francis, this individual was a defrauder seeking to lure Francis into a fraudulent exchange on the Coinbase platform.

175. As part of the fraudulent pool scheme, Francis was directed to “join the node” and receive a voucher to join the HYDEFIECO liquidity mining pool. Francis did as he was instructed.

176. After joining the pool through the Coinbase platform, Francis made small transfers to the pool from his Coinbase Wallet on November 3 and 8. The initial contributions appeared to be yielding interest in accordance with Francis’s understanding of the liquidity mining pool so he continued to make contributions.

177. Francis made 12 deposits of USDT into his Coinbase Wallet between on November 3, 2021 and January 10, 2022 into the fraudulent liquidity pool. On or about November 10, 2021, Francis was fraudulently induced to enter into a smart contract with the aforementioned defrauder which resulted in the theft of the entirety of Francis’s assets held in his Coinbase Wallet.

178. Weeks later Francis was offered an opportunity for “premium users” to participate in a “mining pool pledge campaign,” purportedly offered by Coinbase itself. The scammer told Francis



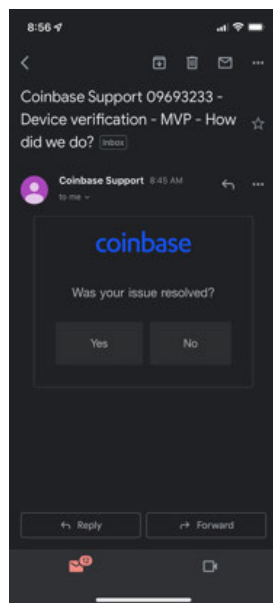
that he had a contact who worked for Coinbase who had given Francis access to the campaign. Francis was sent the following notification through Coinbase Wallet:

179. Francis never provided the defrauder with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

180. Francis never believed—and had no reason to believe—that he had allowed the defrauder or anyone else access to the assets held in his Wallet. Indeed, Coinbase Wallet provided no warning to Francis stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures instructed Francis that the *only* way someone could take his funds was if his “seed phrase” was stolen or compromised.

181. The losses incurred by Francis as a result of the Coinbase Wallet liquidity pooling scheme total \$662,883.48, comprising of assets that Francis had withdrawn from his 401K, Roth IRAs, and family’s personal savings accounts. The fraudulent withdrawal left Francis without any savings or retirement funds and in debt for around \$50,000.00, leaving he and his family in financial ruin.

182. Following the theft, Francis reported the fraudulent withdrawal to Coinbase customer support (Case No. #09693233). Francis’s contact with Coinbase’s customer support was worthless. Francis received an automated, generic response from Coinbase Wallet’s customer service platform that did not address the fraud and instead prompted Francis to undergo various verifications of his



Wallet account. Coinbase denied responsibility for any unauthorized withdrawal and failed to address Francis’s complaint or investigate the reported theft, leaving Francis with no recourse to remedy the fraudulent withdrawal. This loss resulted in significant emotional distress to Francis. Coinbase did not even block the malicious dapp on their platform.

b. Shakeeb Khan

183. On or about January 17, 2022, Claimant Shakeeb Khan (“Khan”) was contacted by an individual on WeChat, a social media messaging platform, who invited Khan to join a liquidity mining pool on Coinbase.

184. On January 18, 2022, Khan was directed to by this individual to create a Coinbase Wallet account and enter into a smart contract through a node or voucher on a dapp exchange called “BIPAI” on Coinbase’s platform in order to join the liquidity mining pool. Khan did as he was instructed. Unbeknownst to Khan, this individual was seeking to lure Khan into a fraudulent exchange on the Coinbase platform.

185. Khan subsequently made 21 deposits of USDT into his Coinbase Wallet between on January 18, 2022 and February 7, 2022 to fund the pool.

186. On or about February 7, 2022, in an unauthorized transaction, the defrauder drained Khan’s entire Coinbase Wallet of all of his crypto assets by way of the fraudulent smart contract.

187. Following the unauthorized withdrawal, Khan contacted the individual who had invited him to join the mining pool. The individual assured Khan that his funds had not been “stolen” but were moved to a “mining pool” and could be retrieved after he deposited more USDT into his Wallet.

188. At this point, Khan realized that he was the victim of a fraudulent scam and would need to seek

189. Khan never provided the defrauder with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

190. Khan never believed—and had no reason to believe—that he had allowed the defrauder or anyone else access to the assets held in his Wallet. Indeed, Coinbase Wallet provided no warning to Khan stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase

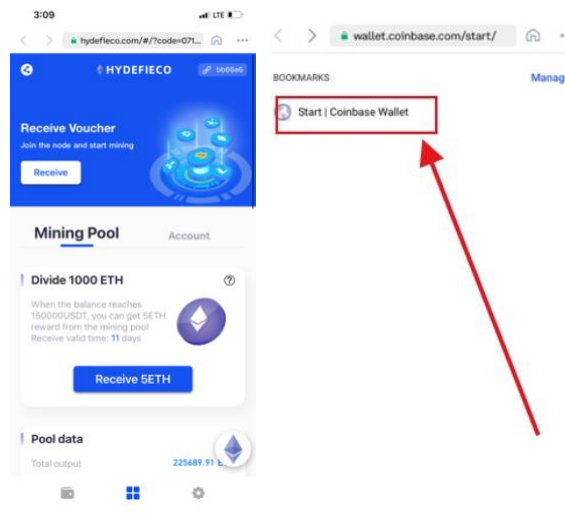
Wallet’s disclosures instructed Khan that the **only** way someone could take his funds was if his “seed phrase” was stolen or compromised.

191. Khan’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$58,000.00, comprising of assets withdrawn from Khan’s personal savings accounts. The fraudulent withdrawal left Khan in a significant savings deficit, which resulted in significant emotional distress to Khan.

192. Following the fraudulent withdrawal, Khan contacted Coinbase customer service to report his stolen assets by phone (Case No. #13052680). On September 14, 2022, Coinbase responded to Khan informing him that it “flagged the malicious web3site [sic] to [its] security and investigation teams” but there was no way for Coinbase to recover his funds. Coinbase provided Khan with a list of third-party applications through which he could try to investigate or revoke the fraudulent transactions, but made no effort of its own to assist Khan’s recovery of his stolen funds. Coinbase denied any responsibility for the loss, stating that “Coinbase plays no role in transactions authorized and signed by the user” and advised Khan to file a report with the FBI.

c. Autumn Pavao

193. On or about January 3, 2022, Claimant Autumn Pavao (“Pavao”) was contacted by an individual named “Sophie” through WhatsApp, a social media messaging platform, who had previously introduced Pavao’s mother and uncle to a liquidity mining pool under the guise of making large returns on crypto investments using a DeFi platform called “HYDEFIECO.com.” Sophie

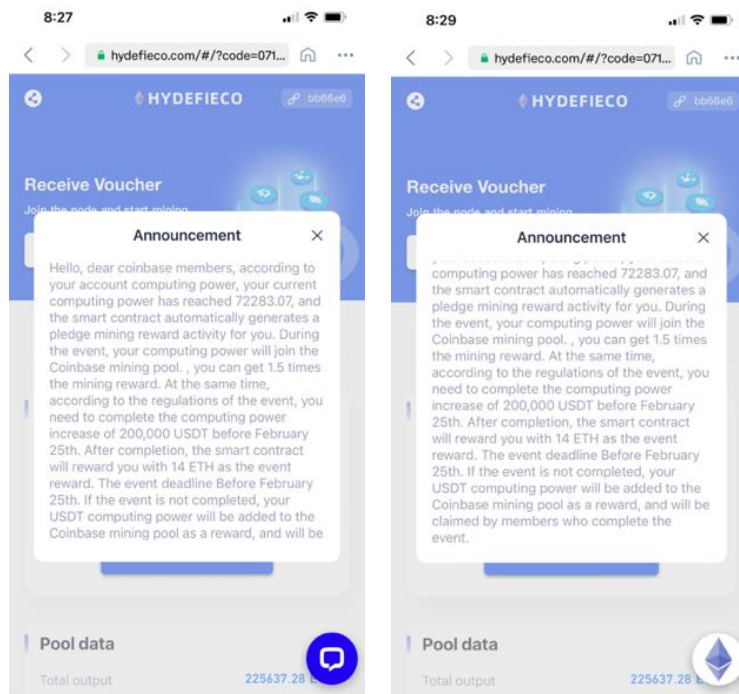


directed Pavao to create a Coinbase Wallet account and transfer money into her Coinbase Wallet to start investing in the pool.

194. On January 3, 2022, Pavao entered into a smart contract through a node or voucher to join the liquidity mining pool.

195. Pavao deposited \$65,000.00 USDT into her Coinbase Wallet account based on Sophie's instruction to fund the pool. Between January 4, 2022 and January 21, 2022, Pavao made three subsequent deposits into her Coinbase Wallet.

196. On February 6, 2022, Pavao's entire Coinbase Wallet was drained by the dapp without her consent. She received the following message from HYDEFIECO on her Coinbase homepage, informing her that the entirety of her crypto wallet had been "pledged" to the pool and would be distributed to other members of the pool unless she deposited \$200,000 USDT to the pool by February 25, 2022. This withdrawal was done without Claimant's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.



197. On or about February 6, 2022, the wallets of Pavao's mother and uncle were also drained. Pavao's mother who had entrusted Coinbase to securely hold her life's saving, lost over a quarter million dollars due to the scheme. Pavao contacted Sophie after the fraudulent withdrawal and

was told that the withdrawal was “a new activity launched by coinbase” and that she would have to “complete the reward activity” or all her assets would be given to individuals who complete the activity. Sophie reminded Pavao that she agreed to the smart contract, and “[o]nce a smart contract is formed, it cannot be changed.” In the wake of Pavao’s distress, Sophie tried to convince her to borrow more money from family members to meet the \$200,000 “activity” for her and her mother.

198. Pavao never provided Sophie or any third party with her security passphrase and did not receive a notification from Coinbase Wallet to confirm that she had agreed to release the entirety of her assets from her Wallet by entering the smart contract.

199. Coinbase Wallet never provided any warning to Pavao that anyone could access her Wallet to take her funds without her express consent or authorization. To the contrary, Coinbase Wallet’s disclosures instructed Pavao that the *only* way someone could access her funds was if she provided her security pass phrase or it was stolen or compromised.

200. Pavao’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$72,283 USDT, comprising of Pavao’s personal savings, and the funds she had recently acquired from the sale of her home.

201. The fraudulent withdrawal left Pavao in financial precarity and, resulted in significant emotional distress to Pavao as she witnessed three of her family members also fall victim to this fraudulent scheme on Coinbase’s platform.

202. Hours after the fraudulent withdrawals occurred on February 6, 2022, Pavao contacted Coinbase to notify it of the theft and to get guidance on how to address the issue (Case Nos. #10124196, #10567387, #10809240, # 11108657). Pavao’s contact with Coinbase’s customer support was entirely unhelpful.

203. Coinbase responded with a generic automated message that informed Pavao of Coinbase’s security passphrase protocol, informed her that Coinbase “cannot help recover any Coinbase Wallet or transfer funds on [her] behalf.” In subsequent correspondence, Coinbase told Pavao that it was her responsibility to “understand the risk when interacting with [dapps]” and it would not “reimburse or credit [her] wallet” for losses incurred due to fraudulent activity on its platform.

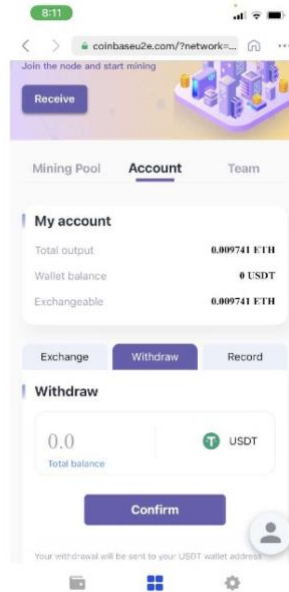
Further, despite providing Coinbase with the name of the scam dApp, Coinbase did nothing to take the dapp down or block it, potentially subjecting many others to their loss.

204. From February 6, 2022 until March 14, 2022, Pavao attempted to get assistance from Coinbase Support team to address her loss and to stop the defrauder from preying on other Coinbase customers. Coinbase continued to reply to Pavao with unresponsive automated messages and told Pavao that it had “flagged” the dapp to its security and investigation teams. Days later, on March 7 and 8, Pavao informed Coinbase that the dapp was still operational and continued to make numerous withdrawals through the Coinbase platform. Coinbase did not respond to Pavao’s email and instead notified her on March 14 that it was “closing” Pavao’s case, although it never conducted an investigation into Pavao’s allegation or provided any recourse for Pavao to retrieve her stolen funds, other than filing a report with the FBI.



d. Johannes Masehi

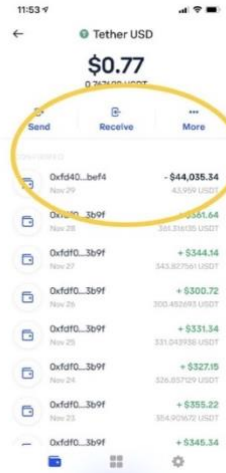
205. On or about August 12, 2021, Claimant Johannes Masehi (“Masehi”) was contacted by an individual on Facebook Messenger and WhatsApp with an invitation to join a liquidity mining pool on Coinbase. Masehi was directed to create a Coinbase Wallet account and deposit funds into the Wallet to begin investing on a dapp called U2E-Free.com on Coinbase’s platform.



206. On November 4, 2021, Masehi was directed to entered into a smart contract through a node or voucher in order to join the liquidity mining pool. Masehi did as he was instructed and deposited approximately \$40,000.00 into his Coinbase Wallet account. Unbeknownst to Masehi, this individual was a defrauder seeking to lure him into a fraudulent exchange on the Coinbase platform.

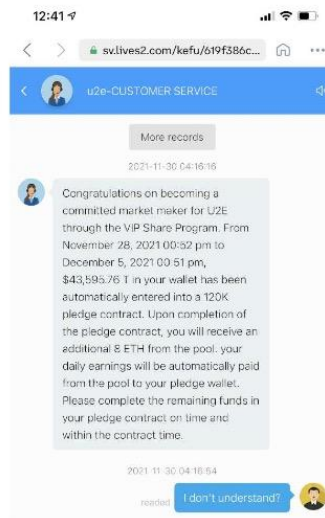
207. Masehi subsequently made 2 additional deposits of USDT into his Coinbase Wallet between November 12 and November 18, 2021 to fund the pool.

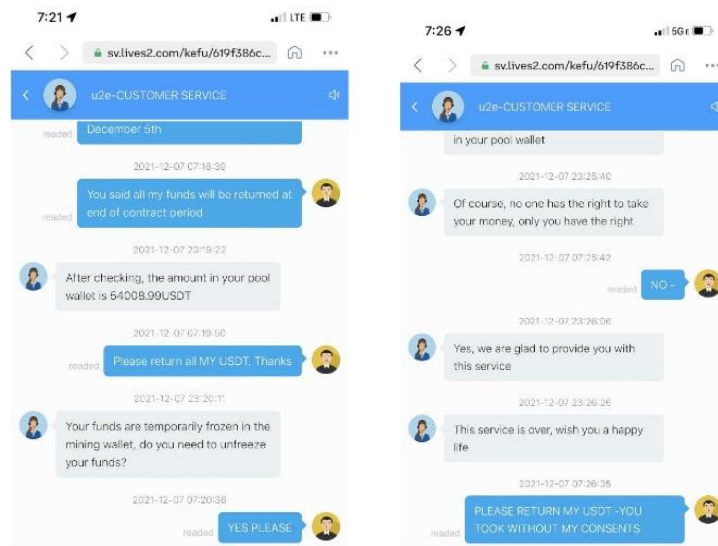
208. On November 29, 2021, the defrauder drained Masehi’s entire Coinbase Wallet of all of his crypto assets by way of the fraudulent smart contract in a transaction that he did not authorize.



209. On November 30, 2021, after the funds were fraudulently withdrawn, Masehi received the following message through Coinbase from U2E-Free, informing him that his Wallet was entered into a “120k pledge contract” requiring him to deposit more funds into the pool to retrieve his assets.

210. On December 5, 2021, Masehi requested that U2E-Free return the stolen funds. U2E-Free informed him that he would have to add 76,000 USDT to the pool to retrieve his assets, despite the fact that Masehi had never pledged the stolen funds to the pool. An individual acting on behalf of U2E-Free later requested that Masehi deposit 16,000 USDT to the pool in order to “unfreeze” his account, otherwise, the entirety of the assets in his Coinbase Wallet would be lost indefinitely.





211. Masehi never provided the defrauder with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

212. Coinbase Wallet provided no warning to Masehi stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures instructed Masehi that the **only** way someone could take his funds was if his “seed phrase” was stolen or compromised.

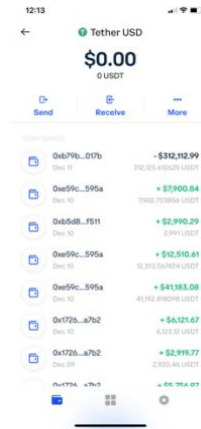
213. Masehi’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$43,959 USDT.

214. In addition to his grave financial loss, Masehi suffered significant emotional distress as a result of the Coinbase liquidity mining pooling scam.

215. When Masehi reported the fraudulent withdrawal to Coinbase (Case Nos. #08964690, #10599025), he received automated, generic responses from Coinbase Wallet’s customer service stating that Coinbase could not do anything to address the fraud or reimburse Masehi. Coinbase’s customer support was entirely unhelpful. Coinbase failed to address Masehi’s complaint or investigate the theft, or even block or flag the malicious dapp, leaving him with no recourse to remedy the fraudulent withdrawal.

e. Leonard Waki

216. On or about December 2, 2021, Claimant Leonard Waki (“Waki”) was introduced by a friend to an individual named QianEn on WeChat who extended an invitation to Waki to join a liquidity mining pool on Coinbase aimed at mining USDT into Ethereum. Waki was directed by



QianEn to download Coinbase Wallet and create an account and deposit funds into the Wallet to begin investing in the pool through a dapp called “Coinbase DeFi 2.0” (<https://defi.ethereum-usd.vip/#/>)

217. Waki was directed by QianEn to click on a “mining certificate” in order to enter the mining pool and receive awards. Waki complied with this request on November 30, 2021. Unbeknownst to Waki, the “mining certificate” he agreed to was actually a malicious smart contract that gave scammers access to the contents of his Coinbase Wallet without his security passphrase.

218. On December 1, 2021, Waki made an initial deposit of \$473.67 USDT into his Coinbase Wallet. Between December 1, 2021 and December 10, 2021 Waki made 33 deposits towards the funding of the liquidity pool.

219. On December 11 2021, Waki became aware that his entire Coinbase Wallet had been emptied of all of his crypto assets by way of the fraudulent smart contract.

220. Waki never provided the defrauder with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

221. Coinbase Wallet provided no warning to Waki stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures instructed Waki that the *only* way someone could take his funds was if his “seed phrase” was stolen or compromised.

222. Waki’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$313,112.99 (\$312,325.61 USDT).

223. In addition to his grave financial loss, Waki suffered significant emotional distress as a result of the Coinbase liquidity mining pooling scam which has greatly impacted his life.

224. Waki immediately reported the fraudulent withdrawal to Coinbase on December 11, 2021 (Case No. #09019652), but he received an automated, generic response from Coinbase Wallet’s customer service stating that Waki’s “recovery phrase has been compromised” but that Coinbase could not “provide any further details about how it was compromised nor can [Coinbase] help recover these funds.”

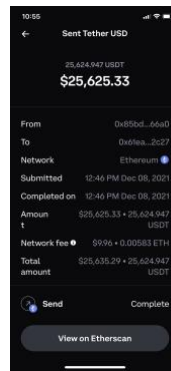
225. On December 12, 2021, Waki filed a complaint with the Internet Crime Complaint Center of the Federal Bureau of Investigation. On January 26, 2022, Waki filed a complaint with the Consumer Financial Protection Bureau. On January 28, 2022, Waki filed a formal complaint with Coinbase regarding the fraudulent withdrawal. On February 10, 2022 Coinbase responded to Waki indicating that it was closing his complaint file because he filed a complaint with Consumer Financial Protection Bureau. Coinbase failed to address Waki’s complaint or investigate the theft, leaving him with no recourse to remedy the fraudulent withdrawal.

f. Jon Leathers

226. On or about December 1, 2021, Claimant Jon Leathers (“Leathers”) was contacted by an individual named Aimee on a social media dating app who extended an invitation to Leathers to join a liquidity mining pool on Coinbase. Leathers was directed by Aimee to download Coinbase Wallet and create an account and deposit funds into the Wallet to begin investing in the pool through a dapp on the Coinbase platform called ETH-Flow cell (<https://eth-flowcell.cc/#/>).

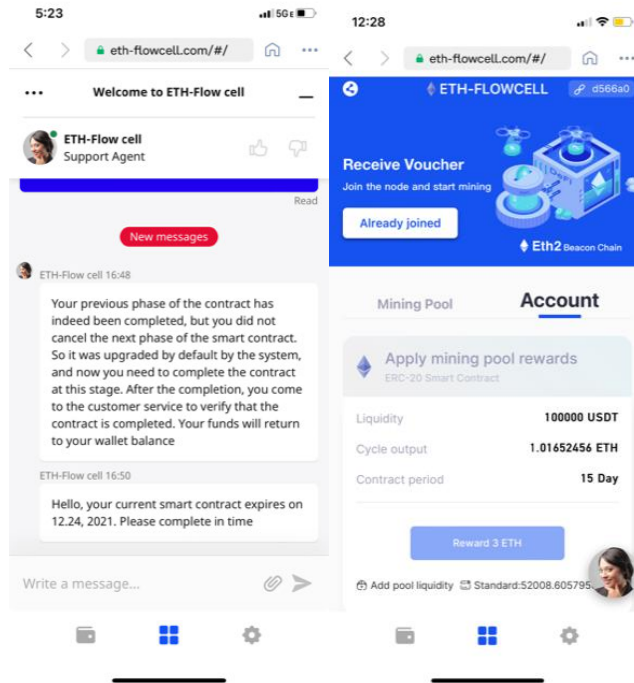
227. Leathers was directed by Aimee to access the dapp using his Coinbase account and “join the node” in order to enter the mining pool and receive awards. Leathers complied with this request on December 8, 2021 and made an initial deposit to his Coinbase Wallet to fund the pool. Unbeknownst to Leathers, he had actually entered into malicious smart contract that gave defrauders on the platform access to his entire Coinbase Wallet without his consent or security passphrase.

228. On December 8, 2021, approximately \$25,625.33 USD was removed from Leather’s Coinbase Wallet. Leathers believed that he still had access to his assets and all of his assets would be returned to his Coinbase Wallet after the end of his contract term.



229. On December 13, 2021, Leathers made one subsequent deposit into his Coinbase Wallet in order to fund the liquidity pool.

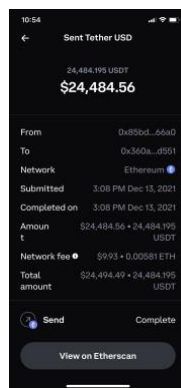
230. Later in the day on December 13, 2021, defrauders emptied Leather’s entire Coinbase Wallet of all of his crypto assets by way of the fraudulent smart contract. Leathers received the following message from ETH-Flow cell’s customer service informing him that it “upgraded [his smart contract] by default” and once he deposited \$100,000 USDT, he could withdraw his funds.



231. Leathers never provided Aimee or anyone else with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

232. Coinbase Wallet provided no warning to Leathers stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures instructed Leathers that the *only* way someone could take his funds was if his “seed phrase” was stolen or compromised.

233. Leather’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$54,000.00 (\$52008.60 USDT), comprised of funds withdrawn from his personal savings. In addition to the financial impact, Leathers suffered significant emotional and mental anguish as a result of the fraudulent scheme.



234. Leathers made multiple attempts to report the fraudulent withdrawals to Coinbase by phone and email through Coinbase’s customer service platform and filed a formal complaint with Coinbase on December 16, 2021. Coinbase’s customer support was entirely unhelpful. Further, Leathers provided Coinbase with the name of the malicious dapp, eth-flowcell, so that other people would not be harmed by the dapp. Nonetheless, months later, the dapp was still active.

235. On January 24, 2022, Coinbase replied to Leathers, informing him that it had no further response to his complaint beyond the automated, generic responses it had previously provided which stated that Coinbase could not do anything to address the fraud or reimburse him.

g. Lawrence Bateman

236. On or about November 24, 2021, Claimant Lawrence Bateman (“Bateman”) was introduced to a Coinbase liquidity mining pool opportunity through a close friend. Bateman created a Coinbase Wallet account and access the liquidity mining pool through a dapp called <https://defi.usdt-defi2.org/#/> on Coinbase’s platform. On or about November 24, 201, Bateman entered into a smart contract disguised as a node or voucher which gave defrauders access to Bateman’s entire Coinbase Wallet.

237. Between November 24, 2021 and December 10, 2021, Bateman made 8 deposits of USDT into this Coinbase Wallet to fund the pool.

238. On December 10, 2021, after Bateman had contributed over \$100,000 USDT to the pool, defrauders drained all the funds in his Coinbase Wallet without his consent or security passphrase.

239. Bateman never provided anyone else with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

240. Coinbase Wallet provided no warning to Bateman stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet's disclosures instructed Leathers that the *only* way someone could take his funds was if his "seed phrase" was stolen or compromised.

241. As a result of the Coinbase Wallet liquidity pooling scheme, Bateman lost total \$104,088.00 USD (\$104,046.86 USDT). These funds consisted of Bateman's entire life savings. Bateman had to take out credit cards to make ends meet and had to borrow money from relatives to afford his living expenses.



242. In addition to the financial distress caused to Bateman as a result of the theft, Bateman suffered significant emotional and mental distress and anxiety as a result of the fraudulent scheme.

243. After his Wallet was drained, Bateman made multiple attempts to contact Coinbase by phone to report the fraudulent withdrawal to Coinbase. Coinbase customer support never opened a support ticket to record or follow up on Bateman's reported theft. The Coinbase customer support

representative told Bateman that Coinbase could not assist him in recovering his funds. Coinbase never investigated the theft reported by Bateman, leaving him with no recourse to remedy the fraudulent withdrawal.

h. Kyle Thome

244. On or about November 23, 2021, Claimant Kyle Thome (“Thome”) was contacted by an individual on Facebook Messenger who invited him to participate in a liquidity mining pool investment opportunity on Coinbase. Thome was directed to create a Coinbase Wallet account and deposit funds into the Wallet to begin investing in the pool through Coinbase’s platform through a dapp called Bitethmine.com.

245. The following day, Thome entered in a smart contract through a node or voucher in order to join the liquidity mining pool. Between November 23, 2021 and January 28, 2022, Thome made five deposits into his Coinbase Wallet to fund the pool.

246. On February 5, 2022, Thome withdrew \$5,000.00 USDT from his Coinbase Wallet. Moments later, Thome’s entire Coinbase Wallet reflected a zero balance although he had not authorized any withdrawals from his account.

247. Thome never gave any third party his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his assets from his Wallet by entering the smart contract.

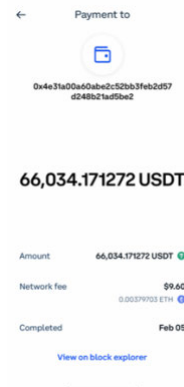
248. Coinbase Wallet never provided any warning to Thome that anyone could access his Wallet to take his funds without his express consent or authorization. To the contrary, Coinbase Wallet’s disclosures instructed Thome that the *only* way someone could access his funds was if he provided his security pass phrase or it was stolen or compromised.

249. Thome’s decision to engage in the liquidity mining pool was based on his reliance on Coinbase’s representations regarding its security protocol, and its reputation as a legitimate forum for cryptocurrency transactions.

250. After his Coinbase Wallet was emptied without his consent, Thome immediately contacted Coinbase’s customer service platform to inform it of the fraudulent withdrawal (Case No. # 10091580). Coinbase informed Thome that he was likely the victim of a malicious “smart contract”

scam and Coinbase would not reverse the transaction or reimburse Thome. According to Thome, the customer service representative, after Thome informed him of the loss, “seemed about as apathetic as someone could be.”

251. Thome’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$66,034.17 USDT, consisting of funds withdrawn from retirement fund. In addition to his grave financial loss, Thome suffered significant emotional distress as a result of the Coinbase liquidity mining pooling scam.

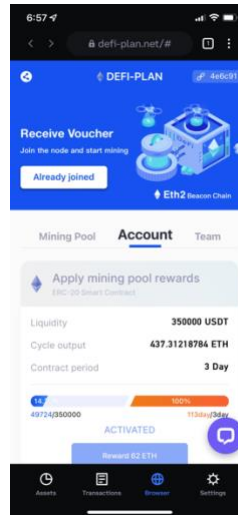


i. Jane Doe 1

252. On or about January 24, 2022, Claimant Jane Doe 1 was contacted by a man named, Mingyang Li on Instagram. Jane Doe 1 and Mingyang Li continued communicating by phone and eventually Mingyang Li raised to the topic of crypto investing. Mingyang Li invited Jane Doe 1 to join a dapp, only available on the Coinbase Wallet browser, called DEFI-PLAN (defi-plan.net). Mingyang Li portrayed the dapp as a legitimate liquidity mining pool through which Jane Doe 1 could earn significant interest on invested USDT.

253. On or about February 17, 2022, Jane Doe 1 agreed to join the liquidity mining pool through the dapp at Mingyang Li’s direction by purchasing a node. Unbeknownst to Jane Doe 1, by

purchasing the node, she entered into a smart contract that allowed the defrauders to access her entire Coinbase Wallet through the dapp.



254. Between February 17, 2022 and March 21, 2022, Jane Doe 1 made 16 deposits of USDT into her Coinbase Wallet to contribute to the liquidity mining pool. Initially, the liquidity mining pool functioned as Mingyang Li described and Jane Doe 1 was earning returns on her deposits.

255. After making several USDT deposits into her Coinbase Wallet, on March 1, 2022, all USDT in her Jane Doe 1's Wallet was removed. Despite the unexpected withdrawal, Jane Doe 1 still believed that the liquidity mining pool was legitimate because she had received the promised returns in connection with her prior deposits. Jane Doe 1 relied on Coinbase's representation that no one could remove assets from her Coinbase Wallet without her security recovery passphrase. Moreover, the dapp website led Jane Doe 1 to the ethereum.org website and named Coinbase as a business partner which indicated to Jane Doe 1 that the dapp was legitimate. Given Coinbase's wide usership and reputation, Jane Doe 1 did not believe that Coinbase would allow a scam website to operate on its platform.

256. Jane Doe 1 continued to participate in the pool and make deposits believing that all of her assets would be returned to her Coinbase Wallet after the completion of her contribution obligations were met.

257. On March 3, 4, 7, 14, 17, 18, 21 and 22, 2022, Jane Doe 1 made additional deposits of USDT in her Coinbase Wallet. After each deposit was made, the contents of Jane Doe 1's Wallet were removed by the dapp.

258. By March 22, 2022, scammers had withdrawn hundreds of thousands of dollars worth of USDT from Jane Doe 1's Wallet. These withdrawals were completed without Jane Doe 1's consent or any notification, warning, or substantive response from Coinbase.

259. Jane Doe 1 lost \$167,383.74 USD as a result of these unauthorized transactions. To fund her contribution to the fraudulent pool, Jane Doe 1 took out a number of personal loans and borrowed from her parent's retirement fund. In addition to her substantial financial loss, Jane Doe 1 suffered severe emotional and mental distress as a result of the scam.

260. On April 4, 2022, Jane Doe 1 brought this matter to Coinbase's attention (Case No. #11395046), explaining that she had not provided her security pass and Coinbase told her that she was the only person with "full control/access" to her Wallet and Coinbase could not provide any assistance to her in retrieving her funds or identifying the defrauders. Jane Doe 1 sent subsequent correspondence to Coinbase by email on April 5, 2022. In response to Jane Doe 1's April 5 email, Coinbase informed Jane Doe 1 that it had flagged the dapp for its security team but could not reimburse or credit her Wallet.

261. Jane Doe 1 also filed a complaint with the local police department in Belmont, Massachusetts.

j. Jeffrey Yeager

262. On or about October 16 2021, Jeffery Yeager ("Yeager") was contacted by an individual named "Alina (Lina) Ai" through Facebook, who offered Yeager an opportunity to participate in cryptocurrency liquidity mining investment on the Coinbase Wallet. Believing Coinbase to be legitimate and reputable exchange platform, Yeager agreed to participate in the pool.

263. Yeager even spoke to "Alina" by phone to confirm the legitimacy of the investment opportunity. Alina assured Yeager that there was no risk associated with the mining pool and enticed Yeager to trust her by noting that she had an uncle who worked for Coinbase.

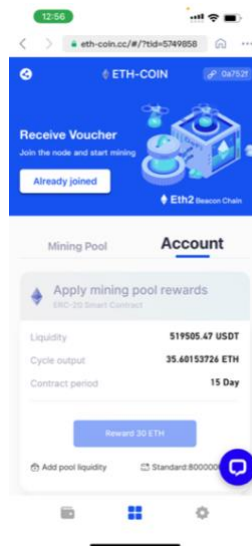
264. After months of consistent messaging and pressuring, Yeager agreed to participate in the mining pool call ETH-COIN on February 8, 2022 and unknowingly entered into a malicious smart contract which gave defrauders access to all of his Coinbase Wallet assets.

265. Alina continued to pressure Yeager into depositing more of his personal assets into his Coinbase Wallet. Between February 8, 2022 and March 24, 2022, Yeager made 22 deposits of USDT into his Coinbase Wallet to fund the pool. Yeager emptied his retirement fund and life savings to fund these contributions.

266. After Yeager had deposited over 344,000 USDT into his Coinbase Wallet account, Alina convinced Yeager to join a “reward event.”

267. On or about March 11, 2022, 344,220.50 USDT was drained from Yeager’s Coinbase Wallet. When Yeager contacted ETH-COIN’s customer service chat to inquire about the withdrawal, he was told that he had to deposit additional money to reach a balance of \$800,000 USDT within 15 days or he would lose all of his original investment.

268. As an alternative, ETH-COIN told Yeager that he could deposit \$172,000 USDT to “hedge” and avoid losing his initial investment. Yeager did not have \$172,000 USDT and asked Alina to borrow 52,000 USDT to complete the hedge. On or about March 24, 2022, Yeager deposited \$175,449 USDT into his Coinbase Wallet.

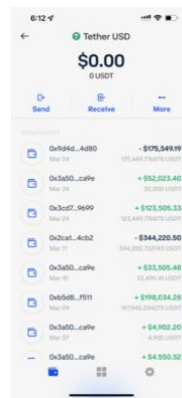


269. Despite successfully meeting his “hedge,” on March 24, 2022, defrauders withdrew the additional deposited assets from Yeager’s account, emptying his entire Coinbase Wallet and leaving him with nothing.

270. Coinbase Wallet never provided any warning to Yeager that anyone could access his Wallet to take his funds without his express consent or authorization. To the contrary, Coinbase Wallet's disclosures instructed him that the *only* way someone could access his funds was if he provided his security pass phrase or it was stolen or compromised.

271. Yeager never revealed his security passphrase to any third party and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his assets from his Wallet by entering the smart contract.

272. As a result of the fraudulent scam conducted on Coinbase's platform, Yeager lost over \$519,505.43 USDT. The theft decimated his life savings, foreclosing any opportunity to Yeager (age 66) to retire in the near future. The financial loss suffered as a result of the scam significantly diminished the financial stability of his family and caused Yeager substantial emotional and mental distress.



273. Yeager immediately contacted Coinbase to report the theft by phone and left several voice messages. Coinbase never returned Yeager's calls. Yeager followed up with Coinbase by email (Case Nos. #12603682, #10780091, #10733312, & #10683894) and Coinbase's customer service informed Yeager that he was likely the victim of a fraudulent scam and Coinbase was not responsible for any third-party transaction taking place on its platform.

274. In addition to notifying Coinbase's customer service about the fraudulent withdrawals, Yeager filed an iC3 report with the Federal Bureau of Investigations on March 14, 2022. On March 24, Yeager filed a police report with the Shelby Township Police department in Michigan. On April

4, 2022, Yeager filed a complaint with the Consumer Financial Protection Bureau (CFPB) against Coinbase for its acts in connection with the fraudulent scheme.

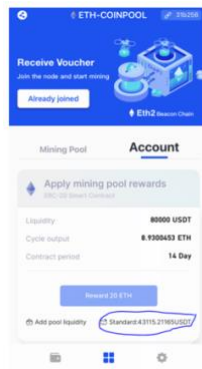
k. Thomas Daly Jr.

275. On or about December 18, 2021, Thomas Daly (“Daly”) was contacted by an individual on LinkedIn with an invitation join a liquidity mining pool on Coinbase. This individual appeared to be connected with several individuals in Daly’s professional network and possessed significant industry expertise when communicating with Daly.

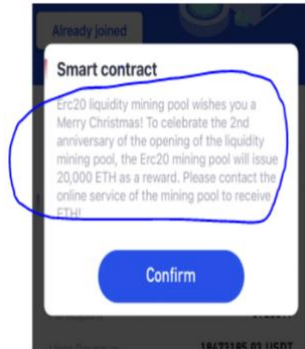
276. On or about December 23, 2021, Daly created a Coinbase Wallet account and deposited funds into the Wallet to begin investing in the pool through a dapp on the Coinbase platform called ETH-COINBASE (<https://eth-coinbase.net/#/?tid=56>).

277. On or about December 24, 2021, Daly purchased a “mining node” to begin mining on the dapp. Unbeknownst to Daly, he was actually entering into a malicious smart contract that gave defrauders on the platform access to his entire Coinbase Wallet without his consent or security passphrase.

278. Between December 24, 2021 and January 29, 2022, Daly made 16 deposits into his Coinbase Wallet in order to fund the pool.



279. On January 29, 2022, Daly received a message offering him a “reward” to celebrate the “2nd anniversary of the opening of the liquidity mining pool.” Daly unknowingly clicked a button confirming the reward, which inadvertently entered Daly into a smart contract which required him to deposit 80,000 USDT within 14 days.



280. Less than an hour after entering the smart contract, defrauders drained all the funds in Daly’s assets from his Coinbase Wallet without his consent or security passphrase.

281. Daly’s assets were removed from his Coinbase Wallet account by defrauder without Daly’s security passphrase. Coinbase Wallet never sent Daly a notification to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

282. Coinbase Wallet provided no warning to Daly stating that anyone could access his Wallet to take his funds through dapps. To the contrary, Coinbase Wallet’s disclosures instructed Daly that the *only* way someone could take his funds was if his “seed phrase” was stolen or compromised.

283. As a result of the Coinbase Wallet liquidity pooling scheme, Daly lost a total of \$43,115.12 USDT. These funds consisted of Daly’s (age 64) entire retirement savings, forcing Daly to re-enter the job market from retirement to make ends meet. However, due to economic downturn in California he has been unable to find a position that will satisfy his financial needs to remain solvent. Daly has suffered significant anxiety and emotional distress as a result of the loss’s impact on his financial future.

284. On or about February 14, 2022, Daly contacted Coinbase’s customer support team to report the fraudulent withdrawal (Case Nos. #10288687, #10289453). Coinbase responded with a generic auto-response which informed Daly that Coinbase “cannot reimburse or credit your wallet.” On February 18, Daly filed a report with the Federal Bureau of Investigation’s Internet Crime Complaint Center. For months after Daly reported the scam to Coinbase, the scam dapp remained fully operational within the Coinbase Wallet platform.

I. Gabriel Rockman

285. On or about November 16, 2021, Gabriel Rockman (“Rockman”) met an individual named “Alice” on WhatsApp, a social media messaging platform, who introduced him to a liquidity mining pool investment opportunity through a dapp called SUSHI DEFI on Coinbase (<https://sushi-defi.com>). Alice promised Rockman that he could earn 0.8% interest return per day on his investments. When Rockman tested the mining pool, he did earn 0.8% interest on USDT deposited into the pool. Based on these early returns, Rockman believed that the opportunity was legitimate.

286. On or about November 29, 2021, Rockman agreed to participate in the mining pool and the following day, he made his initial deposit into the pool. Between November 30, 2021 and December 14, 2021, Rockman made four deposits into his Coinbase Wallet to fund the pool.

287. On or about December 13, 2021, Rockman’s Coinbase Wallet, containing \$8631.41 USDT at the time, was emptied. Rockman immediately contacted Alice, who informed Rockman that he was still earning interest on his investments and despite the zero balance, his assets were still in his Wallet, but had been “pledged” to the pool and they would reappear in his account in 30 days. Based on these assurances, Rockman continued to deposit assets into his Coinbase Wallet. Rockman liquidated his entire savings and sold funds in a taxable brokerage account to meet the funding demands of the dapp.

288. On or about December 16, 2021, Rockman’s subsequent deposits were drained from his Coinbase Wallet in unauthorized transfers. Rockman informed Alice that he would not deposit any more of his liquid assets into his Coinbase Wallet. In response, Alice became verbally abusive and Rockman realized that he was the victim of a fraudulent scheme and would not be receiving his funds back as promised by Alice. Coinbase Wallet never sent Rockman a notification to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

289. Coinbase Wallet provided no warning to Rockman stating that anyone could access his Wallet to take his funds through dapps. To the contrary, Coinbase Wallet’s disclosures instructed Rockman that the *only* way someone could take his funds was if his “seed phrase” was stolen or compromised.

290. As a result of the Coinbase liquidity mining pool scam, Rockman lost \$35,045.78 USDT (approximately \$35,000.00). Rockman suffered additional financial loss by way of fees and transaction costs associated with his attempted retrieval/transfer of ETH from Coinbase.

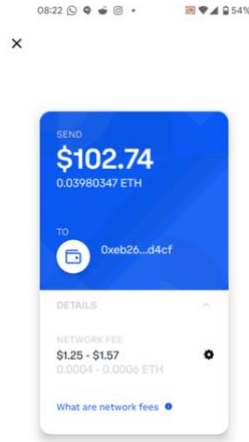
291. Due to the fraudulent scam, which was compounded by Coinbase's ineffective and dishonest representations in response to Rockman's complaint, Rockman suffered significant emotional and mental distress which has impacted his daily life, including his ability to perform his job resulting in Rockman having to request a decrease in his workload at work. Subsequently, Rockman applied for but did not receive a promotion at his job. Rockman experiences persisting effects on his mental health as a result of the Coinbase fraud.

292. On December 20, 2021, Rockman contacted Coinbase to report the fraudulent activity and seek guidance on how to recoup his stolen assets (Case No. # 09166849). Coinbase informed Rockman that his 12-word recovery phrase had been used to access his Coinbase Wallet. However, Rockman never revealed his security passphrase to any third party.

293. On December 27, 2021, Rockman filed a formal complaint with Coinbase. On January 7, 2022, Coinbase informed Rockman that its "investigation" indicated that his recovery passphrase was compromised and "Coinbase cannot recover or reverse the transactions in question" and was therefore denying his complaint. However, when pressed for evidence of the unauthorized use of Rockman's passphrase on January 17, 2022, Coinbase changed its position and instead informed Rockman that he created a "token authorization" that gave defrauders access to his Wallet.

294. Throughout February of 2022, Rockman continued his attempts to receive assistance from Coinbase to address his losses. On or about February 28, 2022, Rockman requested that Coinbase close his Coinbase and Coinbase Wallet accounts. Coinbase continued to respond to Rockman with boilerplate automated messages.

295. Rockman further requested instructions on how to retrieve the remaining Ethereum balance in his Coinbase Wallet (the initial interest earned at the start of the scam).



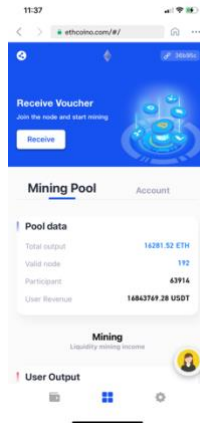
296. On or about March 1 and 2, 2022, Rockman sent Coinbase multiple emails requesting instructions for how to sell the ETH in his account or transfer it to his bank account. Coinbase informed Rockman that he had to sell his ETH to his Coinbase Wallet in order to cash out from Coinbase. Rockman agreed to redownload the Coinbase application but expressly declined to agree to its terms of service. Rockman continued to receive automated, non-responsive replies to his request for the return of his remaining funds and assistance closing his accounts from Coinbase customer service staff.

297. On March 5, 2022, Coinbase informed Rockman that it was closing his account but did not address the return of his remaining ETH balance. On March 7, 2022, Coinbase informed Rockman that it would not be returning his approximately \$102 dollars' worth of ETH because the "small balance . . . is dust" and insufficient to cover blockchain network fees.

m. Maurits van Westenbrugge

298. On or about February 6, 2022, Maurits van Westenbrugge ("van Westenbrugge") was contacted by an individual on Tinder and WhatsApp, a social media messaging platform. This individual invited van Westenbrugge to join a dapp, only available on the Coinbase Wallet browser, called ETHCOINO (ethcoino.com/#/). The individual portrayed ETHCOINO as a USDT mining pool where van Westenbrugge could earn interest on invested USDT.

299. On or about February 15, 2022, van Westenbrugge unknowingly entered into a smart contract by receiving a “voucher” and began depositing additional funds and converting existing crypto to USDT in his Coinbase Wallet to fund the pool.



300. Between February 15, 2022 and February 25, 2022, van Westenbrugge made 6 deposits into his Coinbase Wallet to meet required “Standard Amounts” during the time periods demanded by ETHCOINO. Each time van Westenbrugge hit his Standard Amount, his deposit requirement would increase. This was moment Westenbrugge realized that he had been targeted by a fraudulent scheme.

301. On February 21, February 22, February 24, and February 25, 2022, fraudsters drained significant amounts of crypt from van Westenbrugge’s Coinbase Wallet without his consent in unauthorized transfers. As a result of the fraudulent withdrawals, van Westenbrugge suffered a financial loss totaling \$45,004.13 USDT, exclusive of additional losses incurred by van Westenbrugge through ETH to USDT transfers made in furtherance of the fraudulent mining pool.

302. After reading multiple stories about Coinbase’s deficient customer service support and its reported refusal to compensate victims for losses incurred as a result of the Coinbase liquidity mining schemes, van Westenbrugge declined to formally report the theft of his asset and resolving to simply shoulder the loss.

303. On or around September 18, 2022, van Westenbrugge contacted Coinbase customer support to report the theft of his assets from his Coinbase Wallet (Case No. #13097877). In his email to Coinbase, van Westenbrugge explained that his assets were stolen by scammers through a dapp called ethcoino.com, which he accessed through Coinbase’s browser. In response, Coinbase did not

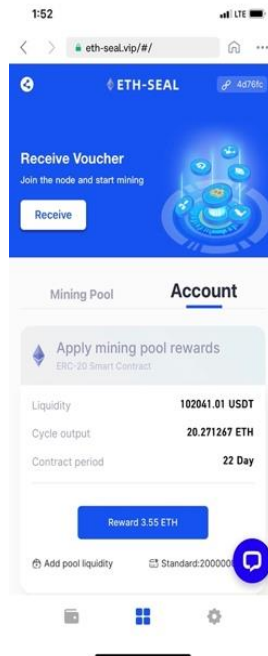
acknowledge the fraudulent dapp or provide van Westenbrugge with any guidance on how to recover his stolen funds or report the theft to law enforcement. Instead, Coinbase informed van Westenbrugge that it was unable to investigate his report without the transaction hash associated with the fraudulent transaction.

n. Chao Tian

304. On or about October 7, 2021, Chao Tian (“Tian”) was contacted by an individual on Instagram. On or about October 9, 2021, the individual told Tian about passive income that she had earned through a liquidity mining pool called ETH-SEAL.

305. On or about October 10, 2021, Tian was invited to join the liquidity mining pool.

306. On or about October 11, 2021 Tian joined the pool by agreeing to “receive a node” on or about October 11, 2021, which unbeknownst to Tian, was a smart contract that gave defrauders access to his entire Coinbase Wallet.



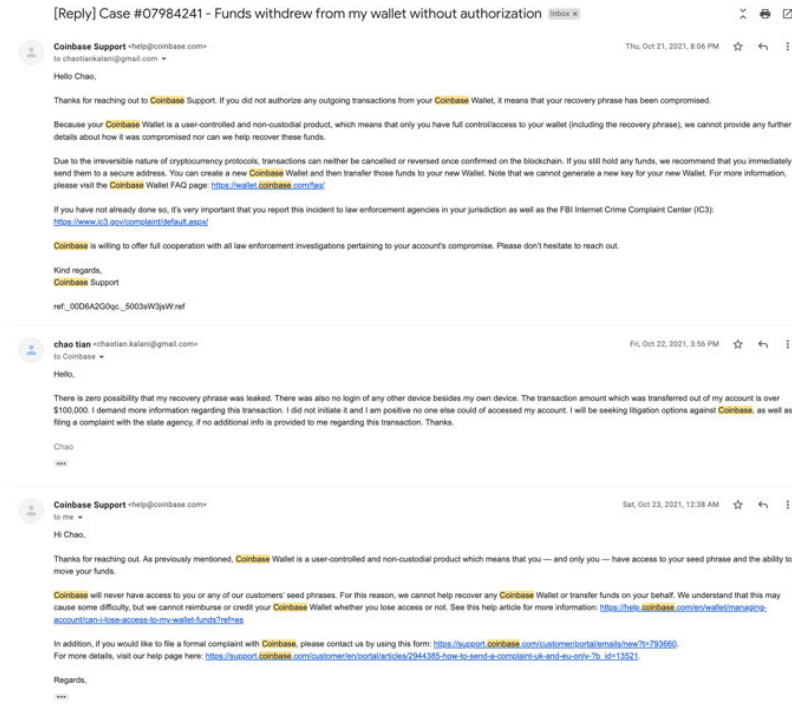
307. Between October 13, 2021 and October 23, 2021, Tian made five deposits into his Coinbase Wallet account to fund the pool. These funds consisted of Tian’s entire life savings.

308. On or about October 21, 2021, the scammer drained Tian’s entire Coinbase Wallet in unauthorized transfers. As a result of the scheme, Tian lost \$102,041 USDT from his Coinbase Wallet.



309. In addition to significant financial loss, Tian suffered serious mental and emotional harm, including depressive episodes and loss of support from family members as a result of the Coinbase liquidity mining scam and Coinbase’s refusal to adequately warn or assist Coinbase customers in recouping their stolen funds.

310. On October 21, 2021, Tian immediately contacted Coinbase by email to inform the Company of the fraudulent withdrawals made from his Coinbase Wallet account without his authorization (Case No. #07984241). The following day, Coinbase Support responded to Tian informing him that his “recovery phrase has been compromised.” The following day, Tian replied to Coinbase Support assuring them that there was “zero possibility that [his] recovery phrase was leaked.” In response, Coinbase replied with a generic message, restating Coinbase’s “non-custodial” feature and stating that Coinbase “cannot help recover any Coinbase Wallet or transfer funds on [Tian’s] behalf.”



o. Filip Lorinc

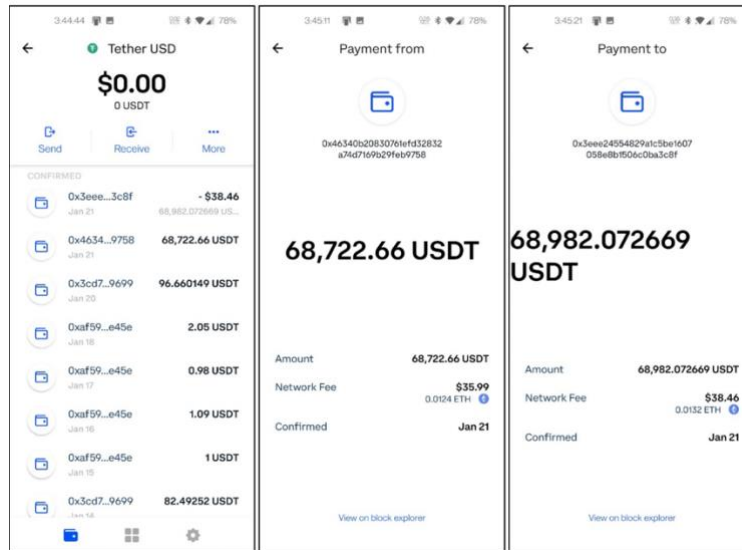
311. On or about January 8, 2022, Filip Lorinc (“Lorinc”) was introduced to an individual named “Elsa Taisiya” on Tinder, a social dating application. Lorinc and Elsa continued to chat on WhatsApp, a social messaging application. Elisa introduced Lorinc to a mining pool operation on a dapp on Coinbase called BIPAI (bteaa.com). Elisa assured Lorinc that the operation was “legitimate.”

312. On or about January 13, 2022, Lorinc agreed to join the mining pool and was instructed to “redeem a voucher” on the dapp via his Coinbase Wallet. In reality, Lorinc (without his knowledge) had consented to a backend token approval transaction through a smart contract would allow defrauders unlimited access to his Coinbase Wallet.

313. Between January 13, 2022 and January 21, 2022, Lorinc made four deposits of USDT into his Coinbase Wallet to contribute to the mining pool.

314. Initially, the operation appeared to be legitimate and even yielded ETH returns consistent with Elisa’s promises. Based on this, Lorinc continued to contribute to the pool.

315. On or about January 21, 2022, Lorinc made a deposit of additional USDT to his Coinbase Wallet, increasing his Coinbase Wallet balance to \$68,982 USDT. Within ten minutes of Lorinc’s deposit, his entire Coinbase Wallet was emptied and sent to an unknown address without his authorization.



316. On January 24, 2022, Lorinc attempted to contact the customer support staff within the dapp to report the unauthorized withdrawal. Lorinc was informed that his funds had been “frozen” temporarily and he would have to deposit additional USDT into his Coinbase Wallet account to “unlock” his account and retrieve his withdrawn assets.

317. Lorinc now realized that he had been targeted as a victim in a fraudulent crypto scheme on Coinbase’s platform. Nevertheless, he attempted to continued negotiating with the dapp’s customer service and requested the return of his funds. The customer service chat replied informing him that his “account” had now been permanently frozen. Shortly thereafter, any trace of his account on bteaa.com vanished.

318. Coinbase Wallet never provided any warning to Lorinc that anyone could access his Wallet to take his funds without his express consent or authorization. To the contrary, Coinbase Wallet’s disclosures instructed him that the *only* way someone could access his funds was if he provided his security pass phrase or it was stolen or compromised.

319. Lorinc never revealed his security passphrase to any third party and did not receive a notification or warning from Coinbase Wallet regarding the risk associated with dapp transactions on the Coinbase platform.

320. As a result of the Coinbase liquidity pool scam, Lorinc lost \$68,982.07 USDT he deposited into his Coinbase Wallet that was later fraudulently withdrawn by the defrauder without his consent or authorization. These funds consisted of Lorinc's retirement funds and personal savings.

321. In addition to the financial losses suffered by Lorinc, he suffered mental stress and anxiety as result of his victimization and expended numerous hours and significant energy to engage in the process of reporting the fraud to Coinbase, local law enforcement and federal agencies.

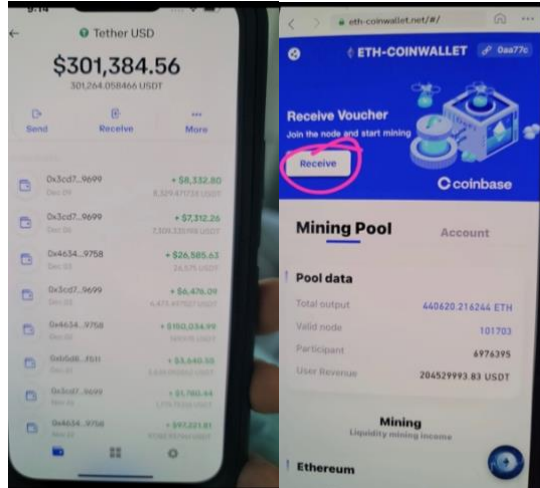
322. Following the fraudulent withdrawal of his assets, Lorinc contacted Coinbase customer support (Case No. # 09796181). Coinbase was wholly unhelpful and failed to provide Lorinc with adequate guidance to assist him in addressing his concerns. Lorinc believes he told Coinbase the name of the malicious dApp in order to prevent additional thefts in the future, but months later the dApp was still active.

323. On or about January 25, 2022, Lorinc filed a complaint with the Internet Crime Complaint Center of the Federal Bureau of Investigation and filed an Identity Theft Report with the Federal Trade Commission recounting the fraudulent activity. On or about January 26, 2022 he reported the stolen assets to the McKinney Texas Police Department.

p. John Doe 1

324. On or about April 25, 2021, John Doe 1 was contacted on Facebook by an individual who invited John Doe 1 to participate in liquidity mining pool investment opportunity. John Doe 1 and this individual continue to discuss the liquidity pool operation on WhatsApp, a social messaging

application. This individual sent John Doe 1 pictures of her account, depicting purported returns on her investments and instruction for John Doe 1 to join the pool by receiving a voucher.



325. On or about November 22, 2021, John Doe 1 unknowingly entered into a smart contract through a dapp called ETH.coinwallet.com on Coinbase’s platform which allowed defrauders access to all of his assets which he believed were secured safely in his Coinbase Wallet account.

326. Between November 22, 2021 and December 15, 2021, John Doe 1 made six deposits of USD into his Coinbase Wallet to enable him to contribute USDT to the pool. These assets were his life savings.

Transaction History		Transaction History	
FRI, DEC 10	USD Deposit Processed \$33,000.00 USD	WED, JAN 12	
FRI, DEC 3	USD → USDT Completed \$27,094.13 USD	WED, DEC 15	USD → USDT Completed \$47,276.84 USD
THU, DEC 2	USD → USDT Completed \$152,833.81 USD		USD → USDT Completed \$152,797.16 USD
MON, NOV 29	USD → MANA Completed \$171.61 USD		USD Deposit Processed \$197,000.00 USD
MON, NOV 22	USD → USDT Completed \$99,825.48 USD	FRI, DEC 10	USD → USDT Completed \$30,000.97 USD
	USD Deposit Processed \$100,000.00 USD	FRI, DEC 3	USD Deposit Processed \$33,000.00 USD
		THU, DEC 2	USD → USDT Completed \$27,094.13 USD
			USD → USDT Completed \$152,833.81 USD

327. As a result of his exposure to this fraudulent scheme on Coinbase’s platform, John Doe 1 suffered \$509,828.39 USDT in losses, plus transaction and wire transfer fees.

328. In addition to his financial losses, John Doe 1 and his family have been placed under serious mental and emotion stress as they now face an impending inability to meet their financial responsibilities as a result of the theft. John Doe 1 is now considering filing for bankruptcy.

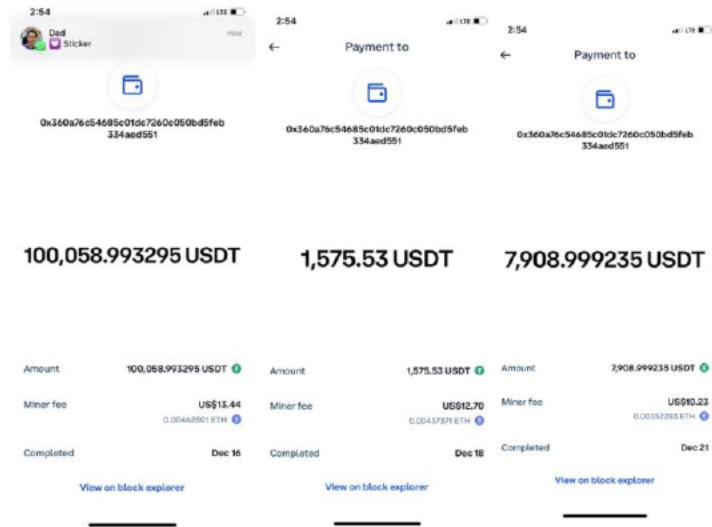
329. John Doe 1 first reported the malicious dapp site to Coinbase in mid-December 2021. On or about February 18, 2022, John Doe 1 contacted Coinbase customer support to report the unauthorized withdrawal and file a formal complaint with Coinbase (Case No. Case #09200587). In response, Coinbase informed John Doe 1 that it would investigate his complaint but Coinbase never provided John Doe 1 with any feedback or guidance for John Doe 1 to recoup his stolen assets. Months after John Doe 1 reported the scam, Coinbase had still not taken down the scam dapp or blocked it on the Wallet platform.

q. Raymond Leung

330. On or about December 4, 2021, Raymond Leung (“Leung”) was contacted by an individual named “Vika” on WhatsApp. Vika advised Leung to join a liquidity crypto mining pool. Vika instructed Leung to deposit USDT into his Coinbase Wallet in order to participate in the pool.

331. On or about December 12, 2021, Leung unknowingly entered into a smart contract through a dapp called “eth-flowcell.cc” on Coinbase and began making contributions to the pool.

332. Between December 16, 2021 and December 21, 2021, Leung made three deposits of USDT into his Coinbase Wallet to fund the pool.



333. Initially, the USDT Leung deposited remained in his Coinbase Wallet and he was able to withdraw profits back into his Coinbase Wallet. Based on this initial experience, Leung decided to increase his contributions to the pool in the hope of receiving increased returns. After the increase, Leung held approximately \$100,000 USDT in his Coinbase Wallet.

334. On or about December 18, 2021, all of the crypto was drained from Leung’s Coinbase Wallet without his consent or authorization. Leung immediately contacted the dapp’s “customer support” chat about the unauthorized withdrawal. The customer support representative informed Leung that his asset had been transferred into the pool and he would need to increase his contribution to \$200,000 USDT.

335. At this point, Leung became suspicious and sought to withdraw from the pool. Leung was told that he had signed a smart contract through the dapp upon joining the liquidity mining pool and would have to deposit an addition \$90,000 USDT to fund the pool or he would lose all of his assets.

336. As a result of this Coinbase liquidity mining pool scam, Leung’s total monetary loss equals \$109,631.82 USDT. Leung withdrew thousands of dollars from his personal savings to participate in the pool. In addition to monetary damages suffered, Leung has experienced significant mental and emotion distress, has accumulated massive debt, and is on the brink of losing his home.

337. On December 21, 2021, Leung contacted Coinbase customer service to report the fraudulent activity and seek assistance in retrieving his stolen assets (Case No. #10151051).

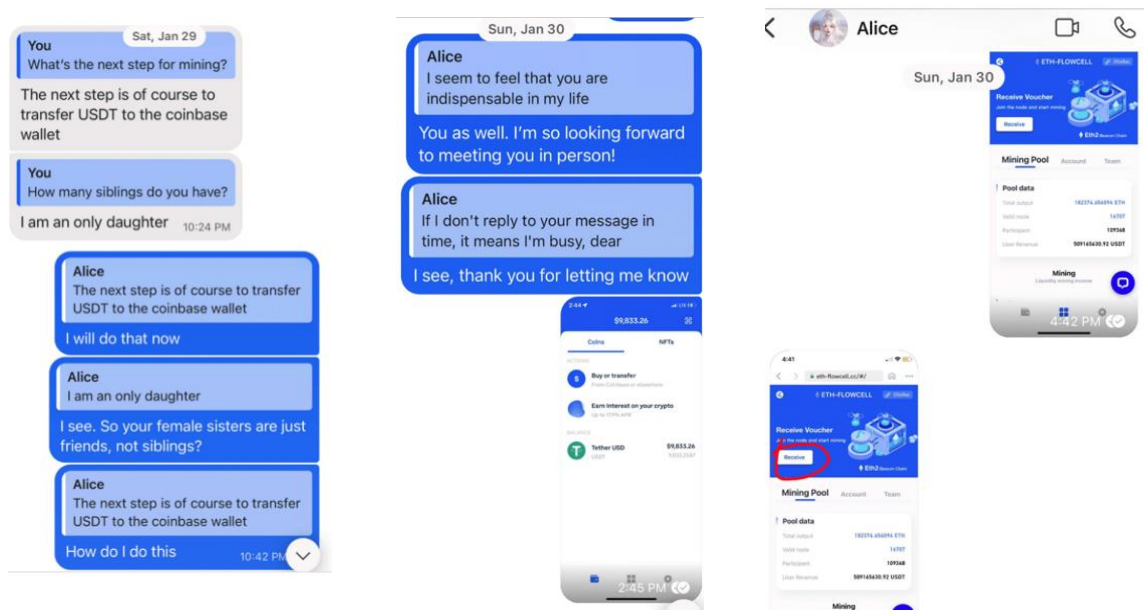
338. On February 9, 2022, Coinbase responded to Leung informing him that “there is no way for Coinbase to cancel, reverse, or recover these funds on [his] behalf” and closed Leung’s complaint case on February 14, 2022.

339. Having received no assistance from Coinbase, Leung filed a complaint with the Federal Bureau of Investigation and his local authorities.

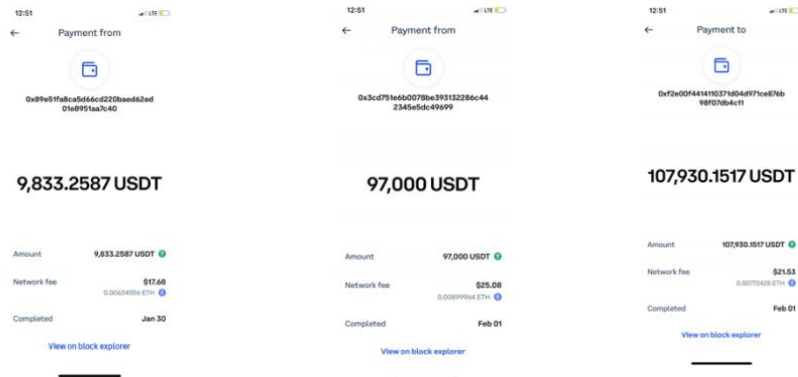
r. Christian Kelly

340. On or about January 11, 2022, Christian Kelly (“Kelly”) was contacted by an individual named “Alice” on a social dating application. Alice continued to chat with Kelly on Signal, a social messaging application.

341. After multiple messages insisting that Kelly could earn money through the DeFi operation, Kelly agreed to participate in a liquidity mining pool on a dapp called “eth-flowcell.com” through Coinbase on or about January 29, 2022.



342. Between January 29, 2022 and February 1, 2022, Kelly made two deposits from his account into his Coinbase Wallet to fund the pool. Alice continued to persuade Kelly to invest more and more of his assets into the pool under the guise that they were working together to build towards a joint financial future for them as a couple. To meet Alice's requests, Kelly took out a loan to meet the deposit targets for the dapp.



343. On or about February 1, 2021, after Kelly's Coinbase Wallet account reached over \$100,000 USDT, all of Kelly's assets in his Coinbase Wallet were drained by the dapp scammer in unauthorized transactions.

344. Kelly never believed – and had no reason to believe – that he had allowed anyone else access to his funds in his Wallet. Indeed, Coinbase Wallet provided no warning to Kelly that he would be relinquishing control of his Coinbase Wallet and his funds. To the contrary, Coinbase Wallet's disclosures told Kelly that the *only* way someone could take his funds was if his "seed phrase" was stolen or compromised.

345. This fraudulent withdrawal was done without Kelly's permission or consent.

346. On or about April 16, 2022, Kelly contacted Coinbase customer support by email to report the fraudulent withdrawal (Case No. # 11384370). That same day, Kelly received a generic response from Coinbase stating that Coinbase cannot reimburse him for the loss. Coinbase's customer support was entirely unhelpful.

347. Kelly has suffered significant loss as a result of the scam facilitated on Coinbase's exchange. Kelly lost \$107,841.02 USDT in crypto assets. These funds were Kelly's entire life savings.

Kelly took on significant debt to make deposits consistent with Alice's request. He will be paying the interest on this loan for years. Kelly's life has been dramatically altered by this scam and continues to suffer mental and emotional anguish.

s. Daniel Chang

348. On or about December 14, 2021, Daniel Chang ("Chang") was contacted by a woman on WeChat, a social messaging application. Chang and this woman began chatting and became very friendly. The woman then introduced Chang to a liquidity mining investment opportunity that she claimed would pay "high interest." Chang was interested in the opportunity, but sought additional information about how the investment pool worked. The woman explained the process and convinced Chang to join the liquidity mining pool, join Coinbase Wallet and deposit USDT into his Wallet.

349. On December 14, 2021, Chang unknowingly entered into a smart contract through a dapp called <https://defi.ethereum-eth.cc> on Coinbase's platform, which enabled defrauders to access his entire Wallet and make withdrawals without his consent.

350. On or about December 14, 2021, Chang began making deposits of small amounts of USDT into the liquidity mining pool.

351. Between December 14, 2021 and March 11, 2022, Chang made four deposits of USDT into his Coinbase Wallet in order to fund the pool. Initially, the pool operated in accordance with the woman's description and Chang believed he would be able to make a return on his investment using the dapp. Based on this understanding, Chang continued depositing USDT into his Wallet and making larger deposits into his Wallet over time.

352. On or about January 16, 2022, approximately \$31,633.01 USDT, was withdrawn from Chang's Coinbase Wallet in an unauthorized transaction. Chang was informed by the dapp's customer support agent that his USDT had been contributed to the pool but was still in his possession. In reliance on these assurances, Chang continued to deposit USDT into his Coinbase Wallet to contribute to the funds.



353. On or about March 3, 2022, Chang made a deposit of \$224,975 USDT into his USDT wallet. Later that day, Chang's Coinbase Wallet was emptied again.

354. Chang contacted the dapp's customer service support who informed Chang that he would have to "pay taxes" and an additional amount equal to what he had earned before the dapp would release his money back to him. On March 11, 2022, Chang, desperate to recoup his funds, deposited another \$34,975 USDT into his Coinbase Wallet.

355. Chang's assets were never returned and as a result, he has suffered substantial financial harm, totaling \$289,916 USDT as a result of the Coinbase liquidity mining pool scam.

356. The loss of the assets contained in his Coinbase Wallet has significantly altered his life. Chang, age 50, had previously planned to purchase a house for his family, but has now lost his entire life savings as a result of the scam.

357. A close friend of Chang's was induced into the scheme and defrauded. When Chang's friend approached the woman who introduced them to the liquidity mining pool, the woman informed Chang and his friend that she was not responsible for what happened to them.

358. Chang’s friend reported the unauthorized withdrawals to Coinbase customer support, however, Coinbase’s response was wholly inadequate. Coinbase informed Chang and his friend that it could not do anything to assist them in retrieving their stolen assets.

t. Raphael Elbaz

359. On or about November 16, 2021, Raphael Elbaz (“Elbaz”) met and began chatting with a woman in group chats on Discord. The woman appeared to be very knowledgeable about cryptocurrency and was followed by many people on social media. After several exchanges in the group chats, the woman and Elbaz continued to chat about crypto and her personal investments on WhatsApp, a social media messaging application. The woman told Elbaz that she had made personal gains using a liquidity mining pool on Coinbase. The woman specifically asked Elbaz if he used “Coinbase Wallet” and whether Coinbase had “sent him the mining node.”

360. The woman sent Elbaz screenshots purportedly showing her participation in the pool and gains of over \$1,000,000 USD and told Elbaz that she would share the Coinbase Wallet mining node with him, but he could not share it with others.

361. The woman further instructed Elbaz to install a dapp called “ETH.prime” on Coinbase and deposit USDT into his Coinbase Wallet to contribute to the fund. Elbaz did as instructed. Unbeknownst to Elbaz, he had actually entered into a fraudulent smart contract which allowed the scammer access to the entirety of his Coinbase Wallet.

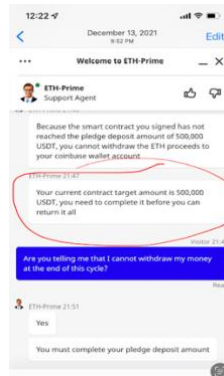
362. Between November 18, 2021 and January 2, 2022, Elbaz made a total of nine deposits of USDT into his Coinbase Wallet to fund the pool.

363. After initial testing with smaller USDT deposits, Elbaz was invited to increase his contribution to the pool in order to earn a reward of additional ETH. Elbaz agreed to meet the pool criteria and deposit \$100,000 USDT. Once Elbaz’s Coinbase Wallet began to reach the \$100,000 USDT target, the target increased without warning to \$300,000 USDT.

364. Throughout the scam, Elbaz was in constant communication with an individual who held himself out to be “Coinbase customer support” through the dapp chat box. The customer service representatives assured Elbaz that he was chatting with an employee of Coinbase and that his funds were still available to him.

365. Before meeting the \$300,000 USDT benchmark, Elbaz contacted customer service who assured him that all of his funds and awards would go back to his wallet automatically upon expiration of his “contract.”

366. As soon as Elbaz’s reached the \$300,000 USDT benchmark, the deposit target automatically increased.



367. On or about December 9, 2021, Elbaz attempted to withdraw his funds from the mining pool, but was again told by the purported customer service representative that he would have to deposit additional USDT to reach a new deposit threshold of \$500,000 USDT in order to fulfill the smart contract and retrieve his assets from the pool. At this point, Elbaz realized that he had been defrauded.

368. Elbaz never believed – and had no reason to believe – that he had allowed anyone else access to his funds in his Wallet. Indeed, Coinbase Wallet provided no warning to Elbaz stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures told Elbaz that the *only* way someone could take his funds was if his “seed phrase” was stolen or compromised.

369. On December 10, 2021, Elbaz sought and procured the services of CoinStructive, a blockchain forensics and analysis firm, to track down and locate his stolen assets. CoinStructive was able to locate Elbaz’s stolen assets and pinpoint the exact wallet addresses that the assets were transferred to with little effort.

370. As a result of the Coinbase Wallet liquidity mining scam, Elbaz lost a total of \$300,924 USDT, which consisted of his entire life savings, in unauthorized transactions. Elbaz has suffered mental and emotion distress as a result of his victimization.

371. Following the fraudulent withdrawal made from his Wallet, Elbaz contacted Coinbase customer support to report the theft (Case No. #09003544). Coinbase’s response was wholly inadequate and failed to provide Elbaz with any guidance or assistance in retrieving his stolen assets. Further, Coinbase did not block or take down the malicious dapp.

u. Leandro Paparelli

372. On or about October 2, 2021, Leandro Paparelli (“Paparelli”) was contacted by a person named “Li na” via Instagram.

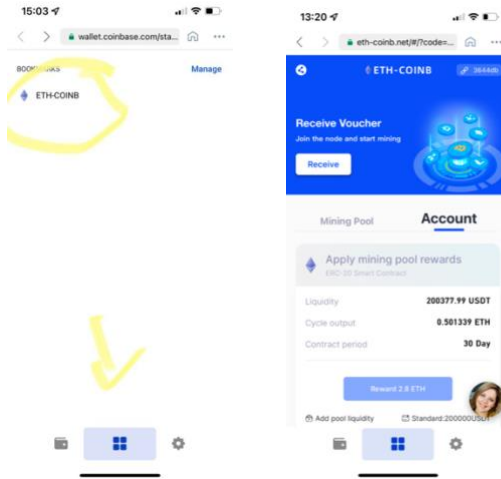
373. After befriending Paparelli, the individual and Paparelli began communicating via WhatsApp, a social messaging application. Li na informed him that she was very successful in trading crypto. Paparelli and Li na discussed a number of investment strategies but ultimately Li na emphasized that she had earned significant income over Coinbase in a liquidity mining pool.



374. Paparelli was skeptical of the opportunity at first, but Li na convinced him that it was a safe and secure investment strategy and emphasized that “no hacker in the world can break into Coinbase Wallet.” Paparelli conducted his own research into the security of Coinbase Wallet. Coinbase held itself out to be a “user centric” platform and represented to users that no funds could be accessed, transferred or withdrawn from a user’s Wallet without a private key. After several months of Li na’s persuading, and in reliance on Coinbase’s assurances, Paparelli agreed to join the pool.

375. On or about October 20, 2021, Li na directed Paparelli to download Coinbase Wallet application and open the link for a dapp called “ETH-COINB” using the Wallet’s browser. Paparelli

did as he was instructed. Unknowingly, Paparelli had just agreed to enter a smart contract that would allow defrauders to access his entire Coinbase Wallet through the dapp.



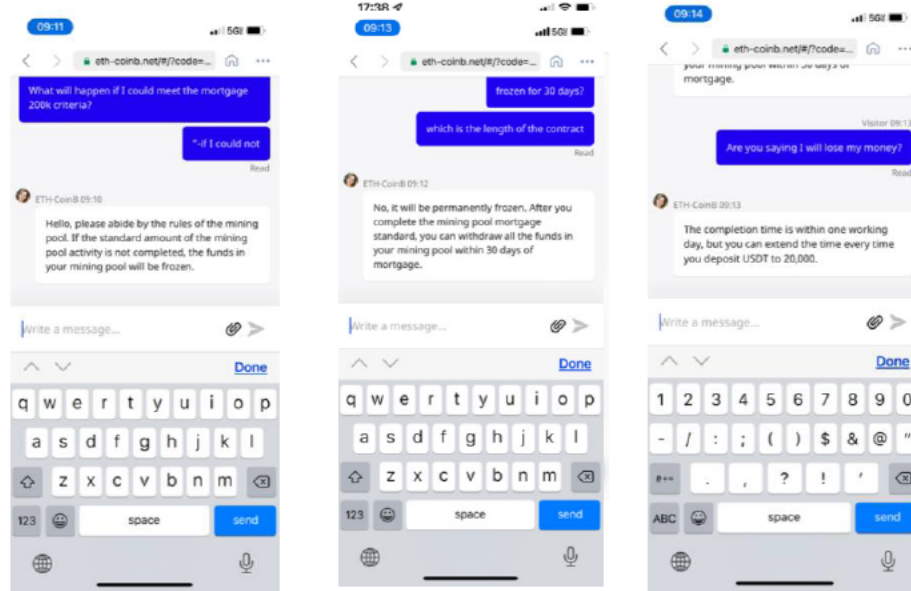
376. Having lulled Paparelli into the liquidity pool, Li na directed to start depositing USDT into his Coinbase Wallet in order to start investing in the pool.

377. Initially, the liquidity mining pool operated as described by Li na and Paparelli received some initial ETH returns on his investment. Paparelli continued to make deposits until he became weary of that the investment model might be a scam and decided to withdraw his funds from the pool.

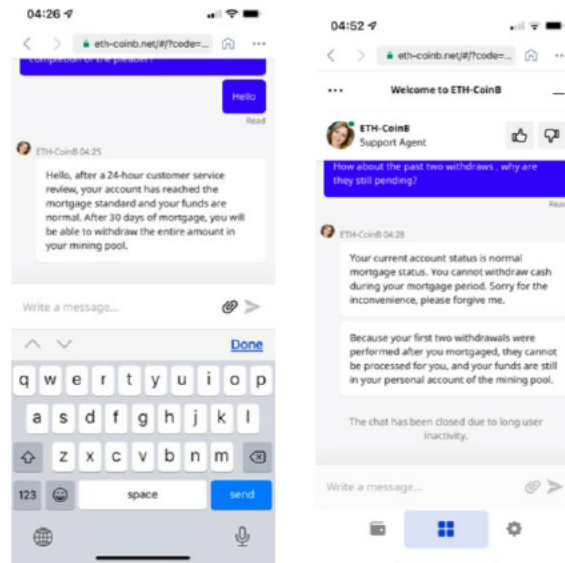
378. Between October 22, 2021 and October 31, 2021, Paparelli made thirty nine deposits of USDT into his Coinbase Wallet. Paparelli's investment appeared to be making a small profit and when he went to claim his returns, his return balance disappeared.

379. Paparelli sent a message inquiring about the status of his account using the customer support chat in the dapp to an agent, who claimed to be a Coinbase Wallet agent.

380. The agent informed Paparelli that he had to deposit another \$100,000 USDT into the pool within 30 days in order to meet the \$200,000 contribution threshold or his funds would be lost.



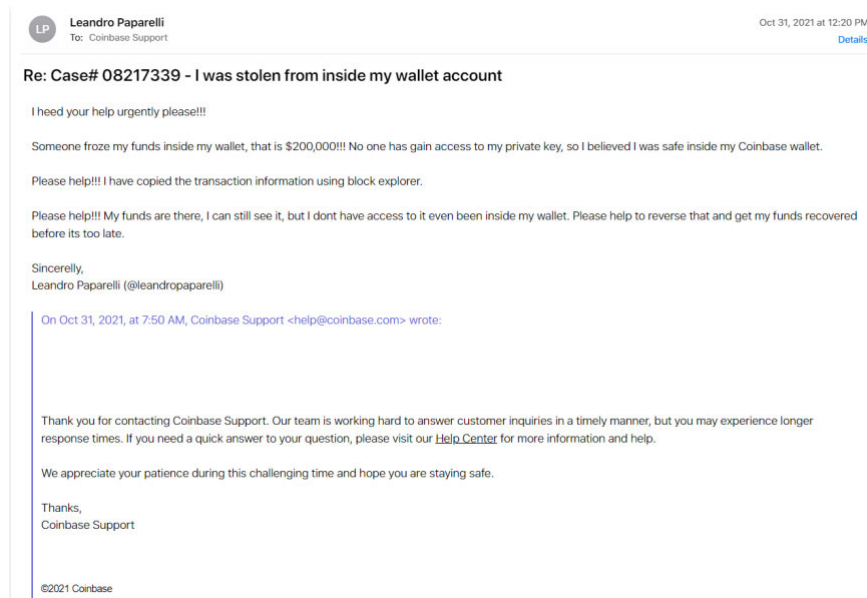
381. In fear of losing all of his assets, Paparelli made the additional contribution to meet the \$200,000 USDT contribution threshold. After making the final deposit on October 31, 2021, Paparelli inquired about his ability to withdraw his assets, as promised. He received the following messages, informing him that he could not withdraw his assets.



382. Despite the promises made to him regarding the return of his assets after the “mortgage period,” Paparelli never received any of his money back. Devastatingly, Paparelli lost his life savings as a result of this investment scam.

383. Paparelli’s total losses amounted to \$200,000 USD. In addition to his financial losses, he suffered serious mental and emotional distress, pushing him to the brink of suicidal ideation.

384. On October 31, 2021, Paparelli contacted Coinbase customer support to report his stolen assets (Case No. #08217339). Coinbase customer response replied to Paparelli informing him that Coinbase support was struggling to respond to customer inquiries in a timely manner.



385. Despite Paparelli insistence that the issue was urgent and time-sensitive, Coinbase failed to respond timely to his multiple emails seeking assistance from Coinbase which included screenshots of the fraudulent activity and the address of the scammer (Case Nos. #08334768 and #08238477).

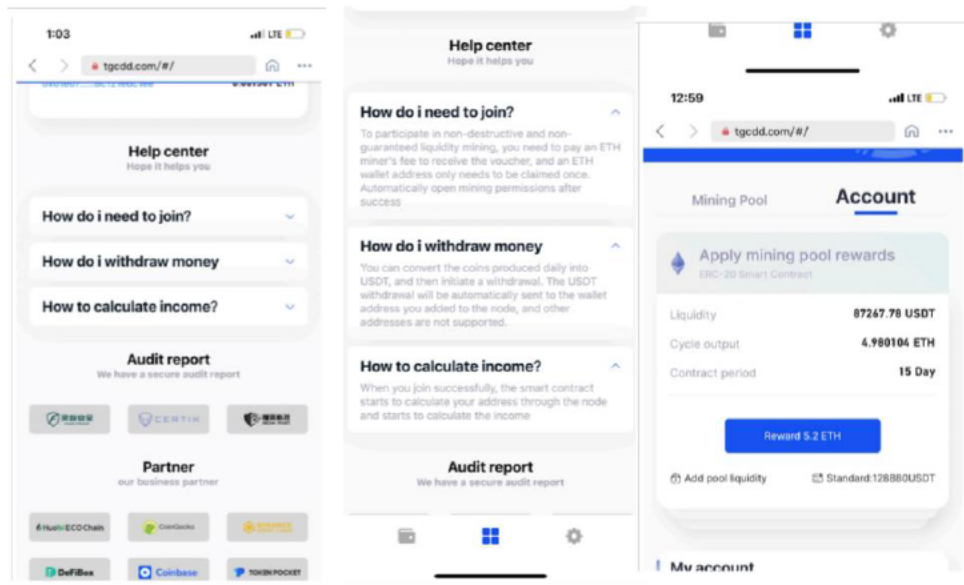
386. On November 1, 2021, Coinbase replied to Paparelli, informing him that his “recovery phrase has been compromised” even though he had not provided his security passphrase to anyone. Having received no assistance from Coinbase, Paparelli filed a formal complaint with Coinbase on November 22, 2021.

v. Grigore Rosca

387. On or about November 25, 2021, Grigore Rosca (“Rosca”) was contacted by woman named Monica on a social media application. Over time, Rosca and Monica chatted consistently and Rosca began to trust her based on the nature of their conversations.

388. After several conversation with the woman, Monica told Rosca about an investment that she had been successfully participating in, and invited Rosca to join a liquidity mining pool on Coinbase.

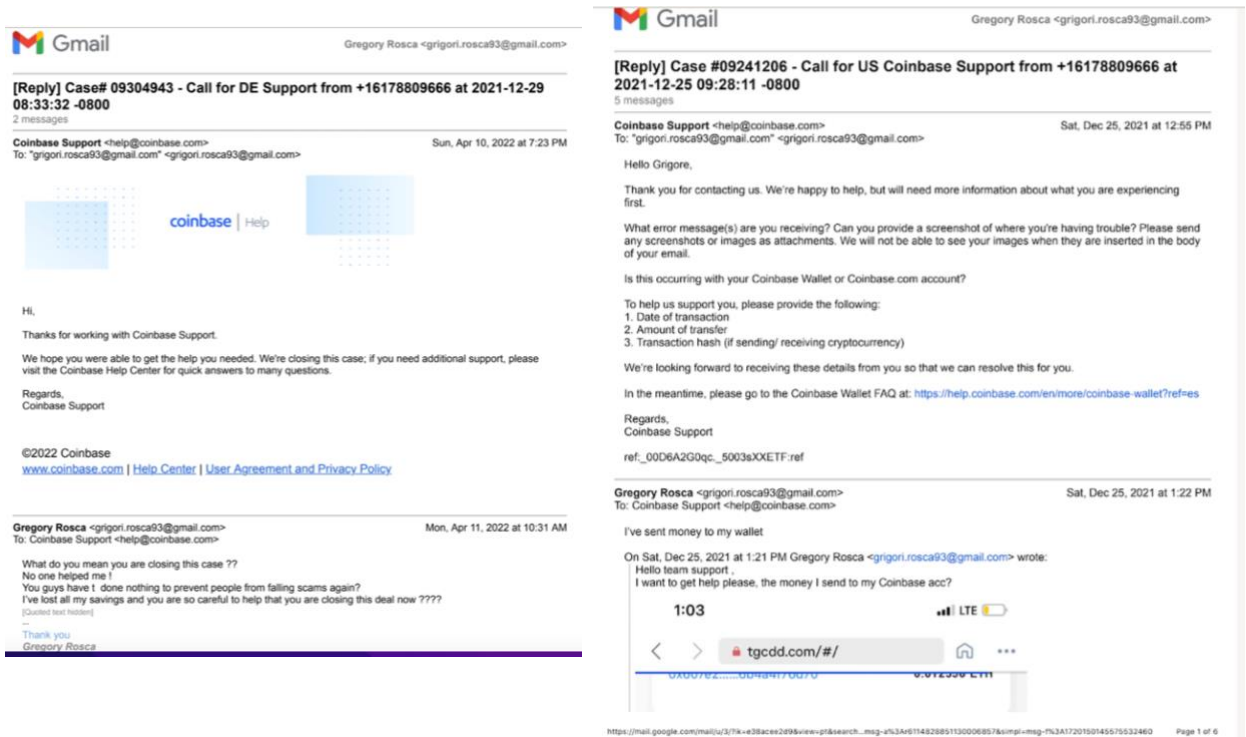
389. On or about November 30, 2021, Rosca was directed to enter into a smart contract through a node or voucher on a dapp called “tgcdd.com” in order to join a liquidity mining pool. Rosca did as he was instructed. The dapp named Coinbase as a “business partner.”



390. Unbeknownst to Rosca, the liquidity mining pool was a fraudulent scam.

391. Rosca subsequently made 6 deposits of USDT into his Coinbase Wallet between November 30, 2021 and December 24, 2021. On or about December 25, 2021, the defrauders utilizing the dapp on Coinbase’s platform drained Rosca’s entire Coinbase Wallet of all of his crypto assets by way of the fraudulent smart contract.

392. Rosca’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$88,400 USD, comprising Rosca’s entire personal savings accounts. The fraudulent withdrawal left Rosca in a significant savings deficit and has completely altered his life. He has experienced significant mental and emotional distress as a result of his victimization, including suicidal ideation.



393. Following the theft, Rosca immediately contacted Coinbase Support to report the fraudulent withdrawals (Case Nos. # 09304943, #09307048, #09311318, # 09244759, # 09304591).

394. In response to Rosca’s report of theft on Coinbase’s application, Coinbase Customer Support instructed Rosca to “reach out to the dapp” that had enabled the fraudulent activity.

395. After repeated attempts to get assistance from Coinbase to recover his losses, to no avail, Rosca filed a formal complaint with Coinbase on December 29, 2021. On January 7, 2022, Coinbase finally responded to Rosca’s complaint and informed him that “after a review, we’ve determined that Coinbase cannot recover or reverse the transactions in question” and “must deny your complaint.”

396. On January 24, 2022, Rosca requested that Coinbase at least deactivate the fraudulent browser on Coinbase Wallet. Almost two months later, Coinbase informed Rosca that they would flag

the dapp for its security and investigation team on March 13, 2022. On April 10, 2022, after Rosca continued to inform Coinbase that his matter had not been resolved, Coinbase closed Rosca’s complaint file.

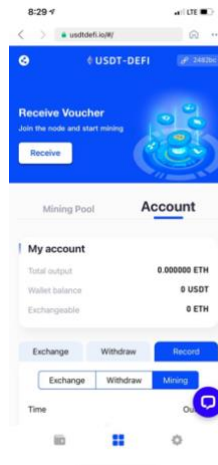
397. Rosca never believed—and had no reason to believe—that he had allowed the defrauder or anyone else access to the assets held in his Wallet. As such, his transactions were unauthorized. Indeed, Coinbase Wallet provided no warning to Rosca stating that anyone could access his Wallet to take his funds.

398. To the contrary, Coinbase Wallet’s disclosures instructed Rosca that the only way someone could take his funds was if his “seed phrase” was stolen or compromised.

w. Wai Chan

399. On or about October 13, 2021, Wai Chan (“Chan”) met an individual on a social dating application. Shortly thereafter, Chan and the man continued to communicate on WhatsApp, a social messaging application. The man told Chan about his successes mining crypt on Coinbase and extended an invitation to Chan to join a liquidity mining pool on Coinbase.

400. The man sent Chan a link to a dapp called “USDT-DEFI” and instructed Chan on how to open a Coinbase Wallet account. The man sent Chan money for the fee to pay for the dapp voucher.



401. On October 14, 2021, Chan, having been lulled into the pool, entered into a smart contract through a node or voucher in order to join the liquidity mining pool.

402. Chan made an initial investment of \$1,000 to test out the security of the dapp. Chan's funds appeared to be secure in his account and he was earning money back, so he decided to deposit more USDT into his Coinbase Wallet to contribute to the pool.

403. On or about November 1, 2021, Chan noticed that his Wallet had been emptied. He contacted the customer support agent through the dapp's chatroom. The agent informed Chan that his assets were contributed to the pool and in order to retrieve them and a bonus award he would have to increase his contribution.

404. Relying on the customer service agent, who he believed to be affiliated with Coinbase, Chan continued to make two additional contributions to his Coinbase Wallet on November 5, 2021 and November 8, 2021. Immediately after each deposit, his Wallet was drained through unauthorized transactions.

405. Between October 21, 2021 and November 8, 2021, Chan made seven deposits into his Coinbase Wallet. Chan incurred network fees for each deposit and transfer he made in furtherance of the liquidity pool operation.

406. After researching the liquidity mining pool, Chan learned from a thread on Reddit that the dapp was a scam and he realized he was a victim of fraud.

407. As a result of the Coinbase liquidity mining pool scam, Chan lost \$223,000 USDT, money he had saved over several years to purchase a home. Chan was devastated when he learned that he had been defrauded and has suffered emotional and physical distress as a result.

408. Chan contacted Coinbase to report the theft on or around April 17, 2022 (Case No. #11385905). Coinbase's response to Chan's report was entirely unhelpful. Coinbase informed Chan that it "remains the customer's responsibility to review the details of the dapps they interact with and understand the risk when interacting with them" and that Coinbase would not be able to reimburse or credit Chan's Wallet. Having received no assistance from Coinbase, Chan filed a report with the Federal Bureau of Investigation on November 17, 2021.

x. Jane Doe 2

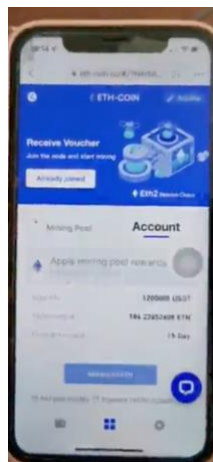
409. On or about November 28, 2021, Jane Doe 2 met a man on WeChat, a social messaging application. The man told Jane Doe 2 about his investment in a liquidity mining pool on Coinbase that

had earned him significant returns on his crypto investments. Jane Doe 2 was already a Coinbase customer at the time and believed that Coinbase was a reputable and safe platform for cryptocurrency transactions. Based on her reliance on Coinbase’s reputation, she trusted that any application used on its platform would be safe and legitimate.

410. The man, who Jane Doe 2 later learned was a scammer, informed all of her assets would remain in her Coinbase Wallet and would be “just as safe as a bank account.”

411. On or about December 2, 2021, Jane Doe 2 agreed to join the liquidity mining pool and was directed to access a dapp called “ETH-COIN” through her Coinbase Wallet application.

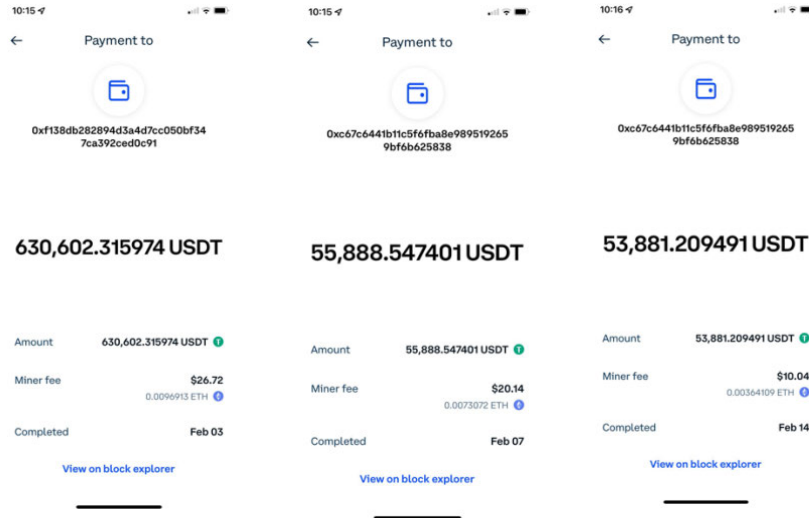
412. Unbeknownst to Jane Doe 2, by “joining the node” she had agreed to enter into a malicious smart contract that gave defrauders on the platform access to her entire Coinbase Wallet.



413. Between December 2, 2021 and February 14, 2022, Jane Doe 2 made seven deposits of USDT into her Coinbase Wallet account to participate in the mining pool. After Jane Doe 2 made her initial deposit of USDT into her Wallet, all her assets appeared to be secure and she was earning ETH automatically.

414. Jane Doe 2 even contacted the customer service agent through a chatroom on the dapp to inquire about the legitimacy of the dapp and the mining pool. The agent, who purported to be a Coinbase employee, assured Jane Doe 2 that the dapp was secure and she should not worry and Coinbase could handle any security issues.

415. Three fraudulent withdrawals were made through the dapp from Jane Doe 2’s Coinbase Wallet on February 3, February 7, and February 14, 2022.



416. On or around February 14, 2021, Jane Doe 2 realized that she was the victim of a fraudulent scam. She was shocked to learn that such activity was being facilitated on Coinbase’s application. When she conducted her own research, she learned that hundreds of other users had been defrauded using dapps on Coinbase.

417. Jane Doe 2’s losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$741,170.21 USDT. Jane Doe 2’s stolen assets were comprised of her life savings and funds she had set aside to refinance her home in hopes of a better life after retirement. As a result of the Coinbase Wallet scam, Jane Doe 2, age 53, now struggles to pay her mortgage and she will be saddled with debt well into retirement. In addition to the financial impact, Jane Doe 2 suffered significant emotional and mental anguish as a result of the fraudulent scheme, and at times contemplated suicide.

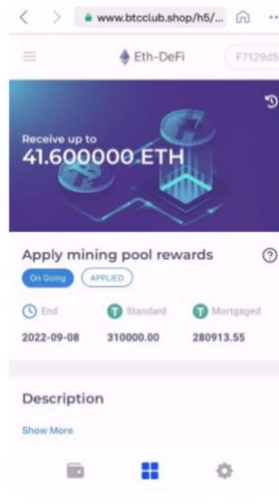
418. Immediately following the theft of her assets, Jane Doe 2 reached out to Coinbase’s customer support by email to report the theft and to inquire whether it was aware of the fraudulent application on its platform (Case No. # #10298568).

419. Coinbase’s customer support was entirely unhelpful and provided Jane Doe 2 with a generic response informing her that Coinbase would be “flagging the malicious dapp to [its] security and investigation teams” but that it “cannot reimburse or credit [her] wallet.”

y. Dominic Chow

420. On or about January 19, 2022, Claimant Dominic Chow (“Chow”) met an individual named Eileen Chou on WhatsApp, a social messaging platform, who told Chow about an investment opportunity using liquidity mining on Coinbase Wallet.

421. After months of deliberation, Chow decided to participate in the mining pool. The individual sent Chow a link to a dapp called www.btclub.shop (now www.btclubpro.com) and instructed him to join the pool through his Coinbase Wallet account. Chow did as he was directed and purchase a vouched for the pool on March 8, 2022.

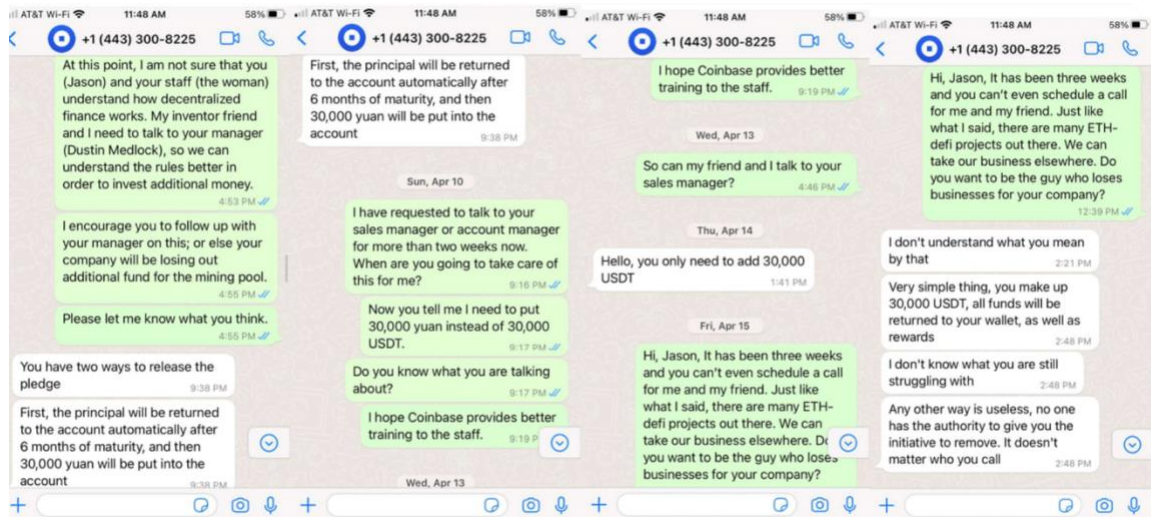


422. That same day, Chow deposited \$105,000 USD into his Coinbase Wallet. Shortly thereafter, Chow’s entire Wallet was emptied and sent to another address without his consent or authorization.

423. Chow had not provided the defrauder or anyone else with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

424. Chow immediately contacted the dapp’s customer support chat and was informed that he needed to contribute more money to into his Wallet to meet a \$280,000.00 USD threshold before he could retrieve his assets and obtain a reward. The dapp agent promised Chow that his funds would be returned to his Wallet within an hour of reaching the \$280,000 USD threshold. In hopes of recouping his funds, Chow continued to contribute to the mining pool.

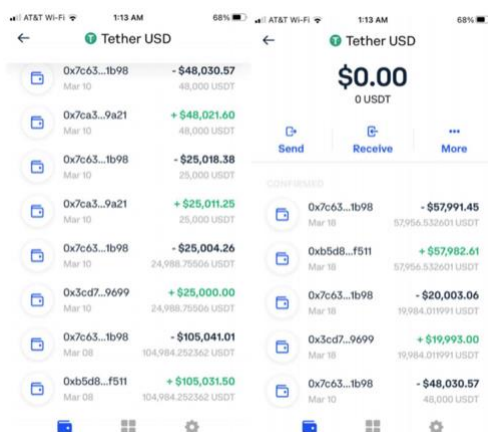
425. Between March 8, 2022 and March 18, 2022, Chow made 6 deposits of USDT into his Wallet to reach the \$280,000 USD threshold. On or around March 18, 2022, when Chow met the requisite contribution level, the account automatically increased his pledge threshold amount and request another \$300,000 USD deposit.



426. Chow even chatted via video chat with the dapp agent who claimed to be a Coinbase customer support agent. Shortly after speaking with the purported Coinbase agent, Chow's account was locked.



427. Chow's losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$280,914 USDT, comprised of funds withdrawn from his personal savings. These losses have greatly impacted his financial standing, including his retirement and child's education funding. In addition to the financial impact, Chow suffered significant emotional and mental anguish as a result of the fraudulent scheme.



428. On March 20, 2022, Chow attempted to contact Coinbase to report the theft (Case Nos. #10883672, #10885693, and #10885762). On each occasion, Coinbase responded to Chow’s complaint with general, boilerplate responses and instructed Chow that it would be “flagging this malicious dapp to [its] security and investigation teams” but “cannot reimburse or credit [Chow’s] wallet.” Coinbase’s response was wholly deficient and did not address Chow’s concerns or assist him in recouping his assets. Coinbase did not block or take down the malicious dApp.

z. Sabiha Goriawala

429. On or about December 16, 2021, Claimant Sabiha Goriawala (“Goriawala”) met a woman named “Melissa Zhang” on Reddit who told Goriawala and her son about a liquidity mining investment opportunity. Melissa and Goriawala communicated for weeks and Melissa eventually invited Goriawala to join the mining pool through a dapp called “Defi.cb-ed.net” on Coinbase.

430. On or about December 18, 2021, Goriawala opened the dapp browser through her Coinbase Wallet account and began making deposits of USDT into her Coinbase Wallet. Between December 18, 2021 and February 13, 2022, Goriawala made 5 deposits of USDT into her Coinbase Wallet.

431. Initially, Goriawala’s assets appeared to be secure in her Wallet and she and her son were earning ETH. After approximately two months of participating in the pool, Goriawala received an offer to earn 5 ETH by depositing an addition \$60,000 USDT. Melissa, who Goriawala and her son later learned was a scammer, encouraged her and her son to make the additional deposit. After selling

all of his crypto in order to meet the \$60,000 threshold, Goriawala's son deposited the USDT into Goriawala's Wallet and received a "miners fee" from the dapp.

432. No information was provided to Goriawala regarding the fee and there was no way to exit the fee screen. Goriawala attempted to restart the dapp and even uninstalled the Coinbase Wallet application to remove the screen, but to no avail.

433. Goriawala believed that the "miners fee" notice was a requirement of Coinbase because she was not able to remove it even after reinstalling the application.

434. On February 13, 2022, Goriawala's son clicked the "miners fee" button. The entire content of Goriawala's Coinbase Wallet was instantly emptied.

435. Goriawala's losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$55,000 USDT.

436. On February 13, 2022, Goriawala contacted Coinbase to report the unauthorized transfer (Case No. # 10266135). Coinbase customer support was entirely unhelpful.

437. On February 14, 2022, she received an automated, generic response from Coinbase Wallet's customer service stating that Coinbase could not do anything to address the fraud or reimburse her. Coinbase failed to address Goriawala's complaint or investigate the theft, leaving her with no recourse to remedy the fraudulent withdrawal.

438. Having received no assistance from Coinbase, Goriawala reported the theft to the FBI and the FTC.

aa. Manash Sharma

439. On or about March 16, 2022, Claimant Manash Sharma ("Sharma") matched with a woman named "Lorena Kuo" on a social dating app called "Plenty of Fish." Lorena continued to communicate on WhatsApp, a social messaging application. After some time, the two began to form a connection and Sharma grew to trust Lorena.

440. During the course of their conversations, Lorena mentioned that she invested in crypto as a hobby and that she could help him to invest. Lorena recommended that Sharma consider liquidity pool mining.

441. On or about March 21, 2022, Sharma agreed to join the liquidity mining pool using decentralized app through Coinbase Wallet called “ethcodefe.com”. Sharma initially deposited a small amount of money into his Coinbase Wallet to confirm that the pool worked as Lorena described. And initially it did – Sharma’s deposits remained in his Wallet amounts and he began earning interest on his deposited crypto.

442. A few weeks later, on March 23, 2022, Lorena pushed Sharma to deposit even more money into his Coinbase Wallet for the liquidity mining pool so that the two of them could “build a better future together.” Sharma agreed and deposited an additional \$18,604 USDT into his Wallet.

443. Lorena continued to insist that the liquidity mining pool would create a pathway for the to be financially successful as a coupe. Lorena even told Sharma that she had taken out a loan for \$50,000 to invest in the pool. When Lorena asked Sharma to increase his contribution, Sharma became skeptical and told her he needed more time to consider it. Lorena immediately resorted to manipulation tactics to guilt Sharma into contributing more money to the pool. After constant prodding by Lorena to increase his contribution, Sharma agreed to deposit another \$50,905.95 USDT on March 28, 2022.

444. After making his deposit on March 28, Lorena told Sharma to “pledge” all of his assets in his Wallet on the dapp. Sharma complied because he trusted Lorena and the pool had functioned as described until this point.

445. Immediately after pledging his assets, his Coinbase Wallet reflected a balance of zero; his crypto had been taken in an unauthorized transaction.

446. After discussing the investment further with Lorena, Sharma realized that he could not pull his deposited crypto until he met the “pledge total”, which was \$150,000 USDT. Sharma told Lorena that he would not be able to contribute that amount, as he had already depleted his total savings.



Lorena offered to ask a friend to contribute \$30,000 USDT if Sharma could contribute the balance. Lorena assured Sharma that once the pledge was reached, he would earn a reward of 22 ETH coins in addition to a large sum of interest.

447. On March 29, 2022, Lorena sent Sharma \$20,000 USDT to his Coinbase Wallet to add to the liquidity pledge. Sharma, in an attempt to retrieve the funds he had already contributed, agreed to contribute his last \$50,000 USDT toward the pool.



448. After conducting some additional research on his own, Sharma came to realize the dapp was a scam and that Lorena lured him into depositing his money into a fraudulent exchange. Sharma was devastated to learn that he had been lied to and manipulated by Lorena and defrauded on what he believed was a legitimate Coinbase application.

449. Coinbase Wallet provided no warning to Sharma stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet's disclosures instructed Sharma that the **only** way someone could take his funds was if his "seed phrase" was stolen or compromised.

450. Sharma's losses incurred as a result of the Coinbase Wallet liquidity pooling scheme total \$116,544.60 USD – his entire life savings. Sharma is now living paycheck to paycheck and saddled with financial anxiety about his future.

451. In addition to his grave financial loss, Sharma suffered significant physical (including hospitalization), mental and emotional distress as a result of the Coinbase liquidity mining pooling scam.

452. Following the thefts, Sharma contacted Coinbase customer support by email on to report the fraudulent dapp and attempt to recover his funds on March 29, 2022 (Case No. #11077561).

453. On March 29, 2022, Sharma received an unhelpful automated, generic response from Coinbase Wallet’s customer service stating that Coinbase could not do anything to address the fraud or reimburse him.

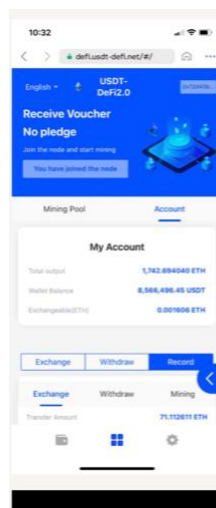
454. Coinbase informed Sharma that it was “flagging this malicious dapp to [Coinbase’s] security and investigation teams,” however the fraudulent dapp remained accessible on Coinbase for at least six months following Sharma’s report without any warning or flag to customers from Coinbase.

bb. Chengguo Dong

455. On or about October 26, 2021, Claimant Chengguo Dong (“Dong”) was approached by an individual on Line, a social media application.

456. The individual extended an invitation to Dong to join a liquidity mining pool on Coinbase aimed at mining USDT to gain interest. Dong, a Coinbase Wallet holder and developer, believed the operation was legitimate due to the dapp’s affiliation with Coinbase.

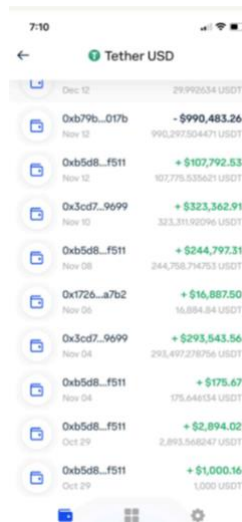
457. On or about October 27, 2021, Dong accessed a dapp called “defi.usdt-defi.net” through his Coinbase Wallet app and purchase a voucher to start liquidity mining. Dong had no idea that by purchasing the node, he had given away permission to a malicious third-party dapp to steal all his USDT from his Coinbase Wallet.



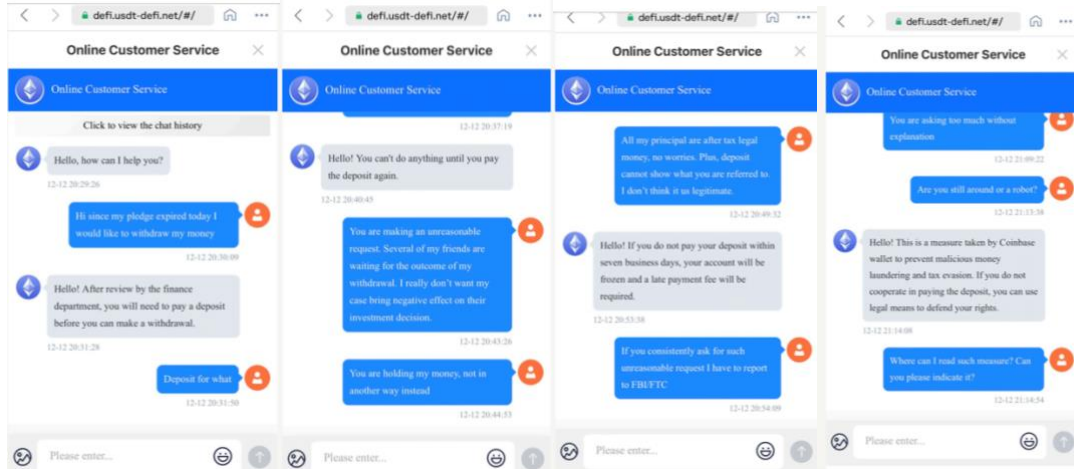
458. Coinbase Wallet provided no warning to Dong stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures instructed Dong that the *only* way someone could take his funds was if his “seed phrase” was stolen or compromised

459. Dong never provided anyone with his security passphrase and did not receive a notification from Coinbase Wallet to confirm that he had agreed to release the entirety of his asset from his Wallet by entering the smart contract.

460. Between October 29, 2021 and November 12, 2021, Dong made 7 deposits of USDT into his Coinbase Wallet to fund the liquidity pool. These assets were comprised of his life savings. On November 12, 2021, defrauders drained Dong’s entire Coinbase Wallet, leaving him with nothing.



461. After realizing that his Coinbase Wallet had been drained, Dong contacted the Online Customer Service chat through the dapp to request to withdraw his money after completing the pledge. The agent, holding himself out to be an employee of Coinbase, informed Dong that he would need to make an additional deposit of 426,182.19 USDT before he could withdraw his assets. Dong protested the additional deposit and the agent informed him that the dapp would freeze his account if he did not comply.



462. Dong's losses, totaling \$994,165 USD were financially devastating. As a result of the Coinbase Wallet liquidity pooling scam, Dong lives in financial precarity and had to withdraw money from his 401k to make ends meet. Dong's victimization at the hands of ruthless scammer has caused him significant emotional and mental suffering, including suicidal ideation.

463. On November 12, 2021, Dong promptly contacted Coinbase customer service to report the fraudulent activity (Case No. #08495237). In response, Coinbase failed to provide any assistance to Dong and instead informed him that Coinbase was not responsible for the loss and could not do anything to help him recover his funds. Over the course of a month, Dong continued to try to reach Coinbase for assistance however he repeatedly received generalized, automatic response which never addressed his dilemma, provided him a pathway to recover his funds, or ensured that other would not be victimized through the same fraudulent dapp.

464. Having received no assistance from Coinbase to recover his stolen assets, Dong filed a complaint with the California Department of Financial Protection on January 26, 2022. Dong also filed a complaint with the Department of Justice's Public Inquiry Unit.

465. Dong, a 50-year-old from Burlingame, California, who immigrated to the United States from China, lost his entire life savings of \$995,000. He had been planning to use the funds to purchase his family a home in California as well as pay his daughter's educational expenses.⁴¹ Losing his life

⁴¹ Although Dong will most likely never be able to purchase a home now due to the security flaws in the Wallet, Coinbase's CEO, Brian Armstrong, has not had such problems. Armstrong reportedly purchased a \$133 million home in Bel Air, California in December, 2021, the same time as Armstrong's customers' Wallets were being drained of their crypto due to the security flaw. *See*

savings has caused this victim tremendous harm, as he now has to withdraw money from his 401k account to support his family. Both this victim and his wife have been devastated by this loss, and their marriage is broken. This victim is very depressed, and there is not a day that goes by that he does not think about this traumatic scam. This victim feels that his life has been “completely ruined by this scam.”

cc. James Moskwa

466. On or around October 10, 2021, Claimant James Moskwa (“Moskwa”) was introduced to a woman named “Tresa” on Instagram. Over several weeks, Moskwa began to develop a friendship with Tresa. Moskwa and Tresa spoke often and she eventually brought up the topic of crypto investments. She told Moskwa that her uncle was assisting her in making investments. She told Moskwa that her uncle was a broker involved in a liquidity mining investment opportunity with Coinbase. Tresa convinced Moskwa to join Coinbase Wallet and participate in the mining pool investment as well. She eventually introduced Moskwa to her uncle describe the technicalities of the pool.

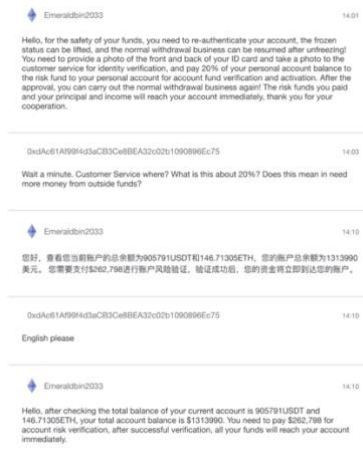
467. On or around November 1, 2021, Moskwa agreed to set up a Coinbase Wallet account and Tresa walked Moskwa through process of purchasing the voucher through a dapp called “Hydefico.com”. Moskwa purchased the voucher using ETH Tresa sent him.

468. On or about November 16, 2021, Moskwa started depositing USDT into his Coinbase account.

469. Between November 16, 2021 and January 21, 2022, Moskwa made six deposits into his Coinbase Wallet to participate in the pool.

470. Between December 24, 2021 through January 21, 2022, scammers withdrew all the USDT from Moskwa’s Wallet. The withdrawals were done without his permission or consent and without any notification, warning, or substantive response from Coinbase.

471. Shortly after the unauthorized withdrawal, Moskwa contacted the dapp’s customer service chat to inform them of the fraudulent withdrawals. The dapp’s customer service agent informed Moskwa that his account was temporarily frozen and he would have to deposit an addition \$262,798.00 for “account risk verification” in order to unfreeze his account and access his assets.



472. Fearful of losing the hundreds of thousands of dollars Moskwa had already deposited, he agreed to comply with the dapp’s request and continued to make additional deposits of USDT to meet the dapp’s various conditions for retrieval.

473. Moskwa lost \$1,417,654.06 USD because of the unauthorized transactions. The funds used by Moskwa to fund deposits made to the fraudulent pool were comprised of his life savings, retirement fund, proceeds from the sale of his personal assets and personal loans from friends. As a result of the scam, Moskwa has had to refinance his mortgage and incurred substantial tax penalties from premature withdrawals from his retirement accounts. The substantial financial loss has caused him significant emotional distress.

474. On or about February 2, 2022, Moskwa began to question the legitimacy of the dapp. On or about February 11, 2022 contacted Coinbase customer support to inquire about the dapp and inform it of the unauthorized withdrawals made from his Coinbase Wallet (Case No. # #10243360).

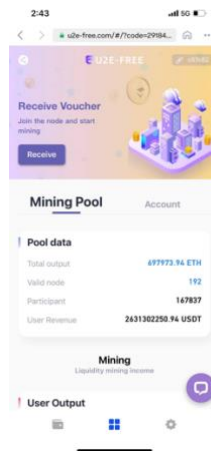
475. On or about February 14, 2022, Coinbase responded to Moskwa informing him that “https://hydefieco[.]com is a malicious dapp and is not in any way affiliated with Coinbase.” Although Coinbase was aware of fraudulent activity taking place through this dapp on its platform, it took no measures to warn customers like Moskwa about the dapp or the block customers from accessing the

dapp. Not only did Coinbase fail to warn Moskwa, but Coinbase denied any responsibility for Moskwa’s loss and informed him that it could not do anything to recover his funds. In addition, it does not appear that Coinbase took steps to block the malicious app, as the dapp was still active weeks later.

dd. Anh Nguyen

476. On or about October 16, 2021, Claimant Anh Nguyen (“Nguyen”) was contacted by a woman named “Teyana Cuffe” on Facebook. After befriending Nguyen, this individual informed him of an investment opportunity on Coinbase through a liquidity mining pool using defi platform called “U2E-FREE”.

477. Having convinced Nguyen that he could gain significant returns on USDT investments through the mining pool, “Teyana” directed Nguyen to open a link to the dapp he was sent and purchase a voucher to start mining. Nguyen was instructed that he had to link his Coinbase Wallet to the dapp and deposit USDT into his Coinbase Wallet in order to collect interest through the pool. On or about October 29, 2021, Nguyen did as he was instructed and purchased a voucher through the dapp. Unbeknownst to Nguyen, he had just entered into a malicious smart contract that allowed scammers direct access to the contents of his Coinbase Wallet.



478. Initially, the mining pool operated as described and Nguyen began to earn interest on his deposited USDT.

479. However, on or about October 29, 2021, all assets were removed from Nguyen’s Wallet by the dapp. When Nguyen inquired about the withdrawal, he was told by a customer service agent

associated with the dapp that his assets had been contributed to a “special pool” in order to yield higher earnings, but all of his funds were still in his Coinbase Wallet.

480. The customer service agent informed Nguyen that he needed to contribute at least \$200,000 USDT into his Coinbase Wallet in order to regain access to his assets and earn his reward.

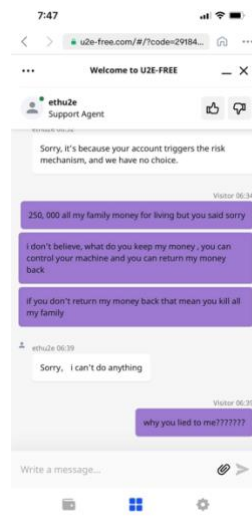
481. On or about October 31, 2021, Nguyen contacted Coinbase Support by email to inform it that his account had been hacked (Case No. #08206608). Coinbase responded and stated it would look into Nguyen’s account and instructed Nguyen to reset his Coinbase Wallet email and password. Nguyen did so, however, Coinbase never provided him with any further assistance in recovering his stolen assets.

482. Nguyen never provided anyone with the new security passphrase to his Wallet.

483. Having received no follow up from Coinbase’s customer support, and desperate to retrieve his funds, Nguyen decided to comply with the dapp agent’s directive to contribute additional USDT to the pool to gain access to his previously withdrawn funds.

484. On or about November 18, 2021, Nguyen deposited additional USDT into his Wallet to meet the \$200,000 USDT threshold requirement.

485. Immediately after his deposit amount reached \$200,000 USDT, Nguyen’s Wallet was drained again. When Nguyen contact the support agent again, he was told there was nothing he could do to retrieve his funds and days later his account was terminated.



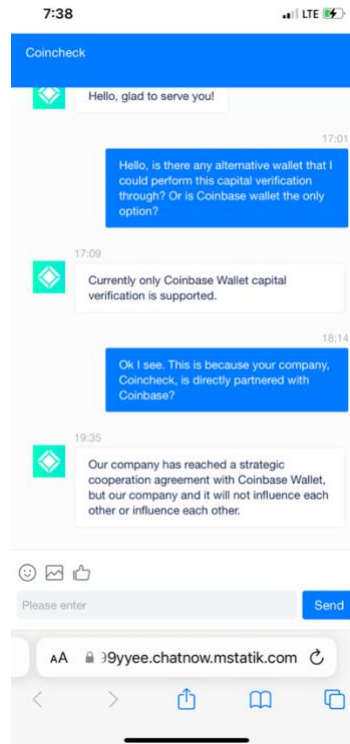
486. Nguyen lost \$222,946 USDT because of the unauthorized transactions made through the Coinbase Wallet scam.

487. The financial and emotional results of the loss have been devastating for Nguyen and his family, causing significant mental anguish and suicidal thoughts. Nguyen and his wife have lost the majority of their life savings and are struggling to make ends meet.

ee. Eisi Mollanji

488. On or about March 28, 2022, a person going by the name Aiden, who allegedly lived in Ottawa, contacted Claimant Eisi Mollanji (“Mollanji”) on the dating app Hinge. After befriending Mollanji, Aiden informed Mollanji about an opportunity to make huge profits through targeted swing trades on a platform called “Coincheck.” At Aiden’s insistence, Mollanji joined Coincheck and deposited \$60,000 USDT into Coincheck. Once Mollanji’s account reached \$120,000 USDT, Coincheck’s “customer service” contacted Mollanji and notified him that if he wanted to withdraw his funds, he would need comply with Coincheck’s money laundering regulations and show proof that he already held \$100,000 USDT so that Coincheck could verify that his crypto funds were not obtained via criminal activity. Aiden assured Mollanji that the same verification was required for all users.

489. Coincheck’s “customer service” informed Mollanji that Coincheck had a strategic cooperation agreement with Coinbase and that Mollanji would need to verify the proof of funds through the Coinbase Wallet app. Mollanji was desperate to get his money back and knew that Coinbase Wallet was a widely used platform that he considered to be secure, so he downloaded the Coinbase Wallet app and deposited \$100,471 USDT into his Wallet as instructed.



490. Coincheck’s “customer service” then directed Mollanji to visit the website daimakerdao.com through the Coinbase Wallet browser. Mollanji did as he was instructed.

491. Once on the daimakerdao.com site, Mollanji was directed to “join the node,” which Coincheck told him would be required, and pay the fee. Mollanji did as he was instructed. Once Mollanji informed Coincheck that he had completed the verification, within ten minutes he noticed that his USDT balance in his Coinbase Wallet was now \$0.

492. Mollanji never believed – and had no reason to believe – that he had allowed Aiden, Coincheck, or anyone else access to his funds in his Wallet. Indeed, Coinbase Wallet provided no warning to Mollanji stating that anyone could access his Wallet to take his funds. To the contrary,

Coinbase Wallet's disclosures told Mollanji that the *only* way someone could take his funds was if his "seed phrase" was stolen or compromised.

493. To verify his funds, Mollanji deposited a total of \$100,471 USDT into his Coinbase Wallet.

494. On or about April 20, 2022, scammers withdrew all of the USDT (approximately \$100,471) from Mollanji's Wallet. This withdrawal was done without Mollanji's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

495. Mollanji's life has been devastated because of this unauthorized transfer. Mollanji borrowed the money to fund his Coinbase Wallet from his professional student line of credit. These funds are essential to funding both his medical education and his costs of living while pursuing his medical degree. The fact that he has lost these funds not only places him in a huge amount of debt, but it also severely limits the remaining credit that he has left to make any large purchases that are essential to finish his last year of medical school and the start of his residency. Moreover, as a result of being scammed, Mollanji often finds himself unable to focus as his thoughts are fixated on the concern of his finances and frustration towards being powerless to do anything about it. This has negatively impacted his performance at work and his ability to study.

496. On April 20, 2022, the same day his funds were stolen, Mollanji notified Coinbase about the unauthorized transfer from his Coinbase Wallet (Case No. #11436630). Coinbase's responses were wholly inadequate and at times, non-sensical.

497. Coinbase responded to Mollanji's initial email with an auto-reply that it was "working hard to quickly address this issue, and we'll reach out to you as soon as we have an update." Immediately after receiving Coinbase's auto-reply, Mollanji informed Coinbase that he would "appreciate being able to speak to someone over the phone about this" and that he was "in a state of crisis right now and have not really had any questions answered or been given the opportunity to provide further details."

498. To expedite the process, Mollanji contacted Coinbase customer support by phone as well. In response to Mollanji's call, Coinbase requested additional information regarding Mollanji's

reported theft. Mollanji promptly provided Coinbase with the requested information detailing the fraudulent transaction.

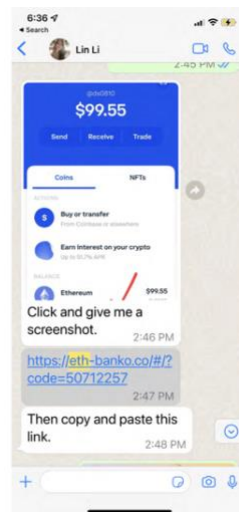
499. In response to Mollanji explanation that \$100,000 USDT was transferred from his account without his authorization, Coinbase replied to Mollanji with generic, boilerplate language regarding “fiat values for assets not being displayed in your Coinbase Wallet”— a topic completely unrelated to Mollanji’s issue.

500. After hours of email exchanges, Coinbase finally provided a response to Mollanji tethered to his actual issue, but stated that Coinbase was not liable for his loss and that “It’s the customer’s responsibility to review the details of the dapp they interact with and understand the risk when interacting with it.”

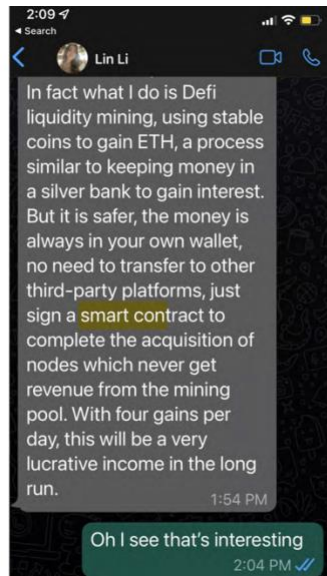
ff. Deepak Soneji

501. On or about November 27, 2021, Claimant Deepak Soneji was contacted by a woman named Lin Li or Evelyn Lee on Facebook. Lin Li invited Soneji to join a social group on Facebook. After befriending Soneji, Lin Li asked if she could message him on WhatsApp. Soneji and Lin Li began chatting and Lin Li told Soneji about her involvement in a liquidity mining pool investment opportunity on Coinbase.

502. Lin Li then directed Soneji how to download the Coinbase Wallet application and open the link for a dapp called ETH-BANKO using the Wallet’s browser. Soneji did as he was instructed.



503. On or about December 24, 2021, Soneji joined the mining pool. He paid the miner's fee to join with ETH sent to him by Lin Li. Soneji believed the dapp was a legitimate operation because the ETH-BANKO dapp listed Coinbase as a "business partner." At no time did Soneji believe that he had allowed Lin Li or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Soneji that anyone could access his Wallet to take his funds.



504. In fact, Lin Li told Soneji that no third party would be able to withdraw funds from his Wallet with his consent or initiation of the transfer.

505. Between December 24, 2021 and April 13, 2022, Soneji made 12 deposits of USDT into his Coinbase Wallet to fund the pool.

506. On or about March 6, 2022, scammers withdrew all the USDT (approximately \$607,592) from Soneji's Wallet. The unauthorized withdrawal was done without Soneji's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

507. On March 6, 2022, Soneji brought this matter to the attention of the customer support agent on the ETH-BANKO dapp, who Soneji believed to be affiliated with Coinbase. The agent informed Soneji that they would have to pay a "100,000 USDT tax" to withdraw his funds.

508. On or about March 10, 2022, Soneji contacted Coinbase Customer Service by email to inquire about the "tax" requested by the dapp (Case No. #10653554). Coinbase responded by informing him that it would flag the dapp, but Coinbase "cannot reimburse or credit [his] wallet." Soneji's contact with Coinbase's customer support was entirely unhelpful.

509. After receiving no meaningful response or assistance from Coinbase, Soneji decided to comply with the dapp's tax request as a last effort to recover his funds. On or about April 13, 2022, Soneji made a final deposit of \$106,762.78 USDT into his Wallet. Shortly after depositing his funds, the dapp withdrew the deposit, never giving Soneji an opportunity to recover any of his deposited funds.

510. Soneji lost \$607,592.78 USDT because of the unauthorized transactions.

511. Soneji has suffered serious emotion and mental anguish as a result of the theft and has lost over 80% of his life savings as a result of the Coinbase scam.

gg. Douglas Herring

512. On or about December 15, 2021, a woman contacted Claimant Douglas Herring ("Herring") on Instagram by commenting on one of his posts. After befriending Herring, the woman invited him to continue their conversations on WhatsApp. The woman informed Herring that her aunt had introduced her to a mining pool and she was earning significant income over Coinbase using a defi platform called CW-ETH (defi.cw-eth.net). The dapp listed Coinbase, as well as other known crypto platforms, as "business partners."

513. Having lulled Herring with the prospect of similar income, the woman directed Herring to download the Coinbase Wallet application and open the link for the CW-ETH dapp using the Wallet's browser. Herring did as he was instructed. The woman gave Herring the ETH necessary to pay the miner's fee to join the pool. On or about January 11, 2022, Herring unknowingly entered into a smart contract and linked his Coinbase Wallet to the fraudulent dapp.

514. At no time did Herring believe that he had allowed anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Herring that anyone could access his Wallet to take his funds.

515. To fund the pool, Herring made 5 deposits of USDT into his Coinbase Wallet between January 11 and 31, 2022.

516. Initially the pool operated as promised and Herring was still able to withdraw his funds. Based on this, he continued to make larger deposits of USDT into his Wallet to fund the pool.

517. On January 31, 2022, scammers withdrew all the USDT from Herring's Wallet. The withdrawal was done without Herring's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

518. Herring lost \$610,000 USD because of the unauthorized transactions. He is devastated and has been trying his best to pull himself out of depression. Herring has lost the majority of his savings and retirement fund as a result of the scam. This experience has caused him significant mental and emotional distress.

519. On or about February 1, 2022, Herring brought this matter to Coinbase's attention by phone (Case Nos. #09912641, #10013848). Coinbase's response to Herring's reported theft was wholly deficient. In response to Herring's detailed account of his loss, Coinbase customer support told Herring that there was nothing it could do to assist him or retrieve his funds.

hh. Sergey Demenko

520. On or about October 21, 2021, after hearing about an investment opportunity from his friend through a liquidity mining pool, Claimant Sergey Demenko ("Demenko") decided to join, what he and his friends thought was a legitimate defi platform, Eth-Base.

521. Being lulled with the prospect of similar earnings as his friend, on or around October 26, 2021, Demenko downloaded the Coinbase Wallet application and opened the link for Eth-Base.biz using the Wallet's browser.

522. At no time did Demenko believe that he had allowed anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Demenko that anyone could access his Wallet to take his funds.

523. To fund the pool, Demenko deposited a total of \$75,251 USDT into his Coinbase Wallet.

524. In November 2021, scammers withdrew all the USDT (approximately \$75,251) from Demenko's Wallet. The withdrawal was done without Demenko's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

525. The unauthorized transaction has caused Demenko and his family significant emotional stress and financial problems.

526. On March 23, 2022, Demenko brought this matter to Coinbase’s attention by email to Coinbase customer support (Case No. #08495237). On March 27 and March 29, 2022, Coinbase informed Demenko that it would be “flagging the malicious dapp to [its] security and investigation teams” and that there was nothing that Coinbase could do, that they took no responsibility, and suggested that Demenko should contact the FBI or attempt to “revoke” any approval of a fraudulent transaction but provided him with no instructions on how to do so.

ii. Jeffrey Osbun

527. On or about November 1, 2021, a person going by the name Maria, who allegedly lived in Los Angeles, CA, contacted Claimant Jeffrey Osbun (“Osbun”) on Hinge. After befriending Osbun, Maria informed Osbun that she was earning significant income over Coinbase using a defi platform called PhiCoinx.

528. Having lulled Osbun with the prospect of similar income, Maria directed Osbun to download the Coinbase Wallet application and open the link for uni-defi.com using the Wallet’s browser. Osbun did as he was instructed.



529. At no time did Osbun believe that he had allowed Maria or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Osbun that anyone could access his Wallet to take his funds.

530. To fund the pool, Osbun deposited a total of \$76,468 USDT into his Coinbase Wallet.

531. In November 2021, scammers withdrew all the USDT (approximately \$76,468) from Osbun's Wallet. The withdrawal was done without Osbun's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

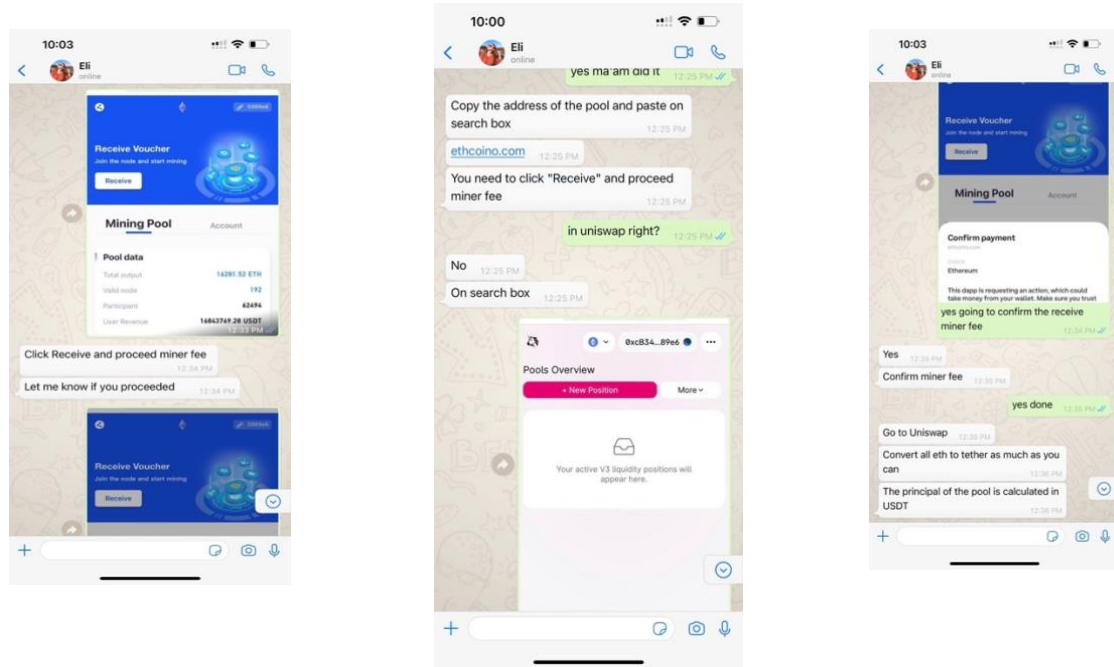
532. As a result of the unauthorized transaction, Osbun had to borrow money from his parents which has prevented his parents from purchasing a house. Osbun's health has also suffered as he suffers from symptoms of post-traumatic stress disorder. Osbun has also been forced to miss out on business opportunities because he can no longer afford to invest because of his lack of funds.

533. On November 19, 2021, Osbun brought this matter to Coinbase's attention through Coinbase customer support (Case No. #08620426), informing Coinbase that he was the victim of the "pig butchering scam". Rather than providing Osbun with any useful information to address the reported theft, Coinbase told him that it put a hold on his account's ability to login for the time being until he was certain that his account is secure. Even after Osbun complied with multiple emails from Coinbase requesting that he verify his account, Coinbase never responded to Osbun acknowledging the subject of his complaint and never provided any assistance to Osbun in recovering his stolen assets. For months afterward, the dapp remained active in the Wallet platform, indicating that Coinbase took no steps to remove or block the dapp after it was reported to Coinbase.

jj. Akshay Raghavendra

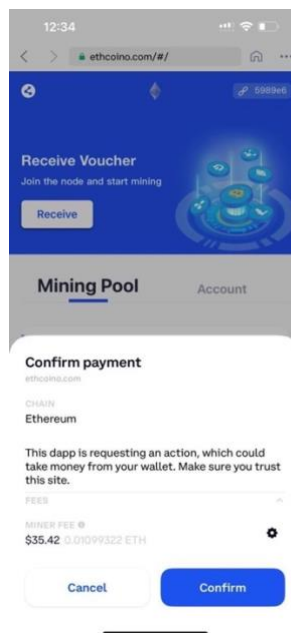
534. On or about January 13, 2022, a person going by the name Eli, contacted Claimant Akshay Raghavendra ("Raghavendra") on Tinder. After befriending Raghavendra, Eli informed Raghavendra that she was earning significant income at Coinbase Wallet using a defi platform called ethcoino.

535. Having lulled Raghavendra with the prospect of similar income, Eli directed Raghavendra to download the Coinbase Wallet application and open the link for ethcoino.com using the Wallet's browser. Raghavendra did as he was instructed.



536. Once on the fraudulent pool's site, Eli told Raghavendra to click receive and proceed to pay the miner fee. Raghavendra did as he was instructed, and this action most likely initiated the malicious smart contract.

537. During the process of joining the pool with the malicious, hidden smart contract, Raghavendra only received a warning that “This dapp is requesting an action, which could take money from your wallet” with a miner fee of \$35.42 listed below the warning. At no time did Raghavendra believe that he had allowed Eli or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Raghavendra that anyone could access his Wallet to take his funds. Raghavendra believed he was only paying the Miner Fee and not giving the scammers unlimited access to the funds in his Wallet.



538. To fund the pool, Raghavendra deposited a total of \$243,559 USDT into his Coinbase Wallet.

539. Between January 2022 and February 2022, scammers withdrew all the USDT (approximately \$243,559) from Raghavendra’s Wallet. The withdrawal was done without Raghavendra’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

540. Raghavendra lost his life savings due to this unauthorized transfer. The loss has deeply affected Raghavendra’s life, he is in substantial debt and is struggling to pay his mortgage and other loans.

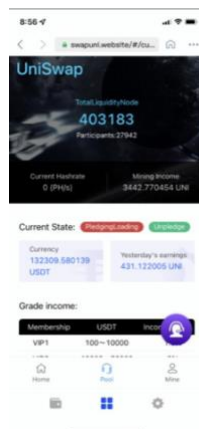
541. On August 14, 2022, Raghavendra contacted Coinbase’s customer support to notify Coinbase about the unauthorized transfer of USDT out of his Wallet (Case No. #12774272). Coinbase responded to Raghavendra’s complaint and informed him that it “takes these reports very seriously, and will be flagging this malicious dapp to our security and investigation teams”, that it “remains the customer’s responsibility to review the details of the dapps they interact with and understand the risk when interacting with them” and that Coinbase would not be able to reimburse or credit Raghavendra’s Wallet.

542. Coinbase suggested that if he had not “already done so, [Raghavendra] may want to report this incident to law enforcement agencies in your jurisdiction” and that he “can submit a report to the FBI Internet Crime Complaint Center (IC3)”

kk. Chris Elkins

543. On or about January 20, 2022, Claimant Chris Elkins (“Elkins”) visited the Coinbase website to learn more about liquidity mining pools. While on Coinbase’s website, Elkins navigated to the “Help & Learn” section where he discovered the fraudulent dapp, UniSwap (<http://swapuni.org>). Elkins conducted additional research and compared various dapps before agreeing to join the UniSwap mining pool.

544. After chatting with a customer service agent, the agent directed Elkins to download Coinbase Wallet application and open the link for the UniSwap dapp using the Wallet’s browser. Because Elkins found the information regarding the dapp on Coinbase’s website, he believed the liquidity mining operation to be legitimate.



545. On or about January 21, 2022, Elkins followed the instructions of the dapp agent and downloaded Coinbase Wallet and the dapp to begin mining.

546. At no time did Elkins believe that he had allowed anyone else access to the funds in his Wallet, and Coinbase provided no warning to Elkins that anyone could access his Wallet to take his funds.

547. Initially, Elkins made deposits of USDT into her Coinbase Wallet without issue and his funds appeared secure. Between January 21 and February 4, 2022, Elkins made approximately eleven deposits of USDT into his Coinbase Wallet to fund the mining pool.

548. On or around February 4, 2022, scammers withdrew all the USDT (approximately \$132,309) from Elkins' Wallet. The withdrawal was done without Elkins' permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

549. Elkins immediately brought this matter to Coinbase's attention in an email sent to Coinbase customer support (Case No. #10054559). In response, Coinbase assured Elkins that it takes "these reports very seriously and will be flagging the malicious dapp to our security and investigation teams." Coinbase made no attempt to assist Elkins in retrieving his stolen funds and took no responsibility for leading him and other customers directly to fraudulent dapps through its application. In addition, even though Elkins had provided the name of the malicious dapp to Coinbase so that others would not have their crypto stolen, Coinbase did nothing to block the dapp or take it down; the malicious dapp was up and running for months after it was reported.

550. As a result of the unauthorized transaction, Elkins lost \$132,337.52 USDT. Due to the loss, Elkins can no longer afford his home mortgage, lost the funds that he saved for his children's college tuition, and has suffered significant emotional distress.

II. Kathleen Warren

551. On or about December 2, 2021, a woman contacted Claimant Kathleen Warren ("Warren") on Instagram. After befriending Warren, the woman invited her to continue their conversations on WhatsApp. The woman informed Warren that she was earning significant income over Coinbase using a defi platform called CW-ETH (defi.cw.eth.net). The dapp listed Coinbase as a "business partner."

552. Having lulled Warren with the prospect of similar income, the woman directed Warren to download the Coinbase Wallet application and open the link for defi.cw-eth.net using the Wallet's browser. Warren did as she was instructed.

553. At no time did Warren believe that she had allowed anyone else access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Warren that anyone could access her Wallet to take her funds.

554. On or around January 19, 2022, Warren deposited USDT into her Coinbase Wallet. On or about January 20, 2022, purchased ETH to pay the miner's fee to begin investing in the mining pool. This action resulted in Warren entering into a smart contract that would later provide scammers access to the assets in her Coinbase Wallet.

555. On or around January 26, 2022, scammers withdrew all the USDT (approximately \$111,051) from Warren's Wallet. The withdrawal was done without Warren's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

556. As a result of the unauthorized transaction, Warren suffered a significant financial loss, which has greatly impacted her financial stability and ability to retire and caused her emotional and mental distress.

557. On or around January 27, 2022, Warren contacted Coinbase customer support by phone to bring the theft to Coinbase's attention (Case No. #09884280). During the phone call, Coinbase accused Warren, without any factual basis, of compromising her security passphrase despite her insistence that she had not shared the passphrase with anyone. Coinbase never asked Warren about the details of her transaction or the dapp scam. On the following day, Coinbase sent Warren regarding the wrong transaction, completely ignoring the fraudulent transaction that she had reported the prior day, and explained that Coinbase would not "cancel, reverse, or recover these funds on [her] behalf." Coinbase never provided Warren with applicable guidance to recover her funds and closed her case without further response.

mm. Henry Chen

558. On or about January 17, 2022, a person going by the name Jenny, who allegedly lived in Richmond, CA, contacted Claimant Henry Chen ("Chen") on Hinge. After befriending Chen, Jenny

informed Chen that she was earning significant income over Coinbase using a defi platform called DeFi Mining.

559. Having lulled Chen with the prospect of similar income, Jenny directed Chen to download the Coinbase Wallet application and open the link for defi.usd-defi.org using the Wallet's browser. Chen did as he was instructed.

```
17:18 Jenny I like to learn and try new things so that I can make progress.
17:19 Jenny You can go to the app store to download coinbase wallet. Now, after registration,
I'll teach you the next steps.
17:19 Henry Chen I'm not exactly off work yet... I'm here for another hour and a half
17:19 Henry Chen Mind if I bug you around then??
17:20 Jenny Don't mind
17:20 Jenny Well, it's actually very simple, if you're smart enough, it only takes a few minutes.
17:34 Henry Chen Apparently 6 mins total
17:34 Jenny haha
17:35 Jenny Have you downloaded and registered yet?
17:38 Henry Chen I'm adding payment method
17:39 Jenny I'm talking about coinbase wallet, not coinbase.
17:40 Henry Chen Oh dang
17:40 Jenny Coinbase is used to buy and trade coins, and wallet is used to store and mine coins.
They are different apps, but they belong to the same company.
17:40 Henry Chen Hold on!
17:41 Henry Chen I've been meaning to buy an offline wallet for my coins
17:41 Henry Chen Or coin?
17:42 Jenny I used usdt to mine ETH in my wallet.
17:43 Jenny It is very stable and the income is good. I think it is a better choice than holding
coins.
```

560. Once on the fraudulent pool's site, Jennie directed Chen to purchase a node that would allow him to join the mining pool. Chen did as he was instructed, and this action most likely initiated the malicious smart contract.

```
18:02 Jenny https://defi.usd-defi.org
18:03 Henry Chen Fascinating!!
18:03 Jenny Copy the link to it and save the bookmark so that you can make it easier next time.
18:05 Henry Chen Saved!!
18:05 Jenny screenshot
18:08 Henry Chen [Photo]
18:08 Jenny [Photo]
18:08 Jenny Click to receive the mining voucher and join the mine pool node.
18:09 Henry Chen I don't have my coins in my wallet yet
18:09 Jenny Yes, I forgot, the first time to get the voucher, you need to pay ETH miner fee,
which is about 30 US dollars, it only needs to pay once.
18:10 Henry Chen Got it
18:10 Jenny Don't worry, it only takes a few minutes.
18:11 Jenny You need to send another ETH of about $30 to your wallet to collect the voucher.
18:12 Jenny ETH doesn't need to send a lot, $30 should be enough.
18:12 Henry Chen Got it
```

561. At no time did Chen believe that he had allowed Jennie or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Chen that anyone could access his Wallet to take his funds.

562. To fund the pool, Chen deposited a total of \$121,516 USDT into his Coinbase Wallet.

563. Between January 2022 and March 2022, scammers withdrew all the USDT (approximately \$121,516) from Chen's Wallet. The withdrawal was done without Chen's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

564. As a result of the unauthorized transaction, Chen is forced to live on the margins of what he can afford in the San Francisco Bay area. His mother lost her job during the pandemic, so he

is the sole bread winner in the household. It has been a tremendous challenge for Chen to figure out how to move from here.

565. On or about March 12, 2022, Chen brought this matter to the attention of the SEC and the California Department of Financial Protection and Innovation (“CA DFPI”). The CA DFPI then submitted a complaint on his behalf to Coinbase.

566. On April 28, 2022, Coinbase emailed Chen a response to his complaint with DFPI. Coinbase informed Chen that after reviewing his complaint with the DFPI, that while sympathetic, Coinbase is not in a position to recover any funds that you send off of the Coinbase platform.

567. Coinbase denied liability, informing Chen that its “Terms of Service for the Wallet application are clear that when using a dapp or other Third Party Materials, you understand that you are at no time transferring your assets to us” and that Coinbase does “not have control over their content, do not warrant or endorse, and are not responsible for the availability or legitimacy of, the content, products or services on or accessible from those Third Party Materials.”

nn. Jun Zhai

568. On or about February 23, 2022, a person going by the name “Julie”, who allegedly lived in Seattle, Washington, contacted Claimant Jun Zhai (“Zhai”) on WeChat. Julie told Zhai that she was in the cosmetic surgery industry and was working from San Diego, California on a business trip. After befriending Zhai, Julie told him about her hobbies and informed Zhai that she had joined and was earning significant income over Coinbase in an ETH mining pool on dapp called defi.ethereumt.net. Zhai believed the mining operation was legitimate based on its presence on the Coinbase platform.

569. Having lulled Zhai with the prospect of similar income, Julie directed Zhai to download the Coinbase Wallet application and open the link for defi.ethereumt.net using the Wallet’s browser. On or about February 28, 2022, Zhai did as he was instructed, and purchased a voucher to begin transferring funds into his Wallet.

570. At no time did Zhai believe that he had allowed Julie or anyone else access to the funds in his Wallet, and Coinbase Wallet provided no warning to Zhai that anyone could access his Wallet to take his funds.

571. Between March 2 and March 22, 2022, Zhai made four deposits of \$71,075 USDT into his Coinbase Wallet to fund the pool.

572. On or about April 5, 2022, scammers withdrew all the USDT (approximately \$71,075) from Zhai's Wallet. The withdrawal was done without Zhai's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

573. On April 18, 2022, Zhai brought this matter to Coinbase's attention and was told that there was nothing that Coinbase could do, that they took no responsibility, and suggested that Zhai contact the FBI. At least until June 2022, Coinbase also did not block or put warnings signs up about the scam dApp.

574. As a result of the Coinbase scam, Zhai lost \$71,075 USDT, comprised of his entire retirement fund and life savings. Since falling victim to the unauthorized transfer, Zhai has trouble sleeping at night and is emotionally depressed, which has negatively impacted his job performance.

oo. Eric Wong

575. In December 2021, a friend introduced Claimant Eric Wong ("Wong") to the fraudulent liquidity mining pool that he was also scammed into joining called <https://defi.ethereum-eth.cc>. Wong joined the liquidity mining pool because his friend convinced him that he was earning a substantial amount of income using the defi platform.

576. After being lulled with the prospect of similar income, Wong joined the pool. At no time did Wong believe that he had allowed anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Wong that anyone could access his Wallet to take his funds.

577. To fund the pool, Wong deposited a total of \$92,455 USDT into his Coinbase Wallet.

578. Between January and February 2022, scammers withdrew all the USDT (approximately \$92,455) from Wong's Wallet. The withdrawal was done without Wong's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

579. On or around August 1, 2022, Wong contacted Coinbase customer service to report his stolen assets (Case No. #12661557). Unhelpfully, Coinbase informed Wong that it "takes these reports very seriously, and will be flagging this malicious dapp to our security and investigation teams", but that it "remains the customer's responsibility to review the details of the dapps they interact with and

understand the risk when interacting with them” and that Coinbase would not be able to reimburse or credit his Wallet.

pp. Bryce Richmond

580. On or about October 29, 2021, a person going by the name Yumiko Miyami, contacted Claimant Bryce Richmond (“Richmond”) on Facebook. After befriending Richmond, Yumiko informed Richmond that she was earning significant income over Coinbase using a defi platform called Aaveeth.

581. Having lulled Richmond with the prospect of similar income, Yumiko directed Richmond to download the Coinbase Wallet application and open the link for aaveeth.xyz using the Wallet’s browser. Richmond did as he was instructed.

582. Once on the fraudulent pool’s site, Yumiko directed Richmond to purchase a certificate that would allow him to join the mining pool. Richmond did as he was instructed, and this action most likely initiated the malicious smart contract.

583. After meeting Yumiko, a person going by the name Bonnie Lee, who allegedly lived in Malibu, contacted Richmond on Facebook. Bonnie befriended Richmond by telling him that Aaveeth was a scam and that he should invest in ETH-Coin instead.

584. Having lulled Richmond with the prospect of similar income and showing him that Aaveeth was a scam, Bonnie directed Richmond to open the link for eth-coin.co using the Wallet’s browser and join Eth-Coin. Richmond did as he was instructed.

585. Once on the fraudulent pool’s site, Bonnie directed Richmond to purchase a certificate that would allow him to join the mining pool. Richmond did as he was instructed, and this action most likely initiated the malicious smart contract.

586. At no time did Richmond believe that he had allowed Yumiko, Bonnie, or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Richmond that anyone could access his Wallet to take his funds.

587. To fund the pool, Richmond deposited a total of \$235,000 USDT into his Coinbase Wallet.

588. In December 2021, scammers withdrew all the USDT (approximately \$155,000) from Richmond's Wallet. The withdrawal was done without Richmond's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

589. In January 2022, scammers again withdrew all the USDT (approximately \$80,000) from Richmond's Wallet. The withdrawal was done without Richmond's permission or consent. It was done without any notification, warning, or substantive response from Coinbase.

590. Richmond's life has been devastated. He is now in significant debt and owes on his credit cards, bank loans, and lost a substantial portion of his retirement funds.

591. Following the fraudulent withdrawal, Richmond brought this matter to Coinbase's attention and Coinbase told him that it was not responsible for his losses and could not recover his funds.

qq. Richard Wisinszky

592. On or about January 8, 2022, a person going by the name Elena, who allegedly was from Lucerne, contacted Claimant Richard Wisinszky ("Wisinszky") on Instagram. After befriending Wisinszky, Elena informed Wisinszky that she was earning significant income over Coinbase using a defi platform called ETH-Coinpool.

593. Having lulled Wisinszky with the prospect of similar income, Elena directed Wisinszky to download the Coinbase Wallet application and open the link for eth-coinpool.com using the Wallet's browser. Wisinszky did as he was instructed.

10:31 PM Richard Wisinszky On which platform do you trade?

10:32 PM Elena I use coinbase wallet

10:32 PM Richard Wisinszky That's good!

10:32 PM Elena All my USDT is in my coinbase wallet

10:32 PM Elena coinbase is a very safe cryptocurrency marketplace

10:33 PM Richard Wisinszky I also have Kraken for my business

10:33 PM Elena It is the largest cryptocurrency company in the world

10:33 PM Richard Wisinszky Yes it's very safe

10:34 PM Elena I currently hold over about 500kUSDT

10:34 PM Elena I am currently using my USDT for liquidity mining

10:34 PM Elena Every day I can make a steady profit

07:53 PM Elena Now I take you to the ethernet mining pool

07:53 PM Richard Wisinszky I'm excited (Excited)

07:53 PM Elena [Photo]

07:56 PM Elena screenshot

07:57 PM Richard Wisinszky [Photo]

07:58 PM Elena eth-coinpool.com

07:58 PM Elena This is the link to enter the ethernet mining pool, you copy and fill in the place I circled, then enter


07:58 PM Elena [Photo]

07:59 PM Richard Wisinszky [Photo]

07:59 PM Elena [Photo]

08:00 PM Elena This is the ethernet mining pool, you click, and then bookmark it for easy access next time

08:01 PM Elena I'll take you to see the daily income after becoming a miner when it's done

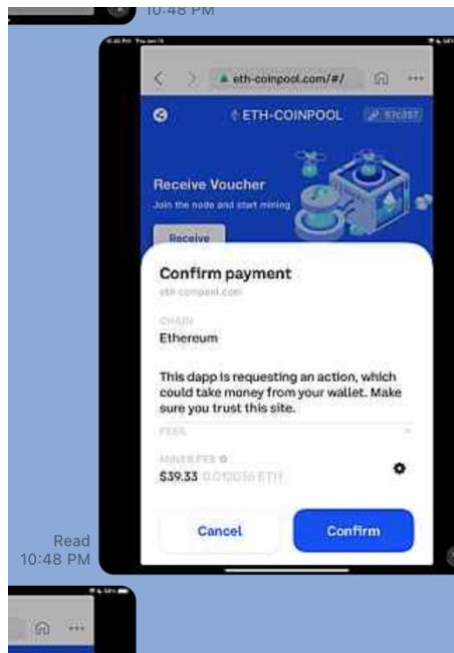
08:01 PM Richard Wisinszky Ok bookmark 

08:01 PM Elena [Photo]

08:02 PM Elena Swipe to the bottom, I will take you to see the daily income after becoming a miner

594. Once on the fraudulent pool's site, Elena directed Wisinszky to purchase a "miner certificate" that would allow him to join the mining pool. Wisinszky did as he was instructed, and this action most likely initiated the malicious smart contract.

08:10 PM Elena Do you know how to become a miner?
08:10 PM Richard Wisinszky No 😞
08:11 PM Elena [Photo]
08:11 PM Elena Come back here, I will teach you how to get the miner certificate
08:12 PM Richard Wisinszky Danke schön!
08:12 PM Elena This is just a sharing between friends, I believe that when you have a good project, you will also share it with me
08:13 PM Elena It's all open, transparent, and everyone can participate
08:13 PM Richard Wisinszky Of course I will!
08:14 PM Elena [Photo]
08:15 PM Richard Wisinszky Ok so I have transfer some ETH from the exchange
08:15 PM Elena After clicking here to get the miner certificate, you will become a miner, and then you can put in USDT to automatically earn profits every day
08:15 PM Richard Wisinszky Do you know how much?
08:15 PM Richard Wisinszky [Photo]
08:16 PM Elena To get the miner certificate, you need to pay the ETH miner fee of about \$50, let the global miners broadcast and record that we also become a miner



595. At no time did Wisinszky believe that he had allowed Elena or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Wisinszky that anyone could access his Wallet to take his funds.

596. To fund the pool, Wisinszky deposited a total of \$78,246 USDT into his Coinbase Wallet.

597. On January 24, 2022, scammers withdrew all the USDT (approximately \$78,246) from Wisinszky's Wallet. The withdrawal was done without Wisinszky's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

598. Upon the loss of the majority of his life savings and his inheritance from his father, Wisinszky's life has been devastated. Wisinszky has had sleepless nights and he is in a deep depression. He is constantly concerned with how he will earn some of the money he lost back.

599. On February 16, 2022, Wisinszky contacted Coinbase's customer support to notify Coinbase about the unauthorized transfer of USDT out of his Wallet (Case No. #10330518). Coinbase's customer support was entirely unhelpful.

600. Coinbase responded to Wisinszky's complaint and informed him that it "takes these reports very seriously, and will be flagging this malicious dapp to our security and investigation teams", that it "remains the customer's responsibility to review the details of the dapps they interact with and understand the risk when interacting with them" and that Coinbase would not be able to reimburse or credit his Wallet.

rr. John Doe 2

601. On or about March 30, 2022, a person going by the name Emily, who allegedly lived in San Jose, contacted Claimant John Doe 2 on Hinge. After befriending John Doe 2, Emily informed John Doe 2 that she was earning significant income over Coinbase using a defi platform called defi.wallet.

[3/30/22, 8:58:08 PM] Emily: You can search and download [coinbase](#) wallet in the mobile phone store. [coinbase](#) wallet is a wallet owned by [coinbase](#).
[3/30/22, 8:58:49 PM] Emily: Ha ha, this is a woman's sixth sense 😊
[3/30/22, 9:00:28 PM] Emily: Therefore, only the right people can stay together for a long time and more interesting things can happen.
[3/30/22, 9:18:02 PM] [REDACTED] Ok, I'll download it tonight. I'm just about to finish cooking dinner
[3/30/22, 9:18:33 PM] [REDACTED] Hahaha this is hilarious 😂 you're teaching me about a lot of things!
[3/30/22, 9:18:54 PM] [REDACTED] I agree!
[3/30/22, 9:19:03 PM] [REDACTED] What kind of food do you like?
[3/30/22, 9:20:27 PM] Emily: Wow, how did you get to dinner now? Irregular diet is very bad for your health.
[3/30/22, 9:21:00 PM] Emily: I like sushi, egg yolk shrimp, hot pot
[3/30/22, 9:22:25 PM] Emily: OK, let me know when you download it, and I will give you the most suitable advice. 😊
[3/30/22, 9:42:51 PM] [REDACTED]: Yes, I never usually eat dinner now. I had to pick up my dog and when I came home from the gym I forgot I hadn't defrosted the chicken 😊
[3/30/22, 9:43:18 PM] [REDACTED] I made pretty good chicken Parmesan though!
[3/30/22, 9:44:09 PM] [REDACTED] Nice, so you mainly like Asian foods. I think you'll like the Bay Area. Have you had Korean barbecue? There is a really good restaurant in San Jose
[3/30/22, 9:44:20 PM] [REDACTED] Downloading it now!

602. Having lulled John Doe 2 with the prospect of similar income, Emily directed John Doe 2 to download the Coinbase Wallet application and open the link for defi.wallet—defi.org using the Wallet’s browser. John Doe 2 did as he was instructed.

603. Once on the fraudulent pool’s site, Emily directed John Doe 2 to purchase a node that would allow him to join the mining pool. John Doe 2 did as he was instructed, and this action most likely initiated the malicious smart contract.

604. At no time did John Doe 2 believe that he had allowed Emily or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to John Doe 2 that anyone could access his Wallet to take his funds.

605. To fund the pool, John Doe 2 deposited a total of \$102,800 USDT into his Coinbase Wallet.

[3/30/22, 10:13:28 PM] Emily: If you need a coin-digging bookmark for your wallet, I will give you a coin-digging bookmark for your wallet and you can use it.
[3/30/22, 10:14:31 PM] ██████████ <attached: 00000139-PHOTO-2022-03-30-22-14-31.jpg>
[3/30/22, 10:15:05 PM] ██████████ 😊
[3/30/22, 10:15:11 PM] Emily: <attached: 00000141-PHOTO-2022-03-30-22-15-11.jpg>
[3/30/22, 10:15:18 PM] Emily: <https://defi.wallet--defi.org>
[3/30/22, 10:15:29 PM] Emily: Copy the coin-digging bookmark of this wallet,
[3/30/22, 10:15:43 PM] Emily: Then paste him here and give me a screenshot after entering,
[3/30/22, 10:16:58 PM] Emily: Have you seen the mine pool of your wallet?
[3/30/22, 10:17:14 PM] ██████████ <attached: 00000146-PHOTO-2022-03-30-22-17-14.jpg>
[3/30/22, 10:17:21 PM] Emily: 😊
[3/30/22, 10:17:31 PM] ██████████ I get this message, does that mean I need to add money?
[3/30/22, 10:17:46 PM] Emily: Because your wallet doesn't have enough ETH, you can't get your coin-digging node voucher, hahaha,
[3/30/22, 10:18:15 PM] Emily: It doesn't matter. I can give you some ETH, about \$30 ETH, and you can get your coin-digging node certificate.
[3/30/22, 10:18:36 PM] ██████████ Oh, is that it?
[3/30/22, 10:18:46 PM] Emily: But when you start digging coins, you have to give them back to me or invite me to dinner, 😊

606. In April 2022, scammers withdrew all the USDT (approximately \$102,800) from John Doe 2’s Wallet. The withdrawal was done without John Doe 2’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

607. John Doe 2 now suffers from anxiety induced depression and is an emotional wreck. It will take him years to recover from the unauthorized transfer both emotionally and financially. It is the first thing he thinks about when he wakes up in the morning and the last thing he thinks about before going to bed.

608. On April 12, 2022, John Doe 2 contacted Coinbase’s customer support to notify Coinbase about the unauthorized transfer (Case No. #11343037). On April 14, 2022, Coinbase emailed

John Doe 2 and informed him that “[s]ince your wallet is a user-controlled and non-custodial product, meaning that only you have full control/access (including the recovery phrase), Coinbase doesn’t have any access to your 12 key seed phrase therefore we cannot transfer or move any funds on your behalf.”

John Doe 2 replied back to Coinbase requesting that it help transfer his Coinbase Wallet assets. Coinbase replied that because his “wallet is a user-controlled and non-custodial product, meaning that only you have full control/access (including the recovery phrase), we cannot provide any additional details about how it was compromised” and suggested that contact the FBI.

ss. Kelly Schmittel

609. On or about April 25, 2022, a person going by the name Darlene, who allegedly lived in Los Angeles, contacted Claimant Kelly Schmittel (“Schmittel”) via text message. After befriending Schmittel, Darlene informed Schmittel that she was earning significant income over Coinbase using a defi platform called Layer2.

610. Having lulled Schmittel with the prospect of similar income, Darlene directed Schmittel to download the Coinbase Wallet application and open the link for eth-layer2.vip using the Wallet’s browser. Schmittel already had a Coinbase Wallet but was not using it the time because he was not active in crypto investing, but following Darlene’s instructions he used his Coinbase Wallet to visit the fraudulent mining pool.

4/28/22, 10:40 AM - +1 (424) 688-0401: It sounds good, but the income is not very stable, I can get \$3500 in income every day when I do liquidity mining
4/28/22, 10:40 AM - +1 (424) 688-0401: 120k income per month
4/28/22, 10:41 AM - Kelly: Stable income sounds more fun than gambling.
4/28/22, 10:42 AM - +1 (424) 688-0401: I only do stable financial management
4/28/22, 10:42 AM - +1 (424) 688-0401: You can download a crypto exchange and coinbase wallet first, I can teach you how to enter

611. Once on the fraudulent pool's site, Darlene directed Schmittel to purchase a node that would allow him to join the mining pool. Schmittel did as he was instructed, and this action most likely initiated the malicious smart contract.

```
5/6/22, 8:08 PM - +1 (424) 688-0401: eth-layer2.vip
5/6/22, 8:09 PM - +1 (424) 688-0401: The link I sent you, you copy and paste it into the link.
5/6/22, 8:09 PM - Kelly: IMG-20220506-WA0014.jpg (file attached)
5/6/22, 8:10 PM - +1 (424) 688-0401: <Media omitted>
5/6/22, 8:10 PM - +1 (424) 688-0401: Click the circled one, and this is the node voucher.
5/6/22, 8:10 PM - +1 (424) 688-0401: You only need to pay a little fee.
5/6/22, 8:12 PM - Kelly: I clicked recieve, paid a few bucks and it's at same screen
5/6/22, 8:13 PM - +1 (424) 688-0401: Yes, you will receive the node voucher when you pay
successfully.
5/6/22, 8:14 PM - Kelly: Where do I recieve node voucher? I paid and nothing happened?
5/6/22, 8:14 PM - +1 (424) 688-0401: Now go back to the homepage of Coinbase wallet, and I'll teach
you how to convert ETH into USDT, because we use USDT to generate revenue.
5/6/22, 8:15 PM - Kelly: Ok
```

612. At no time did Schmittel believe that he had allowed Darlene or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Schmittel that anyone could access his Wallet to take his funds.

613. To fund the pool, Schmittel deposited a total of \$233,000 USDT into his Coinbase Wallet.

614. In May 2022, scammers withdrew all the USDT (approximately \$233,000) from Schmittel's Wallet. The withdrawal was done without Schmittel's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

615. Schmittel's life has been devastated as a result of the unauthorized transaction. He initially felt that he was at risk of losing his family over the loss. Now, he is battling depression and constantly thinks about the loss and how he may never recover from the financial loss.

616. On May 25, 2022, Schmittel contacted Coinbase's customer support to notify Coinbase about the unauthorized transfer. Instead of conducting an investigation, Coinbase replied by informing Schmittel that "if you did not confirm any outgoing transactions from your Wallet, we regret to inform you that this means the funds and seed phrase are now compromised" and that Coinbase is "unable to provide specific details on how your Wallet was compromised" nor can Coinbase "recover the funds in these instances."

617. On May 26, 2022, Coinbase emailed Schmittel again to inform him that it takes "these reports very seriously, and will be flagging this malicious dapp to our security and investigation

teams.” Schmittel replied back to Coinbase’s email and provided the wallet addresses used in connection with the scam and requested that Coinbase help him recover any portion of the funds stolen.

618. On May 28, 2022, Coinbase emailed Schmittel and informed him that “After an extensive review of the transaction details, your Wallet’s history, and the addresses associated with it, the unauthorized activity you reported appears to have resulted from a signed transaction that approved a malicious third party to transfer funds from your Wallet on May-07-2022... .” Coinbase then provided Schmittel with the approval transaction from the malicious smart contract and told him that this “transaction gave the address 0xdac17f958d2ee523a2206206994597c13d831ec7 access to the funds held inside your Coinbase Wallet.” Coinbase did not acknowledge whether the approved transaction compromised Schmittel’s recovery phrase.

tt. Phuong Thanh

619. On or about July 21, 2021, a person going by the name David contacted Claimant Phuong Thanh (“Thanh”) on Tinder. After befriending Thanh, David informed Thanh that he was earning significant income over Coinbase using a defi platform called Eth-Defi29.

620. Having lulled Thanh with the prospect of similar income, David directed Thanh to download the Coinbase Wallet application and open the link for eth-defi29.com using the Wallet’s browser. Thanh did as she was instructed.



621. Once on the fraudulent pool's site, David directed Thanh to purchase a voucher that would allow her to join the mining pool. Thanh did as she was instructed, and this action most likely initiated the malicious smart contract.

622. At no time did Thanh believe that he had allowed David or anyone else access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Thanh that anyone could access her Wallet to take his funds.

623. To fund the pool, Thanh deposited a total of \$225,000 USDT into her Coinbase Wallet.

624. In November 2021, scammers withdrew all the USDT (approximately \$225,000) from Thanh's Wallet. The withdrawal was done without Thanh's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

625. On September 1, 2022, Thanh called Coinbase customer support to report the stolen funds (Case No. #12941895). In response, Coinbase replied to Thanh by email regarding "missing USDT & ETH" despite Thanh's report that these assets were stolen through a dapp on Coinbase's platform. Rather than provide Thanh with any guidance on how to retrieve her funds, Coinbase reminded Thanh that "Coinbase Wallet is a user-controlled, non-custodial product" and requested that Thanh provide "screenshots/screen recordings of where [she is] having trouble."

626. As a result of the scam, Thanh lost \$225,000 USDT, which included all of her life savings. As a result, her health has deteriorated and she cannot eat or sleep.

uu. Dalton Green

627. On or about December 4, 2021, after hearing about an investment opportunity that was earning significant income from his friends, Claimant Dalton Green ("Green") decided to join, what he and his friends thought was a legitimate defi platform, ETH-defi.

628. Having lulled Green with the prospect of similar income, Green downloaded the Coinbase Wallet application and opened the link for eth-defis.co using the Wallet's browser.

629. Once on the fraudulent pool's site, Green purchased a voucher that would allow him to join the mining pool, and this action most likely initiated the malicious smart contract.

630. At no time did Green believe that he had allowed anyone access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Green that anyone could access his Wallet to take his funds. At no time was Green's seed or recovery phrase compromised.

631. To fund the pool, Green deposited a total of \$71,096 USDT into his Coinbase Wallet.

632. In December 2021, scammers withdrew all the USDT (approximately \$71,096) from Green's Wallet. The withdrawal was done without Green's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

633. Green's life has been devastated both financially and emotionally. The financial loss has caused a great deal of stress on his marriage and he has suffered from a spiraling depression. His wife, an active-duty soldier, no longer trusts him financially and the couple has lost the down payment for their house. He is constantly worried that the loss has caused irreparable damage to their relationship, which is on the verge of collapse, that can only be rectified by receiving reimbursement for their loss.

634. On August 8, 2022, Green brought this matter to Coinbase's attention and Coinbase told him that it "flagged this malicious web3 site to our security and investigation team" and that after "an extensive review of the transaction details provided, the unauthorized activity you reported appears to have resulted from a signed transaction that approved a malicious third party to transfer funds from your Wallet on" December 8, 2021. Moreover, Coinbase told Green that as "coinbase Wallet is a non-custodied product, at no point has Coinbase ever had access to your Wallet or funds, and Coinbase plays no role in transactions authorized and signed by the user" and that because "transaction via Coinbase Wallet take place directly on the blockchain, it is not possible to revert them or recover the funds once you have signed the transaction and they are confirmed." Green also reported the theft to the US Secret Service, who was much more helpful, and immediately traced the crypto to Singapore.

vv. Yao Li

635. On or about January 3, 2022, Claimant Yao Li was contacted by a friend who claimed to have earned significant income over Coinbase using a defi platform called GMD Coin (<https://eth-mining001.com>).

636. Having enticed Li with the prospect of similar income, Li's friend directed him to download the Coinbase Wallet application and open the link for dapp using the Wallet's browser. Li did as he was instructed.

637. Once on the fraudulent pool's site, Li purchased a node that would allow him to join the mining pool. This action most likely initiated the malicious smart contract that would give scammers unauthorized access to the contents of Li's Wallet.

638. At no time did Li believe that he had allowed anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Li that anyone could access his Wallet to take his funds.

639. Between January 7 and January 26, Li made four deposits of USDT into his Coinbase Wallet to fund the liquidity mining pool.

640. On or around January 29, 2022, scammers withdrew all the USDT (approximately \$80,000) from Li's Wallet. The withdrawal was done without Li's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

641. As a result of the scam, Li lost \$80,000 USDT. This financial loss greatly impacted his financial stability and caused Li significant emotional and mental distress.

642. On or around October 3, 2022, Li contacted Coinbase customer support to report the stolen assets and request guidance from Coinbase on how to retrieve his funds (Case No. #13254903). Rather than providing Li with relevant information to address his concerns, Coinbase responded to Li with an unhelpful email containing generic language instructing Li how to "view [his] balances and transactions." Coinbase never provided Li with assistance in recouping his stolen assets.

ww. Ethan Dang

643. On or about October 13, 2021, a person going by the name June aka Liu Qinn contacted Claimant Ethan Dang ("Dang") on Plenty of Fish. After befriending Dang, June informed Dang that she was earning significant income over Coinbase using a defi platform called usdtdefi.

644. Having lulled Dang with the prospect of similar income, June directed Dang to download the Coinbase Wallet application and open the link for usdtdefi.net using the Wallet's browser. Dang did as he was instructed.

645. Once on the fraudulent pool's site, June directed Dang to purchase a node that would allow him to join the mining pool. June sent Dang \$52 in Eth to pay for the fee. Dang did as he was instructed, and this action most likely initiated the malicious smart contract.

646. At no time did Dang believe that he had allowed June or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Dang that anyone could access his Wallet to take his funds.

647. To fund the pool, Dang deposited a total of \$438,756 USDT into his Coinbase Wallet.

648. On November 2, 2021, scammers withdrew all the USDT (approximately \$438,756) from Dang's Wallet. The withdrawal was done without Dang's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

649. Dang has lost his life savings as well as some of his family's money. He now owes two family members \$45,000.00. He can no longer provide for his twin twelve-year-old children. He is now depressed and has sleepless nights.

650. Following the fraudulent withdrawal, Dang brought this matter to Coinbase's attention by multiple emails to Coinbase's customer service (Case Nos. # #08286356, #08498957, #08497996, #08780020). On or around November 12, 2021, Coinbase responded to Dang's complaint, informing him that his "account was escalated for review to restore your ability to make purchases and deposits. It has been determined that your account is not eligible for a review at this time. However, you can contact us after December 12, 2021, and we can submit your account for a review at that time."

651. Dang replied to Coinbase's email asking if Coinbase was serious that he would have to wait a month for Coinbase to review his complaint about the loss of his life savings? On December 8, 2021, Coinbase replied to Dang and notified him that it was "working hard to quickly address this issue, and we'll reach out to you as soon as we have an update." On December 9, 2021, Coinbase updated Dang that it had "temporarily locked your account to protect you while we confirm that your devices and email are secure" but did not mention anything about the \$438,000 unauthorized transaction. On December 9, 2021, Dang contacted Coinbase again and inquired about "the status and whereabouts of the USDT balance of over \$438,000 that was removed from my Coinbase Wallet on 11-02-2021 and today, 12-09-2021... ."

652. On December 12, 2021, Dang emailed Coinbase again and stated that “It has been over a month since my USDT balance of over \$438,000 was illegally moved out of my Coinbase Wallet account and Coinbase still has not given me a valid reason.” On December 15, 2021, Coinbase responded to Dang and asked him to answer several questions related to his account, including “Have you provided your login information to a third party, or has a third party ever had access to your account?”

653. Finally, on December 20, 2021, Coinbase contacted Dang and told him that it “advise ceasing any additional engagement with this scam, and we recommend reporting it to the law enforcement agencies in your country.”

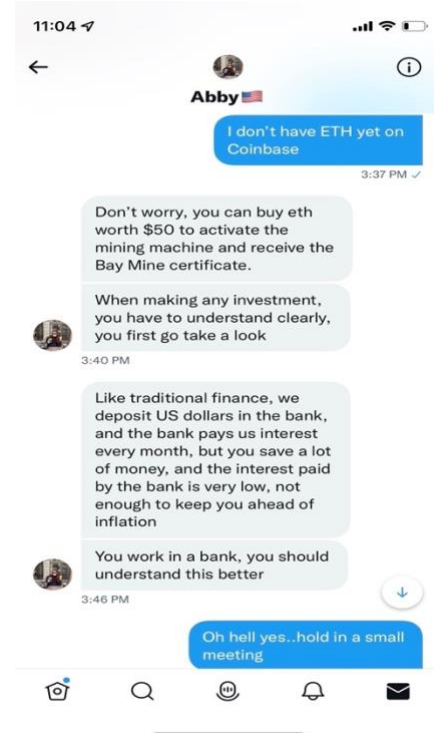
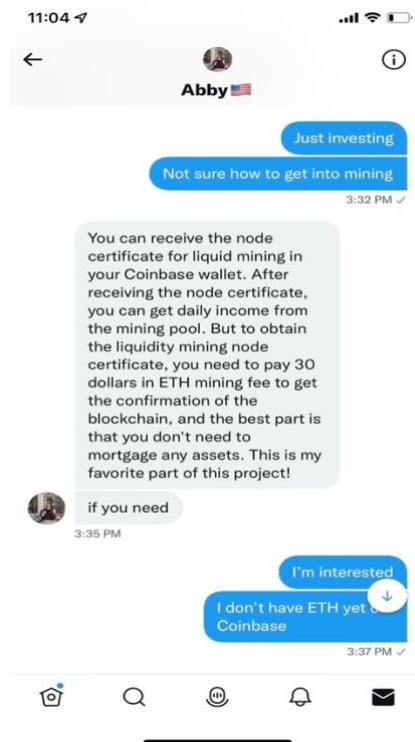
654. Instead of investigating Dang’s claim, Coinbase’s customer support was entirely unhelpful, froze his account in response to his reported complaint, and did not provide Dang with any useful assistance for recovering the loss of his life savings for over a month after his initial complaint.

xx. Trevor Lau

655. In January 2022, a person going by the name Abby, who allegedly lived in San Francisco, contacted Claimant Trevor Lau (“Lau”) on Twitter. After befriending Lau, Abby informed Lau that she was earning significant income over Coinbase using a defi platform called Bellapro.xyz.

656. Having lulled Lau with the prospect of similar income, Abby directed Lau to download the Coinbase Wallet application and open the link for Bellapro.xyz using the Wallet’s browser. Lau did as he was instructed.

657. Once on the fraudulent pool’s site, Abby directed Lau to purchase a node that would allow him to join the mining pool. Lau did as he was instructed, and this action most likely initiated the malicious smart contract.



658. At no time did Lau believe that he had allowed Abby or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Lau that anyone could access his Wallet to take his funds.

659. To fund the pool, Lau deposited a total of \$250,327 USDT into his Coinbase Wallet.

660. In January 2022, scammers withdrew all the USDT (approximately \$250,327) from Lau's Wallet. The withdrawal was done without Lau's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

661. Lau has lost his life savings. He is no longer able to buy a home and does not have any savings for emergencies.

662. On August 8, 2022, Lau brought this matter to Coinbase's attention via email sent to Coinbase customer service (Case Nos. # 08710919, #08882306). In response to Lau's complaint, Coinbase told him that its "team is working hard to answer customer inquiries in a timely manner, but you may experience longer response times." On August 9, 2022, Coinbase emailed Lau and informed him that it "take[s] these reports very seriously, and will be flagging this malicious dapp to our security and investigation teams" but "we cannot reimburse or credit your wallet." Moreover, Coinbase told Lau that "[i]t remains the **customer's responsibility to review the details of the dapps they interact**

with and understand the risk when interacting with them.” (emphasis in original). Finally, Coinbase suggested that Lau contact the FBI.

yy. DongDong Li

663. On or about March 3, 2022, a woman going by the name Emily contacted Claimant DongDong Li (“Li”) on TanTan. After befriending Li, Emily informed Li that she was earning significant income over Coinbase using a defi platform called Sushidexfi.

664. Having lulled Li with the prospect of similar income, Emily directed Li to download the Coinbase Wallet application and open the link for sushidexfi.com using the Wallet’s browser. Li did as he was instructed.

665. Once on the fraudulent pool’s site, Emily directed Li to purchase a node that would allow him to join the mining pool. Li did as he was instructed, initiating a malicious smart contract which allowed defrauders to access Li’s Coinbase Wallet.

666. In years prior, Li had been introduced to a similar dapp investment product by another woman named Amy, who he met in 2020 on a social dating app called Coffee Meets Bagel. Li had been communicating with Amy for almost two years. It was not until Emily mentioned investing in a dapp product that Li agreed to join the dapp investment offered by Amy. Having been invited to join the mining pool investment opportunities by two different women, Li believed it was a low likelihood that this was a scam.

667. After convincing Li to join the mining pool, Amy directed him to open the defi-eth-usdt.com URL through his Wallet’s browser. Li did as he was instructed and joined

668. At no time did Li believe that he had allowed Emily, Amy or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Li that anyone could access his Wallet to take his funds.

669. To fund the pool, Li deposited a total of \$132,702 USDT into his Coinbase Wallet.

670. In April 2022, scammers withdrew all the USDT (approximately \$132,702) from Li’s Wallet. The withdrawal was done without Li’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

671. On April 15, 2022, Li contacted Coinbase’s customer support to inquire about a transfer from his Coinbase Wallet (Case No. #11378410). Coinbase replied and informed Li that “According to our records, it appears the transaction in question has been successfully completed... .” Li replied that he “strongly believe my funds were stolen because the transaction was reflected in my wallet for a very short time if it’s not a system error.” Li informed Coinbase that the transaction was for around \$81,000 and provided a timeline of events. Li followed up and informed Coinbase that it “seems the funds were transferred out from my wallet 2 minutes after I transferred into my wallet. However, I didn’t authorize this transaction.”

672. Li followed up with an additional update, he alerted Coinbase to the fact that the funds in his Wallet were for mining purposes and that he was using the defi-eth-usdt.com mining pool. Coinbase responded by alerting Li that it “takes these reports very seriously, and will be flagging this malicious dapp to our security and investigation teams” and that Coinbase “cannot reimburse or credit your wallet.”

673. Li followed up by requesting the results of the investigation. Coinbase replied by informing Li that “After an extensive review of the transaction details, your Wallet’s history, and the addresses associated with it, the unauthorized activity you reported appears to have resulted from a signed transaction that approved a malicious third party to transfer funds from your Wallet on 2022-03-20 01:18:37.” Moreover, Coinbase denied responsibility and told Li that it could not cancel or reverse the transaction. Coinbase provided Li with instructions on how to revoke the smart contract, which Li followed and Coinbase confirmed that the contracts were revoked.

674. Li has lost his life savings plus money that he borrowed from his parents. The money he borrowed from his parents was for them to pay off their mortgage before they retired. His parents now blame him for them having to continue to work. Li has taken a medical leave from work due to the stress caused by his loss.

zz. Richard Slavant

675. On or about September 27, 2021, a woman contacted Claimant Richard Slavant (“Slavant”) on WhatsApp. After befriending Slavant, the woman informed him that she was earning significant income over Coinbase using a defi platform called ethusdt.buzz and ethusdt.xyt.

676. Having lulled Slavant with the prospect of similar income, the woman directed Slavant to download the Coinbase Wallet application and open the link for the dapp using the Wallet's browser. Slavant did as he was instructed.

677. Once on the fraudulent pool's site, the woman directed Slavant to purchase a node that would allow him to join the mining pool. On or about October 8, 2021, Slavant did as he was instructed, and unknowingly initiated a malicious smart contract.

678. At no time did Slavant believe that he had allowed the woman or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Slavant that anyone could access his Wallet to take his funds.

679. Between October 9 and November 9, 2021, Slavant made four deposits of USDT into his Coinbase Wallet to fund the pool.

680. On or about November 13, 2021, scammers withdrew all the USDT from Slavant's Wallet. The withdrawal was done without Slavant's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

681. As a result of the scam, Slavant lost approximately \$52,380.02 USDT, comprised of funds from loans and other personal savings. The Coinbase scam has been devastating to Slavant, both financially and emotionally, and resulted in significant distress.

682. On or about November 16, 2021, immediately after Slavant realized he was the victim of a fraudulent scam, he contacted Coinbase customer service to report the theft (Case Nos. #09674657, #08544174, #08554881). In response, Coinbase informed him that he should "reach out to the Dapp developer" directly to address his issue, despite having informed Coinbase that the dapp had facilitated the fraudulent withdrawal. After receiving additional emails from Coinbase with information unrelated to Slavant's issue, Coinbase replied on November 19, 2021 to inform Slavant that it cannot help recover his funds and he should report the incident to law enforcement.

aaa. Xiaoli Yuan

683. On or about November 11, 2021, a person going by the name Linzi, who allegedly lived in Canada, contacted Claimant Xiaoli Yuan ("Yuan") and her husband on TikTok. After befriending

Yuan and her husband, Linzi informed them that she was earning significant income over Coinbase using a defi platform called Eth-Starfish.

684. Having lulled Yuan with the prospect of similar income, Linzi directed Yuan and her husband to download the Coinbase Wallet application and open the link for eth-starfish.com using the Wallet's browser. Yuan did as instructed.

685. Once on the fraudulent pool's site, Linzi directed Yuan to purchase a node that would allow him to join the mining pool. Yuan did as she was instructed, and this action most likely initiated the malicious smart contract.

686. At no time did Yuan believe that she had allowed Linzi or anyone else access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Yuan that anyone could access her Wallet to take her funds.

687. To fund the pool, Yuan deposited a total of \$48,992.65 USDT into her Coinbase Wallet.

688. On or around December 17, 2021, scammers withdrew all the USDT (approximately \$48,992.65) from Yuan's Wallet and all the USDT (approximately \$34,082.07) from Song's Wallet. The withdrawal was done without Yuan's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

689. Yuan's life has been devastated. Since she has lost so much, she has been constantly depressed and is worried about being able to provide for their child who is currently in college with a four-year subsidy.

690. On December 17, 2021, Yuan brought this matter to Coinbase's attention via email to Coinbase Customer Service (Case No. #10449662), explaining the nature of the fraudulent dapp, including pictures of their transactions on Coinbase. On December 20, 2021, Coinbase responded to Yuan's complaint insinuating that her recovery passphrase had been shared with someone else and Coinbase "cannot provide any details about how [her recovery passphrase] was compromised" and could not reverse or cancel the transaction. Neither Yuan nor her husband ever provided the scammers or anyone else with their Coinbase recovery passphrase.

691. On December 22, 2021, Yuan contacted Coinbase again to inform it that their funds had been stolen from their Wallet and that they reported the theft to local law enforcement.

692. Coinbase's response was entirely unhelpful. Coinbase reiterated its prior generic,

收件人: Coinbase Support <help@coinbase.com>

Hello

This afternoon, I have reported these 2 cases to the San Bernardino County Police Department, and to the FBI Internet Crime Complaint Center (IC3) in the evening. These 2 cases involved me and my wife's Coinbase Wallet being manipulated by others and be stolen, with a total loss of more than \$82,600.

Coinbase claimed in the email that the loss in this case has nothing to do with Coinbase. The key is kept by the user personally. However, there are obvious technical loopholes in the Coinbase Wallet APP, which allows a third party to use the link to steal our wallet key and steal our money. Coinbase cannot shirk its responsibility. Please cooperate with the police in the investigation and properly handle our losses.

If your company's technicians need the invitation link provided by the criminal party, I can provide it so that your company can fix loopholes in time to prevent criminals from committing crimes again and harm more people.

I'm appreciate for your help.

automated language regarding Yuan's recover passphrase and stated that Coinbase "cannot reimburse or credit [her] Coinbase Wallet" Despite numerous attempts by Yuan to contact Coinbase customer support, Coinbase never provided her or her husband with any meaningful assistance in recovering their stolen assets.

bbb. Zhangting Song

693. On or about November 11, 2021, a person going by the name Linzi, who allegedly lived in Canada, contacted Claimant Zhangting Song ("Song") and his wife on TikTok. After befriending Song and his wife, Linzi informed them that she was earning significant income over Coinbase using a defi platform called Eth-Starfish.

694. Having lulled Song with the prospect of similar income, Linzi directed Song and his wife to download the Coinbase Wallet application and open the link for eth-starfish.com using the Wallet's browser. Song did as instructed.

695. Once on the fraudulent pool's site, Linzi directed Song to purchase a node that would allow him to join the mining pool. Song did as he was instructed, and this action most likely initiated the malicious smart contract.

696. At no time did Song believe that he had allowed Linzi or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Song that anyone could access his Wallet to take his funds.

697. To fund the pool, Song deposited a total of \$34,082.07 USDT into his Coinbase Wallet.

698. On or around December 17, 2021, scammers withdrew all the USDT (approximately \$34,082.07) from Song's Wallet. The withdrawal was done without Song's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

699. Song's life has been devastated. Since he has lost so much, he has been constantly depressed and is worried about being able to provide for his child who is currently in college with a four-year subsidy.

700. On December 17, 2021, Song brought this matter to Coinbase's attention via email to Coinbase Customer Service (Case No. #10449662), explaining the nature of the fraudulent dapp, including pictures of their transactions on Coinbase. On December 20, 2021, Coinbase responded to Song's complaint insinuating that his recovery passphrase had been shared with someone else and Coinbase "cannot provide any details about how [his recovery passphrase] was compromised" and could not reverse or cancel the transaction. Neither Song nor his wife ever provided the scammers or anyone else with their Coinbase recovery passphrase.

701. On December 22, 2021, Song contacted Coinbase again to inform it that his funds had been stolen from their Wallet and that they reported the theft to local law enforcement.

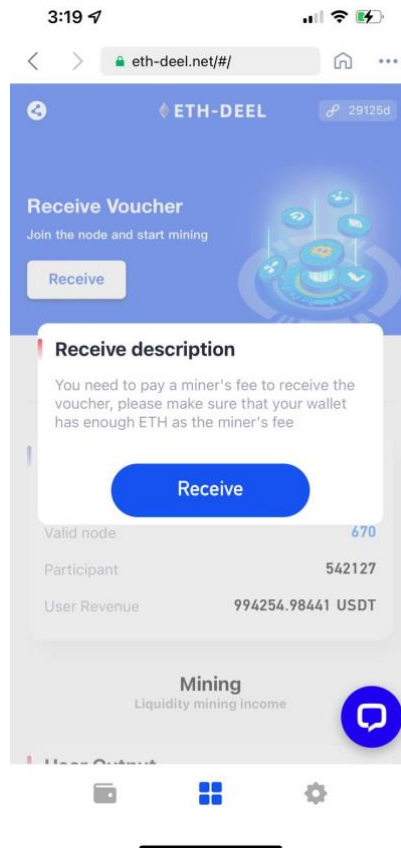
702. Coinbase's response was entirely unhelpful. Coinbase reiterated its prior generic, automated language regarding Song's recovery passphrase and stated that Coinbase "cannot reimburse or credit [her] Coinbase Wallet" Despite numerous attempts by Song to contact Coinbase customer support, Coinbase never provided Song or his wife with any meaningful assistance in recovering their stolen assets.

ccc. Nicholas Chicoine

703. On or about October 16, 2021, a person going by the name Alice contacted Claimant Nicholas Chicoine ("Chicoine") on Instagram. After befriending Chicoine, Alice informed Chicoine that she was earning significant income over Coinbase using a defi platform called Eth-deel.

704. Having lulled Chicoine with the prospect of similar income, Alice directed Chicoine to download the Coinbase Wallet application and open the link for eth-deel.net using the Wallet's browser. Chicoine did as he was instructed.

705. Once on the fraudulent pool's site, Alice directed Chicoine to purchase a miner's fee that would allow him to join the mining pool. Chicoine did as he was instructed, and this action most likely initiated the malicious smart contract.



706. At no time did Chicoine believe that he had allowed Alice or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Chicoine that anyone could access his Wallet to take his funds.

707. To fund the pool, Chicoine deposited a total of 273,772 USDT into his Coinbase Wallet.

708. In October 2021, scammers withdrew all the USDT (approximately 303,452) from Chicoine's Wallet, which included Chicoine's USDT and additional USDT he received from the fake mining pool. The withdrawal was done without Chicoine's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

709. Chicoine's life has been devastated. His mental and physical health has deteriorated since the day of the theft. He took out a loan to fund his Coinbase Wallet with the intentions of

immediately paying it back once he removed his profits. Instead, he has had to borrow money from family members to repay the loan. He is barely able to pay his rent and buy groceries. His life goals have been setback by over five years.

710. On November 28, 2021, Chicoine contacted Coinbase’s customer support to notify Coinbase about the unauthorized transaction (Case Nos. #09044007, #0878381, #08918447). Instead of conducting an investigation, Coinbase replied by informing Chicoine that “if you did not authorize any outgoing transactions from your Coinbase Wallet, it means that your recovery phrase has been compromised” and that Coinbase could “not provide any further details about how it was compromised nor can we help recover these funds.”

711. On December 3, 2021, Chicoine replied to Coinbase’s email and told Coinbase that he never gave out his recovery phrase, explained how he visited the fraudulent mining pool and unbeknownst to him entered into a malicious smart contract, lost life changing sums due to the unauthorized transaction, and that Coinbase should properly warn people that scams could occur through the Wallet’s browser tab. Coinbase responded by again informing Chicoine that it was not liable: “As previously mentioned, Coinbase Wallet is a user-controlled and non-custodial product which means that you – and only you – have access to your seed phrase and the ability to move your funds.” On December 5, 2021, Chicoine responded to Coinbase’s email and informed them that he “never gave out [his] seed phrase” and that his Wallet “was compromised in way [sic] that isn’t specified in any literature from Coinbase.” Coinbase never responded to this message.

712. On December 6, 2021, Chicoine opened a new support ticket with Coinbase’s support to complain about his Wallet being compromised through the dapp browser. Coinbase replied to Chicoine’s email with the same automated reply from his first complaint ticket. Coinbase then informed Chicoine that it was closing the complaint ticket. Chicoine responded to Coinbase by informing it once again that he “never authorized the transaction of [his] USDT out of [his] wallet. [He] never gave out [his] seed phrase” and that Coinbase’s Wallet has a major security flaw. Coinbase replied to Chicoine by informing him that his case had been closed.

713. On or around December 13, 2021, Chicoine submitted a third complaint ticket to Coinbase complaint titled “USDT transaction WITHOUT my Authorization.” Coinbase replied to.

Chicoine’s third complaint by informing him that “**We cannot provide any further details about how it was compromised nor can we help recover these funds.**” (emphasis in original).

ddd. Eva Fengel

714. On or about November 10, 2021, a parent at her daughter’s school informed Claimant Eva Fengel (“Fengel”) that he was earning significant income over Coinbase using a defi platform called Aaveeth.co.

715. Fengel, with hopes of earning similar income, downloaded the Coinbase Wallet application and visited the link for aaveeth.co using the Wallet’s browser.

716. Once on the fraudulent pool’s site, Fengel purchased the voucher to join the mining pool as instructed by the parent, and this action most likely initiated the malicious smart contract.

717. At no time did Fengel believe that she had allowed anyone access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Fengel that anyone could access her Wallet to take her funds.

718. To fund the pool, Fengel deposited a total of \$53,482 USDT into her Coinbase Wallet.

719. In November 2021, scammers withdrew all the USDT (approximately \$53,482) from Fengel’s Wallet. The withdrawal was done without Fengel’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

720. Fengel’s life has been devastated. She was new to the crypto space and this experience has been extremely stressful. She has experienced anxiety not just due to the financial loss, but also because she trusted Coinbase Wallet to protect her funds.

721. On November 30, 2021, Fengel contacted Coinbase’s customer support to notify Coinbase about the unauthorized transaction (Case Nos. #08820998, #09343060, #10066240, #0936729). Coinbase replied to Fengel’s email informing her that “Coinbase Support does not have the ability to raise limits as the Coinbase Wallet limit system is automated and determined at account creation.” Fengel replied to Coinbase’s nonsensical email by providing additional facts about what she believed happened to her funds including that she believed her funds went into a fraudulent liquidity mining pool.

722. Coinbase replied by asking Fengel to provide the “transaction hash” so it could investigate the transfer. Fengel provided the transaction hash. Coinbase informed Fengel that it was “working hard to quickly address this issue, and we’ll reach out to you as soon as we have an update.”

723. On December 2, 2021, Coinbase replied to Fengel’s email and informed her that it advises she cease “any additional engagement with this scam, and we recommend reporting it to law enforcement agencies in [her] country.” Fengel replied and informed Coinbase that she will pursue the issue with law enforcement, but Coinbase’s boilerplate response did not “address [her] specific situation... .” Coinbase replied to Fengel’s complaint by informing her that “If [she] did not authorize any outgoing transactions from your Coinbase Wallet, it means that your recovery phrase has been compromised.”

724. On January 6, 2022, Fengel submitted a new complaint ticket and described her interaction with Aaveeth, the fraudulent mining pool. In response, Coinbase locked her account to protect her while it confirmed that her devices and email were secure. Instead of conducting an investigation into the unauthorized transfer, on January 7, 2022, Coinbase again replied to Fengel to inform her that once her “recovery phrase is exposed to another party, they can use it to transfer funds without your authorization.” Fengel replied by telling Coinbase that she feels “as though you haven’t read what I’ve stated multiple times. **My recovery phrase was backed up manually on paper – not online or digitally.** Do you understand? My recovery phrase was NOT compromised, so your response is irrelevant.” (emphasis in original).

725. Coinbase responded to Fengel’s email by stating that “As previously mentioned, Coinbase Wallet is a user-controlled and non-custodial product which means that you – and only you – have access to your seed phrase and the ability to move your funds” and that it could not help Fengel recover her funds.

726. After several more emails, on February 4, 2022, weeks after Fengel’s crypto was stolen, Coinbase finally acknowledged that after “an extensive review of the transaction details, your Wallet’s history, and the addresses associated with it, the unauthorized activity you reported appears to have resulted from a signed transaction on Nov-10-2021 . . . that approved a malicious third party to transfer funds from your Wallet.” At no time during Coinbase’s investigation did it replenish Fengel’s Wallet.

eee. Robert Willis

727. On or about December 10, 2021, a person going by the name Wuqian, contacted Claimant Robert Willis (“Willis”) on TikTok. After befriending Willis, Wuqian informed Willis that she was earning significant income over Coinbase using a defi platform called Best Ethmine.

728. Having lulled Willis with the prospect of similar income, Wuqian directed Willis to download the Coinbase Wallet application and open the link for bestethmine.com using the Wallet’s browser. Willis did as he was instructed.

729. Once on the fraudulent pool’s site, Wuqian directed Willis to pay a miner’s fee that would allow him to join the mining pool. Willis did as he was instructed, and this action most likely initiated the malicious smart contract.

730. Wuqian then suggested Willis join another mining pool named Eth Super Defi. Wuqian directed Willis to open the link for ethsuperdefi.com using the Wallet’s browser. Willis did as he was instructed.

731. Once again Wuqian directed Willis to pay a miner’s fee that would allow him to join the mining pool. Willis did as he was instructed, and this action most likely initiated another malicious smart contract.

732. At no time did Willis believe that he had allowed Wuqian or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Willis that anyone could access his Wallet to take his funds.

733. To fund the pool, Willis deposited a total of \$270,009 USDT into his Coinbase Wallet.

734. In March 2022, scammers withdrew all the USDT (approximately \$270,009) from Willis’s Wallet. The withdrawal was done without Willis’ permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

735. Willis’s life has been devastated. Willis is seventy-two years old and disabled, so he has no way to earn a living by working. Willis had to sell his home to pay back funds he borrowed to fund the fraudulent pool. He is still paying back additional debt that he took out on his credit cards and loans to fund the fraudulent pool. Willis is worried about his future as he has limited funds after losing a substantial amount of his life savings to this fraudulent pool.

736. Initially, Willis did not contact Coinbase customer support for fear that Coinbase would simply close his account without providing any recovery assistance to him. However, On February 20, 2022, Willis contacted Coinbase’s customer support to notify Coinbase about the unauthorized transaction (Case No. #10402258). Coinbase replied to Mr. Willis by email informing him that “[i]n order to investigate further, we’ll need the transaction hash.” Coinbase further informed Mr. Willis that “[i]f your transaction does not have a hash, it may not have been successfully sent on the network, and that means it won’t be delivered to the recipient.”

737. Following the reported theft, Coinbase’s customer support was unhelpful to Willis and Coinbase has continued to deny responsibility and restricted Willis’s access to assets in his Wallet.

fff. Stephen Parker

738. On or about March 2, 2022, a person going by the name Lin Kexin, who allegedly lived in Florida, contacted Claimant Stephen Parker (“Parker”) on WhatsApp. After befriending Parker, Kexin informed Parker that she was earning significant income over Coinbase using a defi platform called DeFi Mining.

739. Having lulled Parker with the prospect of similar income, Kexin directed Parker to download the Coinbase Wallet application and open the link for usdtapp.com using the Wallet’s browser. Parker did as he was instructed.

740. Once on the fraudulent pool’s site, Kexin directed Parker to purchase a node that would allow him to join the mining pool. Parker did as he was instructed, and this action most likely initiated the malicious smart contract.

741. At no time did Parker believe that he had allowed Kexin or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Parker that anyone could access his Wallet to take his funds.

742. To fund the pool, Parker deposited a total of \$163,000 USDT into his Coinbase Wallet.

743. In March 2022, scammers withdrew all the USDT (approximately \$163,000) from Parker’s Wallet. The withdrawal was done without Parker’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

744. Parker’s life has been devastated and he has suffered significant distress as a result of his financial loss.

745. On March 21, 2022, Parker contacted Coinbase’s customer support to notify Coinbase about the unauthorized transaction (Case No. #10860500). Coinbase replied to Parker by email and informed him that Coinbase is “working hard to quickly address this issue, and we’ll reach out to you as soon as we have an update.” On March 23, 2022, Parker emailed Coinbase and explained that there are “fraudulent people who are stealing crypto through Coinbase wallet.” Parker provided Coinbase with the fraudulent mining pool’s URL and told Coinbase to do “the right thing, find these people suspend them and or turn them into the authorities.” Coinbase replied to Parker’s email by informing Parker that “Coinbase Wallet’s dapp browser currently supports all Ethereum dapps build on Web3” and that this “does not however guarantee a flawless experience with all dapps.” Coinbase then suggested that if Parker is having an issue with a specific dapp then he should reach “out directly to the dapp developer for additional assistance.” Coinbase again emailed Parker and informed him that they “take these reports very seriously, and will be flagging this malicious dapp to our security and investigation teams” but “[d]ue to the irreversible nature of cryptocurrency protocols, transactions can neither be canceled nor reversed once confirmed on the blockchain.” Coinbase informed Parker that they could not reimburse or credit his wallet and suggested contacting the FBI. On April 4, 2022, Coinbase closed Parker’s claim.

ggg. Sachin Garg

746. On or about November 27, 2021, a person going by the name NK contacted Claimant Sachin Garg (“Garg”) on WhatsApp. After befriending Garg, NK informed Garg that she was earning significant income over Coinbase using a defi platform called Eth-Panda.

747. Having lulled Garg with the prospect of similar income, NK directed Garg to download the Coinbase Wallet application and open the link for eth-panda.com using the Wallet’s browser. Garg did as he was instructed.

748. Once on the fraudulent pool’s site, NK directed Garg to purchase a node that would allow him to join the mining pool. Garg did as he was instructed, and this action most likely initiated the malicious smart contract.

749. At no time did Garg believe that he had allowed NK or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Garg that anyone could access his Wallet to take his funds.

750. To fund the pool, Garg deposited a total of \$100,00 USDT into his Coinbase Wallet.

751. In December 2021, scammers withdrew all the USDT (approximately \$100,000) from Garg's Wallet. The withdrawal was done without Garg's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

752. Garg's life has been devastated by the financial loss and he continues to suffer emotionally and mentally as a result of the fraudulent scam.

753. On December 29, 2021, Garg contacted Coinbase's customer support to notify Coinbase about the unauthorized transaction (Case No. #09304791). On January 12, 2022, Coinbase replied to Garg by email informing him that Coinbase "advise ceasing any further engagement with this scam, and we recommend reporting it to law enforcement agencies in [his] country" and that Coinbase "has no information about ownership of external cryptocurrency addresses, and because this is an external process, there is no way for Coinbase to cancel, reverse, or recover these funds on your behalf." Garg provided Coinbase support with the name of the malicious dapp, but Coinbase did not block or take down the dapp.

754. On January 12, 2022, Coinbase emailed Garg and informed him that once his "recovery phrase is exposed to another party, they can use it to transfer funds without your authorization" and because Garg's "wallet is a user-controlled and non-custodial product, meaning that only you have full control/access (including the recovery phrase), we cannot provide any additional details about how it was compromised." Garg, in actuality, had kept full control of his recovery phase. Coinbase followed up with an additional email on the same day to inform Garg that it "cannot help recover any Coinbase Wallet or transfer funds on your behalf."

hhh. Timothy Magnus

755. On or about November 2, 2021, a woman named "Amy" contacted Claimant Timothy Magnus ("Magnus") on LinkedIn. After befriending Magnus, the individual informed him that she was earning significant income over Coinbase using a defi platform called Hydefieco.

756. Having lulled Magnus with the prospect of similar income, Amy directed Magnus to download the Coinbase Wallet application and open the link for Hydefieco.com using the Wallet's browser. Magnus did as he was instructed.

757. Once on the fraudulent pool's site, Amy directed Magnus to purchase a node that would allow him to join the mining pool. Magnus did as he was instructed, and this action most likely initiated the malicious smart contract.

758. At no time did Magnus believe that he had allowed Amy or anyone else access to the funds in his Wallet, and Coinbase Wallet provided no warning to Magnus that anyone could access his Wallet to take his funds.

759. To fund the pool, Magnus deposited a total of \$30,517 USDT into his Coinbase Wallet.

760. On or around December 24, 2021, scammers withdrew all the USDT (approximately \$30,517) from Magnus's Wallet. The withdrawal was done without Magnus's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

761. In addition to the significant financial loss, Magnus has also suffered mental and emotional distress as a result of the Coinbase scam.

762. On or around December 26, 2021, Magnus contacted Coinbase's customer support to notify Coinbase about the unauthorized transaction (Case Nos. #09256130, #09241316, #11551975). On December 26, 2021, Coinbase emailed Magnus to acknowledge receipt of his complaint and to inform him that it was working hard to quickly address the issue. Magnus followed up to Coinbase's email by requesting a photo of his account balance to see what it shows to Coinbase and then sent another email the next day to see if Coinbase had an update on his account.

763. On December 28, 2021, Coinbase replied to Magnus and informed him that if his account was locked because he had a security concern, that he should not attempt self-recovery. Instead, Coinbase informed Magnus that it was conducting a security review and requested information regarding Magnus's Wallet. Magnus replied to Coinbase's email and informed Coinbase that his account was hacked and that his balance went from \$30,336 to \$26.68 without his authorization.

764. Coinbase responded to Magnus’s email to inform him that its “record shows that there are no unauthorized transactions on your Coinbase account.” Coinbase then provided Magnus with the steps necessary to regain access to his account. Magnus replied to Coinbase’s email by informing it once again that there was fraudulent activity in his account because his balance went from \$33,336 to \$26.68 in a couple of hours. Coinbase replied by resending the same message that Magnus replied to, minus the language concerning the unauthorized transaction and informing Magnus that Coinbase’s “recommendation would be to reach out to the party you intended to send these funds to and see if they can help you recover the funds.”

iii. Sudang Tjin

765. On or about November 5, 2021, a woman going by the name Hannah, who allegedly lived in Orlando, Florida, contacted Claimant Sudang Tjin (“Tjin”) on WhatsApp. After months of chatting in an effort to befriend Tjin, Hannah informed Tjin that she was earning significant income over Coinbase using a defi platform called COIN-ETHGO (<https://coin-ethgo.co/#/>).

766. Having lulled Tjin with the prospect of similar income, Hannah directed Tjin to download the Coinbase Wallet application and open the link for the dapp using the Wallet’s browser. Tjin did as he was instructed.

767. Once on the fraudulent pool’s site, Hannah directed Tjin to purchase a node that would allow him to join the mining pool. Tjin did as he was instructed, and this action most likely initiated the malicious smart contract.

768. At no time did Tjin believe that he had allowed Hannah or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Tjin that anyone could access his Wallet to take his funds.

769. On or about December 5, 2021, Tjin began making deposits of USDT into his Coinbase Wallet to fund the mining pool.

770. Between December 5, 2021 and January 1, 2022, Tjin make approximately 10 deposits of USDT into his Wallet.

771. Following Tjin's initial deposit, Hannah convinced him to enter into a "pledge" pool to earn more ETH rewards. Tjin contacted the dapp's customer service agent who informed Tjin that he would need to deposit an additional \$100,000 USDT to participate in the pledge.

772. Tjin informed Hannah that he could not afford the pledge deposit requirement, and Hannah offered to pay half of the pledge. Despite Hannah's offer, Tjin declined to join the pledge.

773. The next day, on December 20, 2021, scammers withdrew all the USDT from Tjin's Wallet. The withdrawal was done without Tjin's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

774. When Tjin contacted Hannah to inquire about the fraudulent withdrawal, Hannah informed Tjin that it was common for the dapp to pledge miners' funds automatically and Tjin would have to deposit \$100,000 USDT to regain access to his funds.

775. To satisfy the pledge, Tjin made three additional deposits of USDT into his Wallet, in addition to the \$50,000 USDT provided by Hannah. Immediately after Tjin made the additional deposits, his Wallet was drained and his account was locked.

776. As a result of the scam, Tjin lost \$48,520 USDT, which was comprised of his life savings. Tjin's life has been devastated because of the unauthorized transaction. He is depressed and is constantly worried about his finances.

777. Tjin first reported the scam to customer service on or about January 17, 2022. Tjin provided Coinbase with the address of the malicious app (Coin-Ethgo), and told Coinbase that it was a "very big scam." Coinbase nonetheless did not take takedown or block the dapp.

778. On or around February 9, 2022, Tjin contacted Coinbase customer service by email to inform it that his USDT had been stolen from his Coinbase Wallet (Case No. #10186518). In response, Coinbase provided Tjin with a generic, automated response, indicating that Coinbase would flag the dapp, but that there was nothing that Coinbase could do to recover his funds. Coinbase denied any responsibility for the loss and directed Tjin to contact law enforcement.

jjj. Jane Doe 3

779. On or about February 9, 2022, Claimant Jane Doe 3 was connected by a friend to an individual on social media. After befriending Jane Doe 3, the person invited Jane Doe 3 and her

husband to communicate on WhatsApp. The person informed Jane Doe 3 about a mining activity of ETH on Coinbase. The person told Jane Doe 3 that they were earning significant income over Coinbase using a defi platform called ETH LIQUIDITY MINING (www.ethliquimining.com).

780. Having lulled Jane Doe 3 with the prospect of similar income, the person directed Jane Doe 3 and her husband to download the Coinbase Wallet application and open the link for the dapp using the Wallet's browser. On or about February 7, 2022, Jane Doe 3 and her husband did as they were instructed and entered into a smart contract with the dapp.

781. Jane Doe 3 and her husband were familiar with Coinbase, and based on its reputation as a trustworthy company, they believed their funds were secure.

782. At no time did Jane Doe 3 allow anyone access to her security passphrase for the Wallet, and the Coinbase Wallet provided no warning to Jane Doe 3 that anyone could access her Wallet to take her funds without the passphrase.

783. Between February 7 and 20, 2022, Jane Doe 3 and her husband made ten deposits of USDT into their Wallet to fund the pool.

784. On or about February 20, 2022, scammers withdrew all the USDT (approximately \$335,218.49 USDT) from Jane Doe 3's Wallet. The withdrawal was done without Jane Doe 3's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

785. Jane Doe 3 and her husband lost \$311,401.19 USDT because of the unauthorized transactions. Jane Doe 3 and her husband suffered significant emotional trauma as a result of the scam and are now unable to purchase a home due to the substantial financial loss.

786. On or about February 22, 2022, Jane Doe 3 brought this matter to Coinbase's attention by phone and email (Case No. #10434168). In response, Coinbase unhelpfully replied that there was "no way" for it to cancel, reverse or recover Jane Doe 3's funds and that Coinbase was not responsible for her losses. Upon information and belief, Coinbase did not take down or block access to the malicious dapp for months after it was reported to Coinbase.

kkk. Dieu Thai

787. On or about October 2, 2021, Dieu Thai (“Thai”) was contacted by a person in a Ethereum group chat on WhatsApp. After befriending Thai, the person informed him of an opportunity to join a liquidity mining pool on Coinbase Wallet. Thai understood Coinbase to be one of the largest and most trusted cryptocurrency platforms and considered Coinbase Wallet to be a safe a secure platform to hold his assets.

788. On or about October 28, 2021, Thai entered into a smart contract and joined the mining pool through a dapp called eth-base.org for a 30-day contract term. At all times, Thai believed that he was mining directly with Coinbase Wallet. He never received a message warning him that he had connected his Coinbase Wallet to the dapp or given the application access to his Wallet.

789. Initially the pool functioned as promised and Thai, relying on the legitimacy of Coinbase, continued to make deposits into this Coinbase Wallet to fund the pool.

790. Between October 28, 2021 and November 30, 2021, Thai made 7 deposits of USDT into his Wallet.

791. At the end of his 30-day contract, Thai attempted to withdraw his assets but was told by the dapp’s customer service representative that he would have to pay a fee to release his funds. At this point, Thai realized he was the victim of a fraudulent scheme. On or about November 30, 2021, all of Thai USDT was drained from his Wallet.

792. Thai lost 218, 185.87 USDT, his entire savings, as a result of this scam. In addition to the substantial financial loss, Thai also suffered emotional and mental distress as a result of the fraud.

793. Following the fraudulent withdrawals, Thai contacted Coinbase customer support for assistance in recovering his stolen assets. Coinbase responded to Thai’s complaint with generic, automated language instructing him that Coinbase was not liable for his losses as the Coinbase Wallet is a “user-controlled product” and explained that it would not assist Thai in recouping his stolen assets.

III. Anna Yuan

794. On or about December 1, 2021, Anna Yuan (“Yuan”) was contacted by an individual named “Chen” on Instagram, who informed her of a liquidity mining pool that this individual had earned significant income through on Coinbase Wallet using a dapp called <https://www.sushidexfi.com>.

795. On or about December 22, 2021, after lulling Yuan with the prospect of similar income, Chen directed Yuan to download the Coinbase Wallet application and open the link to the dapp using her Coinbase Wallet's browser. Yuan did as she was instructed.

796. At no time did Yuan believe that she had allowed Chen or anyone else access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Yuan that anyone could access her Wallet to take her funds.

797. To fund the pool, Yuan made 9 deposits of USDT into her Coinbase Wallet between December 22, 2021 and January 21, 2022. Initially the pool was operating as described by Chen and Yuan was able to withdraw interest earned on her deposits as promised. Chen then encouraged Yuan to deposit more USDT into her Wallet to gain higher rewards.

798. On or about January 21, 2022, scammers withdrew all the USDT (approximately \$102,211.96) from Yuan's Wallet. The withdrawal was done without Yuan's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

799. Yuan lost \$102,500 USD because of the unauthorized transactions. Yuan and her husband lost their entire life savings as a result of the scam. This loss has caused Yuan and her husband significant emotional and mental distress.

800. Following the fraudulent withdrawal, Yuan attempted to bring this matter to Coinbase's attention by calling Coinbase's customer service phone number but she never received a response from Coinbase. On or around March 4, 2022, Yuan contacted Coinbase again to report the theft of her assets from her Coinbase Wallet (Case No. #10622924). Rather than providing Yuan with any actual assistance to recover her funds, Coinbase replied with generic, automated language advising Yuan to "ceas[e] any additional engagement with this scam" and to report the scam to law enforcement.

mmm. Erin Finegold

801. On or about November 20, 2021, an individual contacted Claimant Erin Finegold ("Finegold") through FinTech on Twitter. After chatting with Finegold through Twitter, this individual invited her to participate in an investment opportunity to earning significant interest on USDT using Coinbase through a dapp called defi.cb-ant.net .

802. Having lulled Finegold with the prospect of similar income, the individual directed Finegold to download the Coinbase Wallet application and open the link for defi.cb-ant.net using the Wallet's browser. On or about December 2, 2021, Finegold did as she was instructed, downloaded Coinbase Wallet and entered into what she would later discover to be a malicious smart contract.

803. At no time did Finegold believe that she had anyone else access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Finegold that anyone could access her Wallet to take her funds.

804. Between December 2 and December 12, 2021, Finegold made four deposits of USDT into his Coinbase Wallet.

805. On or about December 15, 2021, scammers withdrew all the USDT (approximately \$303,487.47 USDT) from Finegold's Wallet. The withdrawal was done without Finegold's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

806. Finegold lost \$303,487.47 USDT because of the unauthorized transactions and suffered significant trauma as a result of her financial losses.

807. Finegold immediately brought this matter to Coinbase's attention on December 15, 2021 (Case No. #11284606) and Coinbase provided Finegold with an automated, canned response that did not address her concerns. Coinbase then told Finegold that they had reported the malicious dapp to their security team. Weeks later, Finegold checked, and the dapp was still available in her Coinbase Wallet.

808. On April 10, 2021, Finegold filed a formal complaint with Coinbase after receiving an unhelpful initial response from Coinbase (-Complaint #11284606). The following day, Coinbase responded indicating to Finegold that it would respond in 15 business day. Coinbase never responded.

nnn. John Doe 3

809. On or about June 1, 2022, a person going by the name "Laura", who allegedly lived in New York, contacted Claimant John Doe 3 through social media. After befriending John Doe 3, Laura informed him about her interest in cryptocurrency and her successful investment in Tether through Coinbase using a defi platform called "<http://tether-hgl.co/#/>".

810. Having lulled John Doe 3 with the prospect of similar income, Laura directed John Doe 3 to download the Coinbase Wallet application and open the link for the dapp using the Wallet's browser. John Doe 3 did as he was instructed.

811. On or about June 10, 2022, John Doe 3 began making small deposits into his Coinbase Wallet to test the investment platform. At no time did John Doe 3 believe that anyone else could access the funds in his Wallet, and the Coinbase Wallet provided no warning to John Doe 3 that anyone could access his Wallet to take his funds.

812. After the initial deposit, John Doe 3 earned the promised interest on his original investment and continued to make additional deposits to his Wallet. Between June 10 and June 23, 2022, John Doe 3 made 8 deposits of USDT into his Coinbase Wallet to fund the investment pool. The balance of his wallet was emptied into the investment pool without his authorization. Laura informed John Doe 3 that the funds were deposited as part of a "U Plan Verification" plan.

813. In early July of 2022, John Doe 3 came across an article in Forbes describing the "Pig Butchering Cryptocurrency Scam." At this point, John Doe 3 realized that he was the victim of a fraudulent scheme, and immediately attempted to withdraw his assets from his Coinbase Wallet. John Doe 3 immediately received a message from the dapp informing him that his withdrawal request had "failed."

814. At Laura's instruction, John Doe 3 contacted the customer support agent on the dapp, who he believed to be a Coinbase representative. The agent informed John Doe 3 that he would have to deposit an additional \$2 million dollars by July 30, 2022 in order to retrieve his assets, or his investment would be defaulted and he would lose everything.

815. John Doe 3 lost \$678,243.64 because of the unauthorized transactions, comprised of his life savings and other funds needed to support his dependent father.

816. Days later, John Doe 3 contacted Coinbase Support to report the incident (Case No. #12653356). Coinbase replied with an unhelpful, generic response, informing him that he had entered into a smart contract with the dapp that allowed scammers unauthorized access to his Wallet, but Coinbase could not assist him in recovering the funds that were stolen from his wallet. On or about July 14, 2022, John Doe 3 filed a complaint with Internet Crime Center for the FBI.

ooo. Joseph Beakey

817. On or about March 22, 2022, Claimant Joseph Beakey (“Beakey”) was contacted by an individual on Facebook. After befriending Beakey, the individual informed him about an opportunity to earn significant income over Coinbase using a defi platform called AMMUNI (<http://am-uni.com>).

818. Having lulled Beakey with the prospect of similar income, the individual directed Beakey to download the Coinbase Wallet application and open the link for the dapp using the Wallet’s browser. Beakey did as he was instructed.

819. On or about April 27, 2022, Beakey unknowingly entered into a malicious smart contract on the dapp which allowed scammers to access the funds in his Wallet. Coinbase Wallet provided no warning to Beakey that anyone could access his Wallet to take his funds.

820. Between April 27 and July 6, 2022, Beakey made 22 deposits of USDT into his Coinbase Wallet.

821. Beakey lost \$1,149,225.00 USDT because of the unauthorized transactions and suffered significant emotional distress as a result of his losses and the egregious deception that Coinbase allowed to operate on its platform.

822. On June 22, 2022, Beakey contacted Coinbase Customer Service by phone and email to inquire about the validity of the AMMUNI dapp (Case No. #12290283). That same day, Coinbase replied to Beakey informing him that it would flag the dapp as a malicious dapp. Beakey did not realize that he was the victim of a fraudulent scam until he contacted Coinbase Support. After notifying Beakey of the nature of the dapp, however, Coinbase provided no further support to Beakey in recovering his stolen funds. To the best of Beakey’s knowledge, the scam dApp reported by Beakey to Coinbase was not blocked by Coinbase.

ppp. Michael Gibson

823. On or about January 18, 2022, a person going by the name “Soon Wei”, contacted Claimant Michael Gibson (“Gibson”) on WhatsApp. Gibson connected with Soon Wei after applying for a freelancing copywriting job post for a company promoting a new crypto financial system through Upwork. Soon Wei, who introduced herself to Gibson as the director of the company’s “Coinbase

affiliate program” purported to interview Gibson for the role. After answering some initial questions, Soon Wei offered Gibson the job.

824. Soon Wei informed Gibson that he would be tasked with promoting the company’s Coinbase Wallet function to new customers. Gibson was told that he would also earn additional bonuses for new customer deposits as well as his own investments into Coinbase Wallet.

825. On or about January 25, 2022, after conducting research and learning about Coinbase’s Affiliate Program, Gibson decided to accept the role and downloaded and opened a Coinbase Wallet account. Between January 25 and February 15, 2022, Gibson made 11 deposits of USDT into his Coinbase Wallet.

826. After Gibson’s initial deposit, the assets from his Wallet were removed and he was informed that by Soon Wei that the assets had simply been “pledged” to a mining pool, and Gibson would be receiving a reward for his pledge. On February 3, 2022, Gibson did receive an award of ETH but was instructed that he would have to deposit an additional \$40,000 USDT to receive the reward, otherwise all of his pledged assets would be forfeited. On February 12, 2022, Gibson deposited the additional \$40,000 USDT into his Wallet.

827. On February 12, 2022, rather than returning Gibson’s assets plus the reward, the dapp informed him that he “won” a second opportunity to earn an ETH reward and would have to deposit additional USDT to reach a \$250,000 USDT pledge threshold, otherwise his funds would be locked.

828. Soon Wei convinced Gibson that he was lucky to be receiving such a high reward opportunity and encouraged him to meet the new pledge threshold. On or about February 14 and 15, 2022, Gibson deposited the additional USDT to satisfy the new pledge. Immediately after depositing the funds, Gibson’s assets were drained.

829. The withdrawal was done without Gibson’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

830. Gibson lost \$271,758.08 USDT because of the unauthorized transactions. Gibson lost an additional \$143,286.23 USDT which was stolen from Gibson’s other digital wallets through spyware installed on his personal computer by the scammer.

831. Not only did Gibson lose his entire savings as a result of the scam and continues to suffer significant mental and emotional distress, but Gibson borrowed \$174,934.33 USDT to meet the necessary funds to meet the capital requirements imposed by the scammers to release the funds that were locked in the mining pool. Gibson has creditors constantly contacting him to repay the debt.

832. On or about September 20, 2022, Gibson contacted Coinbase customer support to report his stolen assets (Case No. #13122951). In response, Coinbase informed Gibson that Coinbase cannot recover his funds and that his security passphrase had been compromised. Gibson never shared his passphrase with anyone.

qqq. Terrance Smith

833. On or about July 17, 2022, a person going by the name of Zhang contacted Claimant Terrance Smith (“Smith”) on WhatsApp. After befriending Smith, Zhang informed him that he was earning significant income using a mining pool over Coinbase through a defi platform called DEFI.USDT.org.

834. Having lulled Smith with the prospect of similar income, Zhang directed Smith to download the Coinbase Wallet application and open the link for the dapp using the Wallet’s browser. On or about June 30, 2022, Smith did as he was instructed and unknowingly entered into a smart contract through the dapp which permitted scammers to access his Wallet without his consent.

835. At no time did Smith believe that he had allowed Zhang or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Smith that anyone could access his Wallet to take his funds.

836. Between June 30 and July 26, 2022, Smith made a total of 20 USDT deposits into his Coinbase Wallet to fund the mining pool.

837. On or about July 13, July 15, and July 27, 2022, scammers withdrew all the USDT from Smith’s Wallet. These withdrawals were done without Smith’s permission or consent and without any notification, warning, or substantive response from Coinbase.

838. Smith lost \$51,100.00 USD because of the unauthorized transactions and suffered significant stress and trauma as result of the substantial financial loss.

839. On or about July 28, 2022, Smith brought this matter to Coinbase’s attention via email explaining the fraudulent withdrawals conducted through the dapp on Coinbase’s browser (Case No. # #12617015). In response, Coinbase noted that it “flagged the malicious web3 site [sic] to [its] security and investigation teams” but told Smith that there was nothing Coinbase could do to retrieve his assets. Coinbase provided Smith with a list of third parties websites through which he could attempt to revoke the smart contract he entered into through the dapp.

rrr. Mike Liadov

840. On or about July 15, 2022, Claimant Mike Liadov (“Liadov”) was contacted by a woman on a social dating website. After befriending Liadov, the two began communicating over WhatsApp. The woman informed Liadov of a profitable investment using mining over Coinbase through a defi platform called Sink Effect (<http://sinkeffect.info/#/>).

841. Having lulled Liadov with the prospect of similar income, the woman directed Liadov to download the Coinbase Wallet application and open the link for the dapp using the Wallet’s browser. On or about July 15, 2022, Liadov did as he was instructed and unknowingly entered into a malicious smart contract which allowed scammers access to the contents of his Wallet.

842. At no time did Liadov believe that he had allowed anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Liadov that anyone could access his Wallet to take his funds.

843. Between July 27 and August 9, 2022, Liadov made 6 deposits of USDT into his Coinbase Wallet to fund the mining pool.

844. On or about August 9, 2022, scammers withdrew all the USDT from Liadov’s Wallet. The withdrawal was done without Liadov’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

845. Liadov lost \$ 120,000.00 USD because of the unauthorized transactions, comprised of his life savings, and continues to suffer significant emotion harm.

846. Immediately following the fraudulent withdrawal, Liadov brought this matter to Coinbase’s attention by email to Coinbase customer support (Case No. # 12772791). In response,

Coinbase told Liadov that there was nothing Coinbase could retrieve the stolen assets. Further, even weeks after communicating the theft to Coinbase, the malicious dapp, sinkeffect.info, remained live.

sss. Jad Ghandour

847. On or about November 18, 2021, an individual contacted Claimant Jad Ghandour (“Ghandour”) on Twitter. After befriending Ghandour, the individual continued to communicate with Ghandour via WhatsApp and informed him about an investment opportunity over Coinbase using a defi platform called ETH-COIN (“eth-coin.info”).

848. Having lulled Ghandour with the prospect of similar income, the individual directed Ghandour to download the Coinbase Wallet application and open the link to the dapp using the Wallet’s browser. Ghandour did as he was instructed and on November 19, 2021 entered into a malicious smart contract which gave scammers unfettered access to his Coinbase Wallet.

849. Coinbase Wallet provided no warning to Ghandour that anyone could access his Wallet to take his funds.

850. Between November 19 and November 23, 2021, Ghandour made 21 deposits of USDT into his Coinbase Wallet to fund the mining pool.

851. On or about November 23, 2021, scammers withdrew all the USDT from Ghandour’s Wallet. The withdrawal was done without Ghandour’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

852. On or about November 23, 2021, Ghandour brought this matter to Coinbase’s attention by phone and via email (Case Nos. # 0871812, # 08717456). Coinbase customer support was entirely unhelpful. In response, Coinbase told him that it was not responsible for his loss and could not assist him in recouping his stolen assets.

853. Ghandour lost \$196,629.71 USDT because of the unauthorized transactions and as a result of the significant financial loss, suffered mental and emotional harm.

ttt. Jian Jing Shen

854. On or about May 23, 2022, Claimant Jian Jing Shen (“Shen”) was contacted by an individual on Instagram. After befriending Shen, the individual informed her about an opportunity to

earn significant income over Coinbase using a defi platform called META (<https://meta-data.top/#/pages/index/index>).

855. Having lulled Shen with the prospect of similar income, the individual directed her to download the Coinbase Wallet application to take part in the investment. On or about June 7, 2022, Shen opened the dapp and paid a one-time membership fee to participate in the investment opportunity. Unbeknownst to Shen, she was actually entering into a smart contract, imbedded in the transaction, that would grant scammers access to her Wallet without her consent.

856. Between June 7 and July 9, 2022, Shen made 3 deposits of USDT into her Coinbase Wallet. Shen was able to view the assets in her Wallet and believed that her funds were secure.

857. On or about July 9, 2022, Shen made a large deposit of USDT into her Wallet. After the deposit, Shen was offered a loan of \$100,000 USDT to allow her to make additional bids through the investment. Seeing no downside, she agreed to accept the loan. Immediately after agreeing to the loan, Shen's Wallet was drained of all funds. The dapp informed Shen that because she agreed to the loan, all funds were "locked" and that the loan was irrevocable.

858. Shen lost \$182,889.08 USDT, her life savings and retirement funds, because of the unauthorized transactions and suffered significant emotional distress as a result of her losses.

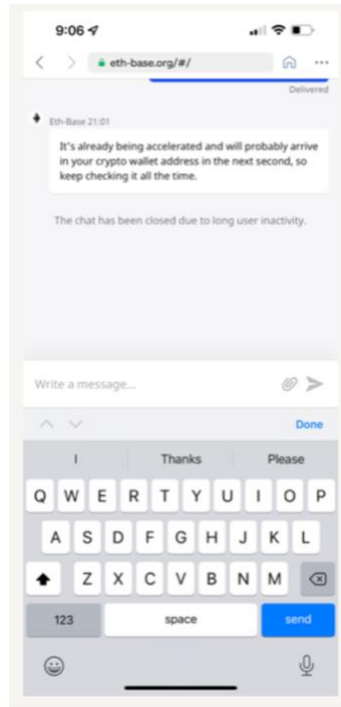
859. On or around July 9, 2022, Shen immediately contacted Coinbase by email to report the stolen assets (Case No. #12442095). In response, Coinbase offered Shen generic responses regarding malicious dapps and informed her that there was nothing Coinbase could do to assist her or return her funds. On July 19, 2022, Shen contacted Coinbase again to request that it reopen her complaint as she believed she was the victim of a scam. In response Coinbase informed her that it was not responsible for transactions using Coinbase Wallet as it is a "non-custodial product" and advised her to cease further engagement with the dapp and report the theft to law enforcement.

uuu. Canh Thai

860. On or about October 6, 2021, Claimant Canh Thai ("Thai") was introduced to Coinbase Wallet by his brother. After doing some research on Coinbase Wallet, Thai came to the conclusion that it was one of the most secure crypto wallets in the market, so he installed it to start mining. Thai

then joined the dapp eth-base.org under the impression that it was a legit mining pool and his funds were secure through Coinbase Wallet.

861. Thai connected his Coinbase Wallet to eth-base.org through the Coinbase Wallet browser. For the first few weeks eth-base.org operated as Thai expected and he was promised higher profits if he deposited more USDT into his wallet.



862. Between October 28 and November 30, 2021, Thai made 10 deposits of USDT into his Coinbase Wallet to fund the mining pool, totaling \$1,199,294.64 USDT. Initially, his deposits were earning returns as promised, so Thai continued to make additional deposits of larger value. Confident in the security of Coinbase, Thai had no doubt that the mining operation was legitimate.

863. At no time did Thai believe that he had allowed anyone access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Thai that anyone could access his Wallet to take his funds.

864. In or around November 27, 2021, Thai's "30-day contract" ended, after which he was promised access to his deposited assets, as well as rewards earned. After complying with the dapp's requested "gas fee" in or around November 30, 2021, the dapp refused to release Thai's assets and

ceased communication with Thai. At this point, Thai realized that he was the victim of a fraudulent scam and scammers had withdrawn all the USDT (approximately \$1,199,294.64) from his Wallet.

865. The withdrawals were done without Thai's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

866. Thai's life has been devastated because of the unauthorized transaction. He is retired and the money he lost was his life savings. This situation has been extremely frustrating for his both mentally and physically and has impacted his family's life forever.

867. In December 2021, Thai brought this matter to Coinbase's attention by email to Coinbase customer support (Case No. 09340774). Coinbase responded by informing Thai that because of the irreversible nature of cryptocurrency protocol there was nothing it could do. On June 8, 2022, Thai again brought this matter to Coinbase's attention by email to Coinbase customer support (Case No. #11472985). In response, Coinbase advised Thai to "cease all communication with these parties" and contact local authorities. Coinbase took no responsibility for the matter and told Thai that there was nothing that Coinbase could do to recover his stolen funds.

vvv. Troy Gochenour

868. On or about September 30, 2021, Claimant Troy Gochenour ("Gochenour") was contacted by an individual on Facebook. After befriending Gochenour, the individual informed him about an opportunity to earn significant income over Coinbase using a defi platform called Ethusdt.co/#/.

869. Having lulled Gochenour with the prospect of similar income, the individual directed him to download the Coinbase Wallet application to take part in the investment. On or about October 21, 2021, Gochenour opened the dapp and paid a one-time miners fee, which the individual supplied the funds for, to participate in the investment opportunity. Unbeknownst to Gochenour, he was actually entering into a smart contract, imbedded in the transaction, that would grant scammers access to his Wallet without his consent.

870. Between October 26 and November 9, 2021, Gochenour made several deposits of USDT into his Coinbase Wallet. Gochenour was able to view the assets in his Wallet and make

withdrawals from the pool and believed that his funds were secure. Gochenour deposited a total of \$25,800 USDT into his Coinbase Wallet.

871. In November 2021, the scammers begin withdrew Gochenour's initial deposit of \$5,000 USDT from his Wallet without his consent. Gochenour contacted the dapps customer service who instructed him to deposit an additional \$10,000 USDT to fulfill his contract. Gochenour did as he was instructed. The scammers withdrew the \$10,000 USDT deposit immediately. Gochenour was then told that he needed to deposit an additional \$10,000 USDT into his Wallet to be able to receive all his money back plus the promised rewards.

872. As a result, Gochenour used his savings of \$2,000 and borrowed \$8,000 to deposit into his Wallet. The scammers withdrew the money out and then told Gochenour that he had to pay taxes on over 200,000 USDT to receive his deposits back. It was then that Gochenour realized he had been scammed.

873. Gochenor lost \$25,800 USDT, because of the unauthorized transactions and now suffers from mental and emotional distress as a result of the fraudulent scam.

874. Gochenour immediately contacted Coinbase support to report the stolen assets (Case Nos. #08302411, #08427513). In response, Coinbase offered Gochenour generic responses regarding Gochenour's responsibility to secure his Wallet's seed phrase and informed him that there was nothing Coinbase could do to assist him or return his funds and suggested Gochenour contact the FBI.

www. Curtis Cecil

875. On or about August 2, 2022, Claimant Curtis Cecil ("Cecil") was introduced by a friend to a liquidity mining investment opportunity over Coinbase using a defi platform called mingethn-top (<https://go.cb-w.com/dapp>). The friend referred Cecil to an individual who agreed to get Cecil set up with a Coinbase Account to begin participating in the mining pool.

876. Enticed by the prospect of similar income, Cecil agreed to join the mining pool and followed the direction of the referral contract who instructed Cecil to download the Coinbase Wallet application and open the link to the dapp using the Wallet's browser. Cecil did as he was instructed and on August 2, 2022 entered into a malicious smart contract which gave scammers unfettered access to his Coinbase Wallet, unbeknownst to him.

877. Coinbase Wallet provided no warning to Cecil that anyone could access his Wallet to take his funds, which he believed were secured by his security passphrase.

878. Between August 2 and August 5, 2022, Cecil made 3 deposits of USDT into his Coinbase Wallet to fund the mining pool.

879. Initially, Cecil received a return on his initial deposits as promised. Based on this experience, and his belief that Coinbase was a safe and secure platform to store his funds, Cecil continued to make additional deposits of larger monetary value into his Wallet.

880. On or about August 5, 2022, scammers withdrew all the USDT from Cecil's Wallet. The withdrawal was done without Cecil's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

881. Cecil promptly contacted the customer support agent through the dapp to report the fraudulent withdrawal. In response, the dapp agent informed Cecil that his account had been placed under review by his referral contact and in order to regain access to his assets he would have to deposit an additional 20% of the total value of his withdrawn assets to comply with "federal taxes."

882. As a result of the Coinbase liquidity mining scam, Cecil lost \$60,712.66 USDT. He has been financially devastated by the scam and suffered significant harm to his emotional and mental state as a result.

883. Immediately following the theft of his assets, Cecil contacted Coinbase customer support by phone to report the incident. Coinbase customer support was entirely unhelpful. In response, Coinbase told him that it was not responsible for his loss and could not assist him in recouping his stolen assets.

xxx. John Doe 4

884. On or about June 27, 2022, Claimant John Doe 4 was connected with a woman on a social dating website called Luxy. After befriending John Doe 4, the woman introduced him to a liquidity mining investment opportunity over Coinbase through a defi platform called mingethn-top (<https://go.cb-w.com/dapp>).

885. Having lulled John Doe 4 with the prospect of similar income, the woman directed John Doe 4 to download the Coinbase Wallet application and open the link for the dapp using the Wallet's

browser. The woman even deposited ETH into John Doe 4's Wallet account. John Doe 4 did as he was instructed and unknowingly entered into a malicious smart contract which allowed scammers access to the contents of his Wallet.

886. At no time did John Doe 4 believe that he had allowed anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to John Doe 4 that anyone could access his Wallet to take his funds.

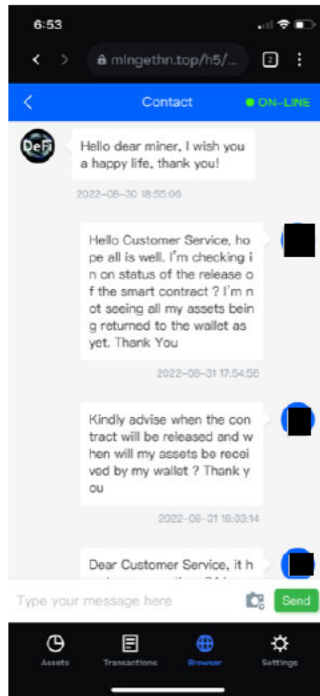
887. Between July 7 and August 30, 2022, John Doe 4 made 8 deposits of USDT into his Coinbase Wallet to fund the mining pool. After several weeks of successful participation in the mining pool, John Doe 4 invited two friends to join the investment mining pool as well.

888. On or about August 4, 2022, scammers withdrew all the USDT from John Doe 4's Wallet. The withdrawal was done without John Doe 4's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase. Shortly thereafter, John Doe 4 found that the two individuals who he invited to join the pool had also had their Wallets drained by the dapp.

889. John Doe 4 immediately contacted the customer support chat through the dapp to inquire about the fraudulent withdrawal. The dapp agent informed John Doe 4 that his funds were "on hold" in the pool and he would have to contribute an additional \$200,000 USDT to his Wallet or refer 5 people with a Coinbase Wallet balance of \$50,000 USDT within 30 days in order to regain access to his funds. The dapp warned that failure to comply would lead to daily fines.

890. To avoid fines, John Doe 4 contributed an additional \$150,000 USDT into his wallet to meet the \$200,000 USDT threshold. After depositing the additional USDT, the dapp still refused to release John Doe 4's funds. The dapp agent informed John Doe 4's that his account had been locked based on the IP address he used to access the dapp and he would need to pay 30% of his Wallet value to verify his account and unfreeze his account.

891. On August 8, 2022, John Doe 4 deposited the requested funds and requested the release of his assets.



892. After the August 26, 2022 deposit, the dapp unfroze John Doe 4's account but then demanded that John Doe 4's deposit an additional 20% to pay for "US Federal taxes" and provide his personal bank account information. On August 30, 2022, John Doe 4's deposited an additional \$74,990 USDT into his Wallet to meet the new "tax" threshold described by the dapp agent.

893. As a result of the fraudulent scam, John Doe 4 lost \$ 282,554.02 USDT, comprising his entire life savings and retirement fund. He has suffered significant emotional and mental harm.

894. Following the fraudulent withdrawal, on or around September 1, 2022, John Doe 4 brought this matter to Coinbase's attention by email to Coinbase customer support (Case No. # 12937821). In response, Coinbase told John Doe 4 that there was nothing Coinbase could retrieve the stolen assets. John Doe 4 replied to Coinbase on September 2, 2022, the dapp claimed to be a partner

9/15/22, 8:48 AM Yahoo Mail - Re: [Reply] Case #12937821 - Suspected Fraud - MVP

Re: [Reply] Case #12937821 - Suspected Fraud - MVP

From: [REDACTED]
To: help@coinbase.com
Date: Friday, September 2, 2022 at 11:02 AM EDT

Hello,

Thank you for the additional clarification around the taxes and further guidance. Much appreciated.

I would like to share that their website displays coinbase, amongst others as a partner. It may be in your best interest to have them remove such false claims.

Thank You
[REDACTED]

of Coinbase, hosted on the Coinbase platform – a representation that John Doe 4 reasonably relied on when deciding to engage with in transactions through the dapp on Coinbase. Further, Coinbase did not take or block the dapp, even after being contacted by John Doe 4.

yyy. James Buchan

895. In or around February, 2022, a person going by the name Ella Gulnazar contacted Claimant James Buchan, a resident of the United Kingdom, on Facebook. After befriending Mr. Buchan, Ms. Gulnazar informed Mr. Buchan that she was earning significant income over Coinbase using a DeFi platform called AAVE 3.0 Artificial Intelligence Trading.

896. Having lulled Mr. Buchan into the scheme with the prospect of similar income, Ms. Gulnazar directed Mr. Buchan to download the Coinbase Wallet application and open the link for aav30.com using the Wallet’s browser. Mr. Buchan did as he was told.

897. Ms. Gulnazar directed Mr. Buchan to click on a link to purchase a mining certificate in order to join AAVE 3.0’s liquidity mining pool. Mr. Buchan did as he was instructed.

898. Mr. Buchan never believed—and had no reason to believe—that he had allowed Ms. Gulnazar or anyone else access to the funds in his Wallet. Indeed, Coinbase Wallet provided no warning to Mr. Buchan stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures had told Mr. Buchan that the *only* way someone could take his funds was if his “seed phrase” were stolen or compromised.

899. To fund the pool, Mr. Buchan deposited a total of \$87,105 in USDT into his Coinbase Wallet.

900. On March 22, 2022, scammers withdrew all of the USDT (approximately \$87,105) from Mr. Buchan’s Wallet. This withdrawal was done without Mr. Buchan’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

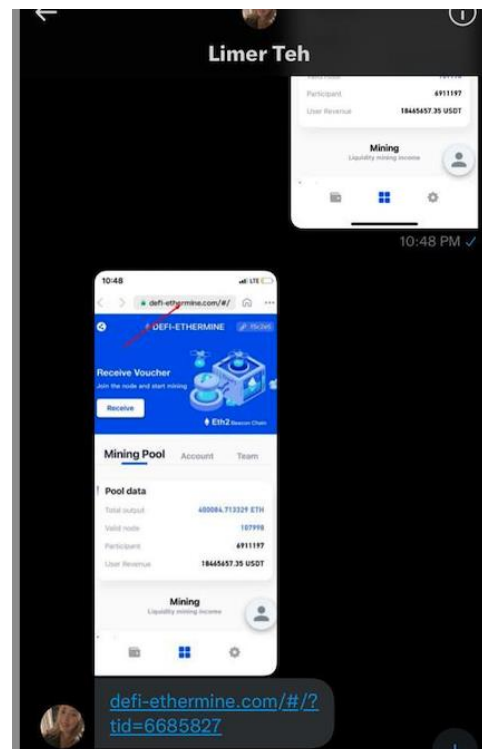
901. On March 22, 2022, Mr. Buchan notified Coinbase about the unauthorized transfer from his Coinbase Wallet. Coinbase responded that it “remains the customer’s responsibility to review the details of the dapps they interact with and understand the risk when interacting with them” and that “due to the irreversible nature of cryptocurrency protocols, transactions can neither be canceled nor reversed once confirmed on the blockchain.”

902. Mr. Buchan followed up and informed Coinbase that it was his understanding that his Wallet was safe, but he has now lost \$87,000 USDT. Coinbase had no interest in learning about or doing anything about the scam, or even shutting down or blocking the malicious dApp. Coinbase responded by informing Mr. Buchan that when he “created [his] Wallet, it generated a unique 12-word recovery phrase representing the private keys of the cryptocurrencies associated with your wallet” and that “once this recovery phrase is exposed to another party, they can use it to transfer funds without your authorization.” Coinbase then suggested that Mr. Buchan contact the FBI to report the incident.

903. Mr. Buchan followed up to Coinbase’s response by informing Coinbase that he never exposed his recovery phrase and that it was not until he tried to withdraw his money that it went elsewhere. Mr. Buchan sent another email to Coinbase informing them that its Wallet is being used to scam people. Coinbase responded by once again denying liability and informing Mr. Buchan that it “cannot help recover any Coinbase Wallet or transfer funds on your behalf.”

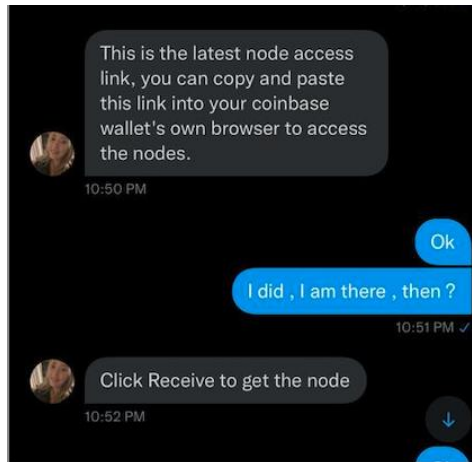
zzz. Ali Comert

904. On or about March 16, 2022, a person going by the name Limer Teh, who allegedly lived in Canada, contacted Claimant Ali Comert on Twitter. After befriending Mr. Comert, Ms. Teh informed Mr. Comert that she was earning significant income on Coinbase Wallet using a DeFi platform called defi-ethermine.com.



905. Having lulled Mr. Comert with the prospect of similar income, Ms. Teh directed Mr. Comert to download the Coinbase Wallet application and open the link for defi-ethermine.com using the Wallet’s browser. Mr. Comert did as he was told.

906. Ms. Teh directed Mr. Comert to click on a “node access link” in order to join defi-ethermine’s liquidity mining pool. Mr. Comert did as he was instructed.



907. Mr. Comert never believed—and had no reason to believe—that he had allowed Ms. Teh or anyone else access to the funds in his Wallet. Indeed, Coinbase Wallet provided no warning to Mr. Comert stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet’s disclosures had told Mr. Comert that the *only* way someone could take his funds was if his “seed phrase” were stolen or compromised.

908. To fund the pool, Mr. Comert deposited a total of \$89,661 in USDT into his Coinbase Wallet.

909. On or about March 16, 2022, scammers withdrew all of the USDT (approximately \$89,568) from Mr. Comert’s Wallet. This withdrawal was done without Mr. Comert’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

910. On March 17, 2022, Mr. Comert notified Coinbase about the unauthorized transfer from his Coinbase Wallet. Coinbase did not take any responsibility and suggested he contact the FBI.

911. On May 27, 2022, Coinbase sent an email to Mr. Comert in response to Complaint #10822152. Coinbase informed Mr. Comert that after “a review, we’ve determined that the transactions in question cannot be recovered or reversed, and we cannot reimburse your alleged

losses.” Moreover, Coinbase informed Mr. Comert that “[n]either Coinbase nor Toshi Holdings has any relationship with www.defi-ethermine.com or any person known to operate it” and only provides access to third party materials as a convenience.

912. At no time did Coinbase inform Mr. Comert that it was conducting an investigation into his complaint. Nor did Coinbase replenish Mr. Comert’s funds between March 17, 2022, and May 27, 2022, while it was conducting its investigation. Further, Coinbase did not even block the malicious dapp; it was still in operation months later.

913. Coinbase acknowledged that its “response to [Mr. Comert’s] formal complaint was not up to our standards” and issued him a credit of 200 USD in Bitcoin for the inconvenience.

aaaa. David Evdokimow

914. In October 2021, a person using the name LiLi Yang contacted Claimant David Evdokimow through Facebook.

915. After befriending Mr. Evdokimow, Ms. Yang insisted that he join a liquidity mining pool and directed him to download the Coinbase Wallet. Ms. Yang told Mr. Evdokimow that the Coinbase Wallet was the most secure wallet to join the liquidity mining pool. Mr. Evdokimow registered for the pool and paid the pool’s registration fee of \$100. This payment most likely initiated the malicious smart contract.

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

917. To fund the pool, Mr. Evdokimow linked his Coinbase.com account to his Coinbase Wallet and transferred USDT from his Coinbase.com account to his Coinbase Wallet.

918. Ultimately, Mr. Evdokimow deposited a total of \$492,449 USDT into his Coinbase Wallet.

919. On November 26, 2021, after Mr. Evdokimow was told to send money to a different account, he grew suspicious about the mining pool. That day, Mr. Evdokimow contacted Coinbase’s customer support who assured Mr. Evdokimow that his account was not compromised and that because of the two-step verification process no one would be able to access his funds without his permission.

920. Later that same day, a scammer, through an unauthorized transfer, stole all of the USDT from Mr. Evdokimow's Wallet, amounting to \$492,182.62.

921. Mr. Evdokimow contacted Coinbase's customer support several times after his Coinbase Wallet was drained. Coinbase denied liability and informed Mr. Evdokimow that it could not provide any further details about how his wallet was compromised, nor could it help recover the funds.

922. As set forth above, Mr. Evdokimow first reached out to Coinbase on November 25, 2021, in a customer service email titled "promotions associated with the liquidity mining pools." Coinbase responded in an auto-reply that its "team is working hard to answer customer inquiries in a timely manner" but that "longer response times" may be expected. Coinbase then responded that Mr. Evdokimow would need to contact the Dapp developer for specific questions or issues with Dapps." That evening, on November 26, 2021, Mr. Evdokimow called Coinbase *before* his wallet had been drained. During the phone call, customer service assured Mr. Evdokimow that his funds were secure and intact because no one could access his wallet without his permission. Because of this reassurance from Coinbase, Mr. Evdokimow took no steps to transfer his funds to a different wallet. That day, his funds were stolen.

923. Shortly after Mr. Evdokimow's funds were stolen, he called Coinbase support again, the representative that he spoke with did not help him and refused to address the issue with his supervisors, despite multiple requests from Mr. Evdokimow.

924. Mr. Evdokimow thereafter made multiple attempts to contact Coinbase, each was met with no real response. For example, on November 28, 2021, Coinbase wrote to Mr. Evdokimow stating that if he "did not authorize any outgoing transactions" it (incorrectly) meant that his "recovery phrase has been compromised" and Coinbase could not help. Coinbase urged him to report the theft to the FBI. On December 1, 2021, just a few days later, Coinbase told Mr. Evdokimow that they were closing his case.

925. On March 18, 2022, Coinbase contacted Mr. Evdokimow and informed him that "[a]fter an extensive review of the transaction details, your Wallet's history, and the addresses associated with it, the unauthorized activity you reported appears to have resulted from a signed

transaction dated Oct-10-2021 that approved a malicious third party transfer funds from your wallet.” Coinbase did not inform Mr. Evdokimow that it was conducting an investigation.

926. Between November 25, 2021, and March 18, 2022, Coinbase did not provisionally recredit or refund Mr. Evdokimow’s account for the unauthorized transfer. Nor did Coinbase correct the error. Instead, Coinbase denied liability for the unauthorized transfer: “[p]er the Coinbase Wallet terms of service (<https://wallet.coinbase.com/terms-of-service>), Coinbase does not warrant or endorse, and is not responsible for the availability or legitimacy of, the content, products or services on or accessible from third party dApps.”

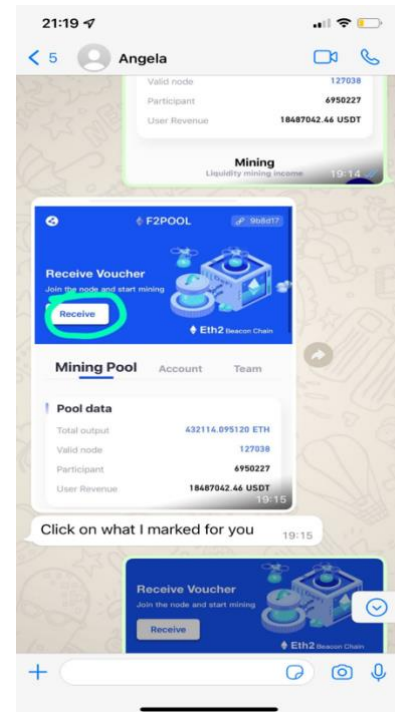
927. For months after Mr. Evdokimow reported the scam to Coinbase, Coinbase did not take down or block the malicious dapp, exposing other users to certain financial loss.

928. This has been a life changing event for Mr. Evdokimow. He is not working at the moment and feels enormous guilt for depriving his family of savings which the family needs right now.

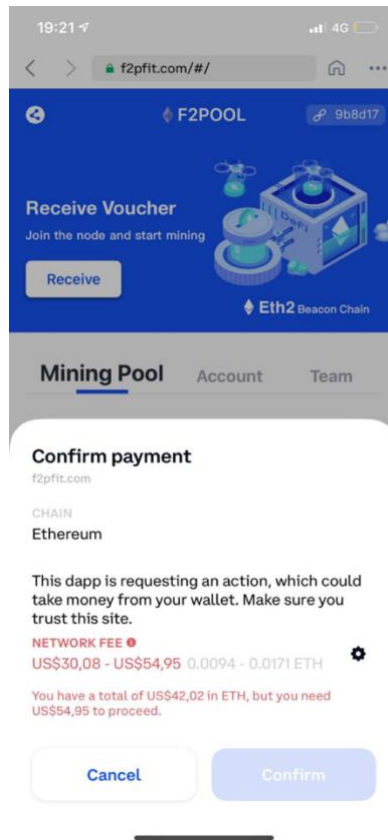
bbbb. Amine Fennane

929. On March 15, 2022, a person going by the name of Angela Andrew, who allegedly lived in Paris, contacted Claimant Amine Fennane on Instagram. After befriending Mr. Fennane through social media, Ms. Andrew introduced him to a liquidity mining pool that Ms. Andrew insisted he join through the Coinbase Wallet application. Ms. Andrew instructed Fennane to “[n]ow go to the app store and download the Coinbase wallet.” Mr. Fennane did as he was told.

930. Ms. Andrew directed Fennane to the F2Pool fraudulent mining pool located at <https://f2pfit.com/#/>. Ms. Andrew told Mr. Fennane to click on the receive voucher to join the liquidity mining pool. Mr. Fennane did as he was instructed, and this action most likely initiated the malicious smart contract.



931. During the process of joining the pool with the malicious, hidden smart contract, Mr. Fennane only received a warning that “This dapp is requesting an action, which could take money from your wallet” with a network fee of US \$30.08-54.95 listed below the warning. At no time did Mr. Fennane believe that he had allowed Ms. Andrew or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Mr. Fennane that anyone could access his Wallet to take his funds. Mr. Fennane believed he was only paying the Network Fee and not giving the scammers unlimited access to the funds in his Wallet.



932. At no time did Mr. Fennane believe that he had allowed Ms. Andrew or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Mr. Fennane stating that anyone could access his Wallet to take his funds.

933. To fund the pool, Mr. Fennane deposited a total of \$160,307 in USDT into his Coinbase Wallet.

934. Between April 6, 2022, and May 9, 2022, scammers withdrew all the USDT (approximately \$160,307) from Mr. Fennane’s Wallet without Mr. Fennane’s permission or consent. The withdrawal was also effected without any notification, warning, or substantive response from Coinbase.

935. Mr. Fennane’s contact with Coinbase’s customer support was entirely unhelpful. On May 19, 2022, Mr. Fennane contacted Coinbase’s customer support to report the unauthorized transfer. Coinbase responded by advising Mr. Fennane to cease “any further engagement with this scam, and we recommend reporting it to law enforcement agencies in your country.”

936. After analyzing how the scam worked, on June 6, 2022, Mr. Fennane contacted Coinbase again detailing how the scam works and requesting Coinbase to help recover his funds.

937. Coinbase responded in an auto-reply that its “currently receiving a high number of requests so we may take longer to respond, but our team is working hard to get to every inquiry quickly” and “please do not contact our partner banks, as they will be unable to assist you since your account is managed by Coinbase.” Coinbase followed up with an email explaining that “Coinbase Wallet and Standalone Wallet Extension are user-controlled and non-custodial, meaning that the private keys (representing ownership of the cryptocurrency via a 12-word seed phrase) for your wallet are not stored within a custodial or centralized exchange like Coinbase.com” and this “seed phrase can be imported to another non-custodial wallet like Metamask, Trust Wallet, etc. to access the funds. That said, if this seed has been exposed to another party, that party can use it to import your wallet to these non-custodial wallet providers and access your funds.”

938. On June 6, 2022, Mr. Fennane followed up with two additional questions for Coinbase support: (1) “How come that this DAPP can access the private key and then validate transactions?” and (2) “Why is coinbase wallet not informing users what is going on behind the scenes?”

939. Coinbase responded by informing Mr. Fennane that Coinbase “flagged this malicious dapp to our security and investigation teams to take the necessary action against the third party involved” and after “an extensive review of the transaction details, your Wallet’s history, and the addresses associated with it, the unauthorized activity you reported appears to have resulted from a signed transaction that approved the malicious dApp to transfer funds from your Wallet on Apr-06-2022... .” Coinbase then provided Mr. Fennane with the approval transaction from the malicious smart contract and told Mr. Fennane that this “transaction gave the address 0xe96738d136dab16c45ea87993a7c5ad0530f401a access to the funds held inside your Coinbase Wallet.” Coinbase did not acknowledge whether the approved transaction compromised Mr. Fennane’s recovery phrase.

940. In addition to losing his life savings, Mr. Fennane also took out loans from his family and financial institutions. Mr. Fennane has gone into substantial debt due to the unauthorized transactions from his Coinbase Wallet. Mr. Fennane feels depressed and frustrated and cannot sleep

properly since falling victim to this scam. He now acknowledges that he will have to work for many years to recover the money he lost and pay all his debts.

cccc. Vitaly Geyman

941. On or about May 13, 2022, a person going by the name Xin Zhang, who allegedly lived in Singapore and owned businesses in New York, contacted Claimant Vitaly Geyman on LinkedIn. After befriending Mr. Geyman, Ms. Zhang informed Mr. Geyman that she was earning significant income over Coinbase using a DeFi platform called ETH-CBASE.

942. Having lulled Mr. Geyman with the prospect of similar income, Ms. Zhang directed Mr. Geyman to download the Coinbase Wallet application and open the link for eth-cbase.com using the Wallet's browser. Mr. Geyman did as instructed.

943. Ms. Zhang directed Mr. Geyman to click on a link to pay a 60 ETH joining fee ("node" ticket) in order to join ETH-CBASE's liquidity mining pool. Mr. Geyman did as he was instructed.

944. Mr. Geyman never believed—and had no reason to believe—that he had allowed Ms. Zhang or anyone else access to the funds in his Wallet by purchasing a "node" ticket. Indeed, Coinbase Wallet provided no warning to Mr. Geyman stating that anyone could access his Wallet to take his funds. To the contrary, Coinbase Wallet's disclosures had told Mr. Geyman that the *only* way someone could take his funds was if his "seed phrase" were stolen or compromised.

945. To fund the pool, Mr. Geyman deposited a total of \$240,000 in USDT into his Coinbase Wallet.

946. On or about July 16, 2022, scammers withdrew all the USDT (approximately \$240,000) from Mr. Geyman's Wallet. This withdrawal was done without Mr. Geyman's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

947. Mr. Geyman brought this matter to Coinbase's attention and Coinbase told him that there was nothing that Coinbase could do, that they took no responsibility, and that they suggested that Mr. Geyman contact the FBI.

948. On or around July 20, 2022, Mr. Geyman contacted Coinbase's customer support to notify Coinbase about the unauthorized transfer. Coinbase replied and informed Mr. Geyman that "[a]fter an extensive review of the transaction details provided, the unauthorized activity you reported

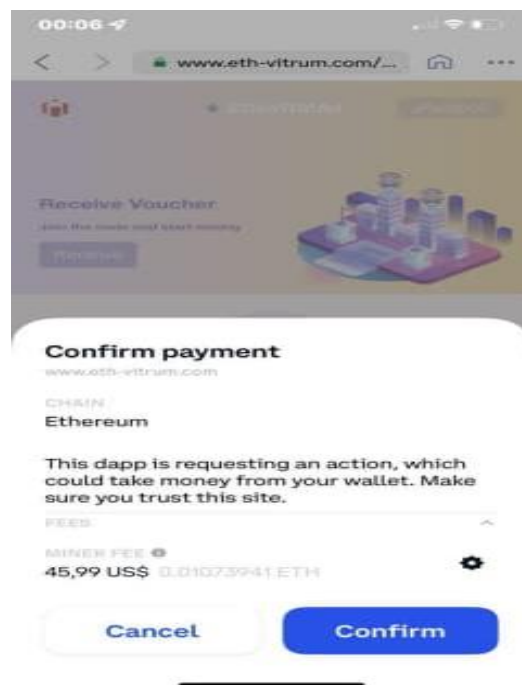
appears to have resulted from a signed transaction that approved a malicious third party to transfer funds from your Wallet on Jul-16-2022” and the “transaction gave the malicious third party access to the funds held inside your coinbase Wallet.” While Coinbase acknowledged and conceded that Mr. Geyman “**did not consent to this Approval transaction** with the intent of actively compromising your funds” because “transactions via Coinbase Wallet take place directly on the blockchain, it is not possible to revert them or recover the funds once you have signed the transaction and they are confirmed.” Coinbase suggested that Mr. Geyman contact the FBI Internet Crime Complaint Center (IC3) to report the incident. Coinbase did not take down or block the malicious dapp for weeks thereafter.

dddd. Shai Granovski

949. On October 20, 2021, a person going by the name Miriam, who allegedly lived in Hong Kong, contacted Claimant Shai Granovski through Instagram and informed Mr. Granovski of a way to join a liquidity mining pool. Miriam was an online friend of one of Mr. Granovski’s real life friends. Mr. Granovski’s friend informed Mr. Granovski that he did not know Miriam in real life, but Miriam seemed to be legitimate.

950. After gaining Mr. Granovski’s trust, Miriam directed Mr. Granovski to download the Coinbase Wallet app and on November 20, 2021, convinced Mr. Granovski to purchase a “node” to join the liquidity mining pool. Mr. Granovski did as he was instructed, and this action most likely initiated the malicious smart contract.

951. During the process of joining the pool with the malicious, hidden smart contract, Mr. Granovski only received a warning that “This dapp is requesting an action, which could take money from your wallet” with a network fee of \$45.99 listed below the warning. At no time did Mr. Granovski believe that he had allowed Miriam or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Mr. Granovski that anyone could access his Wallet rob him. Mr. Granovski believed he was paying only the “Network Fee” and not giving the scammers unlimited access to the funds in his Wallet.



952. To fund the pool, Mr. Granovski deposited a total of \$517,477 in USDT into his Coinbase Wallet.

953. On or around December 9, 2021, scammers withdrew all the USDT (approximately \$517,477) from Mr. Granovski’s Wallet. This withdrawal was done without Mr. Granovski’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

954. Mr. Granovski brought this matter to Coinbase’s attention and Coinbase told him that there was nothing that they could do, that they took no responsibility, and that they suggested that Mr. Granovski contact the FBI.

955. On or around December 14, 2021, Mr. Granovski contacted Coinbase’s customer support to notify Coinbase about the unauthorized transfer. Instead of conducting an investigation, Coinbase replied by informing Mr. Granovski that “if you did not authorize any outgoing transactions from your Coinbase Wallet, it means that your recovery phrase has been compromised” and that Coinbase could “not provide any further details about how it was compromised nor can we help recover these funds.”

956. On or around January 11, 2022, Mr. Granovski contacted Coinbase again to complain about the crypto stolen from his account. Once again, instead of conducting an investigation into whether Mr. Granovski’s recovery phrase was compromised or if something else occurred, Coinbase informed Mr. Granovski that “once this recovery phrase is exposed to another party, they can use it to transfer funds without your authorization” and that it “cannot provide any additional details about how it was compromised.”

957. Mr. Granovski lost his life savings due to this unauthorized transfer. Since the unauthorized transfer from his Wallet, Mr. Granovski has fallen into a severe depression.

eeee. Chris Haeusser

958. On or around June 24, 2021, a person using the name Wang Qi, who allegedly lived in Stuttgart, Germany, contacted Chris Haeusser through Facebook and WhatsApp to introduce him to a liquidity mining pool that she insisted he join through the Coinbase Wallet application.

```
[10/28/21, 8:27:28 PM] Wang Qi Kiki: I teach you to transfer your USDT to coinbase wallet. Because we invest in the coinbase wallet
[10/28/21, 8:27:43 PM] chris haeusser: <attached: 00000030-PHOTO-2021-10-28-20-27-43.jpg>
[10/28/21, 8:28:09 PM] chris haeusser: <attached: 00000031-PHOTO-2021-10-28-20-28-08.jpg>
[10/28/21, 8:28:26 PM] Wang Qi Kiki: <attached: 00000032-PHOTO-2021-10-28-20-28-26.jpg>
[10/28/21, 8:28:56 PM] chris haeusser: And to what
[10/28/21, 8:29:17 PM] Wang Qi Kiki: You long press this address to copy it. Tell me after you copy successfully
[10/28/21, 8:29:43 PM] Wang Qi Kiki: <attached: 00000035-PHOTO-2021-10-28-20-29-43.jpg>
[10/28/21, 8:29:54 PM] Wang Qi Kiki: Click this
[10/28/21, 8:30:04 PM] chris haeusser: Copy
[10/28/21, 8:30:09 PM] Wang Qi Kiki: Did you make it?
[10/28/21, 8:30:16 PM] chris haeusser: Yes
[10/28/21, 8:30:51 PM] chris haeusser: And now
[10/28/21, 8:30:58 PM] Wang Qi Kiki: <attached: 00000041-PHOTO-2021-10-28-20-30-58.jpg>
[10/28/21, 8:31:18 PM] Wang Qi Kiki: Go back to your coinbase and click on the place I marked for you
```

959. After months of communication, on November 26, 2021, Ms. Qi directed Mr. Haeusser to open his Coinbase Wallet and open the link for eth-event.co using the Wallet's browser. Mr. Haeusser did as he was instructed and entered into the mining pool.

```
[10/28/21, 8:54:09 PM] Wang Qi Kiki: https://eth-event.co/#/?code=77328282
[10/28/21, 8:54:19 PM] Wang Qi Kiki: Enter the URL of the mining pool in the place I marked. Enter it
[10/28/21, 8:55:38 PM] Wang Qi Kiki: Don't worry too much. All mining pools need to access it through a link. Take a screenshot for me after you enter. I teach you the next step
[10/28/21, 8:55:52 PM] chris haeusser: <attached: 00000089-PHOTO-2021-10-28-20-55-52.jpg>
[10/28/21, 8:56:13 PM] Wang Qi Kiki: <attached: 00000090-PHOTO-2021-10-28-20-56-13.jpg>
[10/28/21, 8:56:31 PM] Wang Qi Kiki: Click on it to get a proof of mining. He will have some safety prompts that you can operate according to the prompts.
[10/28/21, 8:56:35 PM] chris haeusser: <attached: 00000092-PHOTO-2021-10-28-20-56-34.jpg>
[10/28/21, 8:56:43 PM] chris haeusser: Click
[10/28/21, 8:56:47 PM] Wang Qi Kiki: yes
[10/28/21, 8:57:31 PM] chris haeusser: <attached: 00000095-PHOTO-2021-10-28-20-57-31.jpg>
[10/28/21, 8:57:34 PM] Wang Qi Kiki: Its security tips are very normal. This is a reminder that every mining pool will appear. Just like many people smoking will prompt the same reason that smoking is harmful to health.
```

960. At no time did Mr. Haeusser believe that he had allowed Ms. Qi or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Mr. Haeusser that anyone could access his Wallet to take his funds.

961. To fund the pool, Mr. Haeusser deposited a total of \$52,893 in USDT into his Coinbase Wallet account.

962. On November 26, 2021, scammers withdrew all the USDT (approximately \$52,893) from Mr. Haeusser's Wallet. This withdrawal was done without Mr. Haeusser's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

963. Mr. Haeusser brought this matter to Coinbase's attention in early December 2021 and Coinbase denied liability or fault for the unauthorized transaction. Coinbase also did not block the malicious dapp.

964. On or around January 23, 2022, Mr. Haeusser contacted Coinbase's customer support to notify Coinbase about the unauthorized transfer of USDT out of his Wallet. Coinbase responded in an auto-reply that it was in receipt of Mr. Haeusser's complaint and that Coinbase "will review your complaint and you will receive a response from Customer Complaints Officer within 15 business days" and that "[w]e hope there will never be a need for you to refer your complaint to the Financial Ombudsman Service but please be advised that our internal complaints process will need to be completed before the Financial Ombudsman Service will be able to look into your complaint."

965. On January 24, 2022, Coinbase responded to Mr. Haeusser’s complaint and informed him that “[i]t’s solely the user’s responsibility to review the details of the Dapp they interact with and understand the risk when interacting with it.” Coinbase did not immediately investigate the unauthorized transfer or provide Mr. Haeusser with any information regarding the wallet that his funds were transferred to.

966. Coinbase provided Mr. Haeusser with the following summary on how the scam worked. In this summary, Coinbase effectively admitted the security flaws in its Wallet, and further conceded that certain scams did not require the “seed-phrase” to steal the crypto, contrary to what Coinbase had previously represented to its customers:

Usually untrustworthy projects offering services such as mining pools are working with manipulated smart contracts. This means after connecting the wallet to the untrustworthy project, the user usually approves a transaction to add funds to the mining pools. **While the user thinks that he/she approved a one-off transaction (the amount they wish to invest into the project) untrustworthy projects work with manipulated smart contracts, that grants them the permission to remove all your funds from your wallet, once you submitted a transaction to them. For this type of scam the project does not need your seed-phrase.**

967. Instead, Coinbase informed Mr. Haeusser that “[a]lthough we have no official information on the third party you are inquiring about, we are happy to provide further background on how those types of potential scams work.” Coinbase then proceeded to detail how the fraudulent mining pool scam generally works and provided that “[w]hile the user thinks that he/she approved a one-off transaction (the amount they wish to invest into the project) untrustworthy projects work with manipulated smart contracts, that grants them the permission to remove all your funds you’re your wallet, once you submitted a transaction to them. For this type of scam the project does not need your seed-phrase.”

968. On March 11, 2022, Coinbase sent Mr. Haeusser an unsolicited email regarding his January 23, 2022, complaint. Coinbase informed Mr. Haeusser that “[a]fter a review, we’ve determined that Coinbase cannot recover or reverse the transaction in question.” Moreover, Coinbase informed Mr. Haeusser, in direct contradiction of its earlier response, that its “support investigation indicates that your 12 word recovery phrase was used in this alleged account compromise, and

imported into a wallet software outside of Coinbase Wallet to perform these transactions.” Coinbase never informed Mr. Haeusser that they were conducting an investigation into his complaint, nor did they replenish Mr. Haeusser’s Coinbase Wallet account while the investigation was pending.

969. Approximately three months after Mr. Haeusser’s initial complaint, on March 11, 2022, Coinbase contacted Mr. Haeusser unsolicited to inform him that Coinbase was “technically (and “physically”) unable to retrieve the funds that a third party allegedly transferred out of [his] Coinbase account” and that its “support investigation indicates that [Mr. Haeusser’s] 12 word recovery phrase was used in this alleged account compromise, and imported into a wallet software outside of Coinbase Wallet to perform these transactions.”

970. Mr. Haeusser lost his life savings because of this unauthorized transaction.

fff. Jianling Hao

971. On September 21, 2021, a person going by the name of Andy Zhang, who allegedly lived in the United States, contacted Claimant Jianling Hao on the dating site jiyuan.com. After befriending Ms. Hao, Mr. Zhang said that he could teach Ms. Hao a way to make stable returns through Coinbase for significant gains.

972. Mr. Zhang insisted that Ms. Hao download Coinbase Wallet, then deposit “money in coinbase, then exchange it for USDT, and then transfer it to wallet.”

[2/03/2022 00:19:34] Zhang Hang Andy: Have you slept yet?
[2/03/2022 00:33:49] Teresa Hao: No
[2/03/2022 00:34:27] Zhang Hang Andy: Teach you to mine in coinbase, and the benefits are considerable.
[2/03/2022 00:35:13] Teresa Hao: I don't understand, what is it?
[2/03/2022 16:24:08] Zhang Hang Andy: Baby, you're done early, you download coinbase and wallet first.
[2/03/2022 16:26:36] Teresa Hao: Downloaded.
[2/03/2022 16:27:02] Zhang Hang Andy: You have registered an account, and then tell me.
[2/03/2022 16:38:14] Teresa Hao: Okay.
[2/03/2022 16:39:32] Zhang Hang Andy: Then you make money in coinbase, then exchange it for USDT, and then transfer it to wallet.

42

⁴² WhatsApp chat between Mr. Zhang and Ms. Hao translated from Chinese to English.

973. After Ms. Hao set up her Coinbase Wallet account and transferred the USDT into her wallet, Mr. Zhang directed Ms. Hao to open the link for <https://eth-usdt.xyz/#/> through the Coinbase Wallet browser. Ms. Hao did as she was instructed and joined the mining pool.

[2/03/2022 19:09:36] Zhang Hang Andy: You return to the homepage and take a screenshot for me
[2/03/2022 19:10:10] Teresa Hao: The photo has been ignored
[2/03/2022 19:10:33] Zhang Hang Andy: The photo has been ignored
[2/03/2022 19:11:02] Zhang Hang Andy: You click on the place I marked
[2/03/2022 19:12:35] Zhang Hang Andy: Audio has been ignored
[2/03/2022 19:13:08] Zhang Hang Andy: [https://eth-usdt .xyz/#/](https://eth-usdt.xyz/#/)

974. While registering, Mr. Zhang directed Ms. Hao to click on the receive voucher button to join the pool. Ms. Hao did as she was instructed.

975. At no time did Ms. Hao believe that she had allowed Mr. Zhang or anyone else access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Ms. Hao that anyone could access her Wallet to take her funds.

976. To fund the pool, Ms. Hao deposited a total of \$80,000 USDT into her Coinbase Wallet.

977. Between March 29, 2022 and April 7, 2022, scammers withdraw all the USDT (approximately \$80,000) from Ms. Hao's Wallet. This withdrawal was done without Ms. Hao's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

978. Ms. Hao brought this matter to Coinbase's attention and Coinbase replied by denying liability or fault for the unauthorized transactions and told Ms. Hao that they could not reimburse or credit her wallet.

979. On April 25, 2022, Ms. Hao contacted Coinbase's customer support, in an email titled "Coinbase wallet for smart contract scammed." Coinbase responded with multiple auto-replies, the first one stated that "[i]n an effort to respond more rapidly to support requests, direct emails to this address are no longer enabled" and to "get a response from our support team, please visit the following page to submit a request: <https://help.coinbase.com/en/contract-us.html>." The second auto-reply stated

that “[o]ur team is working hard to answer customer inquiries in a timely manner, but you may experience longer response times.”

980. When Coinbase responded to Hao’s complaint, it simply told Hao that it “takes these reports very seriously, and will be flagging this malicious dapp to our security and investigation team”, that it “remains the customer’s responsibility to review the details of the dapps they interact with and understand the risk when interacting with them” and that Coinbase would not be able to reimburse or credit Hao’s wallet. On May 1, 2022, Coinbase closed Hao’s case.

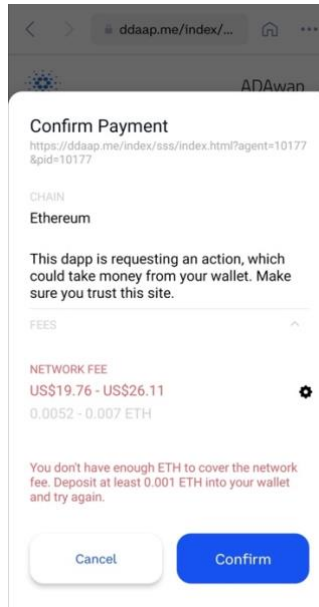
981. Ms. Hao lost her life savings and children’s educational fund because of these unauthorized transactions. This scam has devastated Ms. Hao’s life. She has become very ill and is suffering from serious depression.

gggg. E. Kong

982. On or around December 30, 2021, a person using the name Zijing Li contacted Claimant E. Kong through the dating app OKCupid and introduced him to the Coinbase Wallet application.

983. After befriending Mr. Kong, Ms. Li insisted he join a liquidity mining pool and directed him to download Coinbase Wallet. Ms. Li directed Mr. Kong to open the link for <https://i08.me/dnxXa> using the Wallet’s browser. Mr. Kong did as he was instructed.

984. Ms. Li then directed Mr. Kong to register with the dapp and transferred .006 Ethereum to Mr. Kong’s Wallet to pay for the registration fee.



985. During the process of joining the pool with the malicious, hidden smart contract, Mr. Kong only received a warning that “This dapp is requesting an action, which could take money from your wallet” with a network fee of \$19.76-\$26.11 listed below the warning. At no time did Mr. Kong believe that he had allowed Ms. Li or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Kong that anyone could access his Wallet to take his funds. Mr. Kong believed he was only paying the “Network Fee” and not giving the scammers unlimited access to the funds in his Wallet.

986. To fund the pool, Mr. Kong deposited a total of \$40,398 USDT into his Coinbase Wallet and transferred \$520,000 from his bank account directly to the scammers.

987. Between January 2022 and February 2022, scammers withdrew all the USDT (approximately \$40,398) from Mr. Kong’s Wallet. This withdrawal was done without Mr. Kong’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

988. On or around July 15, 2022, Mr. Kong contacted Coinbase’s customer support in an email titled “All USDT transferred out of wallet via smart contract attached by fraudulent dApp” to report his stolen crypto. Coinbase responded to Mr. Kong and informed him that it “remains the customer’s responsibility to review the details of the dapps they interact with and understand the risk when interacting with them. We recognize the difficult position this puts you in, but we cannot

reimburse or credit your wallet” and that Coinbase will be flagging the malicious dapp to its security and investigation teams.

989. As a result of this scam, in less than two weeks, Mr. Kong lost his life savings that took him over two decades to accumulate. This scam has devastated his life as he is no longer able to buy a house and is suffering immense guilt and shame; he occasionally gets panic attacks when thinking about his future. The financial losses and the trauma will take many years to recover from, if he is able to recover at all. Mr. Kong is also in considerable debt as part of the losses came from money borrowed under the influence, persuasion, and manipulation of the scammers.

hhhh. Alicia Lau

990. On or around May 29, 2021, a person going by the name of Toby Yan, who allegedly lived in London, contacted Claimant Alicia Lau (Lau Pu Mei) through Instagram. After befriending Ms. Lau, Mr. Yan encouraged Ms. Lau to join a liquidity mining pool from which he insisted she would be able to earn significant income. Mr. Yan directed Ms. Lau to deposit USDT into her Coinbase Wallet. Mr. Yan then directed Ms. Lau to open the link for eth-event.co through her Coinbase Wallet browser and provided Ms. Lau with the “voucher” fee to register and join the mining pool.

991. During the process of joining the pool, Ms. Lau received no warnings stating that she was giving any third parties access to withdraw crypto from her Coinbase Wallet.

992. To fund the pool, Ms. Lau deposited a total of \$205,744 USDT into her Coinbase Wallet.

993. Once the scammers increased the amount that Ms. Lau needed to deposit into her Coinbase Wallet to earn “bonuses,” she became suspicious of the pool, and on November 24, 2021, Ms. Lau contacted Coinbase’s customer support to inquire about the pool.

994. Between October 7, 2021, and December 2, 2021, the scammers, through unauthorized transactions, stole all of the USDT in Ms. Lau’s Coinbase Wallet, amounting to approximately \$205,743. These withdrawals were done without Ms. Lau’s permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

995. Ms. Lau contacted Coinbase’s customer support several times after realizing her Coinbase Wallet was drained. Coinbase denied liability or fault and informed Ms. Lau that “they could

not provide information as to why your Coinbase Wallet was compromised since Coinbase Wallet is a user-controlled and non-custodial product” and since “cryptocurrency transactions on the blockchain are irreversible, meaning once they are sent, there is no way to recover funds.”

996. Ms. Lau contacted Coinbase on December 4, 2021, in a customer service email titled “Is this liquidity mining backed by Coinbase?” Coinbase responded in an auto-reply that its “working hard to quickly address this issue, and we’ll reach out to you as soon as we have an update.” On December 5, 2021, Ms. Lau replied to Coinbase’s auto-reply and informed Coinbase that her “wallet had been compromised” and that \$200,000 had been stolen.

997. On December 6, 2021, still with no response from Coinbase, Ms. Lau once again contacted Coinbase and informed them that she had filed a complaint with IC3, and would appreciate if Coinbase could reverse all the unauthorized transactions back into her Wallet. On December 6, 2021, Coinbase finally responded to Ms. Lau and informed her that “[a]ccording to our records, the funds you asked about were successfully sent out of your Coinbase Wallet. If you did not authorize this, then it means that your Coinbase Wallet has been compromised.” Moreover, Coinbase did not immediately investigate the unauthorized transfer or provide Ms. Lau with any information regarding the wallet that her funds were transferred to.

998. To the contrary, Coinbase informed Ms. Lau that it “could not provide any information as to why your Coinbase Wallet was compromised since Coinbase Wallet is a user-controlled and non-custodial product. Only our users have full control of their wallets and solely responsible for taking care of their wallets’ security” and since “cryptocurrency transactions on the blockchain are irreversible, meaning once they are sent, there is no way to recover funds.” In its response, Coinbase also informed Ms. Lau that it was not affiliated nor connected with <https://eth-event.co>, the fraudulent mining pool.

999. Ms. Lau followed up with Coinbase and informed it that she did not share her seed phrase and did not authorize the transactions. Coinbase responded by stating “[t]o reiterate, Coinbase Wallet is a user-controlled and non-custodial product. Thus, we are unable to prevent your wallet from getting compromised since we do not have access to it.”

1000. Ms. Lau has lost her life savings, has gone into substantial debt from loans undertaken due to the trust she placed in Coinbase Wallet, and suffers from depression because of the unauthorized transactions.

iii. Richard Mokrý

1001. On July 23, 2022, a person using the name Sin Soledad contacted Claimant Richard Mokrý through Twitter. After befriending Mr. Mokrý, Ms. Soledad informed Mr. Mokrý about a liquidity mining pool that she insisted he join through the Coinbase Wallet application. Ms. Soledad directed Mr. Mokrý to visit and join her mining pool located at AI-SWAP.TOP.

1002. Having lulled Mr. Mokrý with the prospect of similar income, Ms. Soledad directed Mr. Mokrý to download the Coinbase Wallet application and open the link for AI-SWAP.TOP using the Wallet's browser. Mr. Mokrý did as he was told.

1003. After entering the link into his Coinbase Wallet browser, a pop-up window was displayed that said Mr. Mokrý was a lucky winner of a blockchain reward and the only way to get the reward was by clicking on a "got it" button, which entered Mr. Mokrý into the fraudulent mining pool.

1004. During the process of joining the pool, Mr. Mokrý received no warnings stating that by pressing on the "got it" button that he was giving any third parties access to withdraw all the crypto from his Coinbase Wallet.

1005. To fund the fraudulent mining pool, Mr. Mokrý deposited a total of \$26,201 USDT into his Coinbase Wallet.

1006. In August 2022, scammers withdrew all of the USDT (approximately \$26,201) from Mr. Mokrý's Wallet. This withdrawal was done without Mr. Mokrý's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1007. Mr. Mokrý brought this matter to Coinbase's attention and Coinbase told him that there was nothing that Coinbase could do, that they took no responsibility, and that they suggested that Mr. Mokrý contact the FBI.

1008. After notifying Coinbase about the unauthorized transfer, on August 5, 2022, Coinbase responded to Mr. Mokrý and informed him that "due to the nature of the blockchain, Coinbase has no way of knowing where these funds were sent" and as "a result, we are unable to provide specific

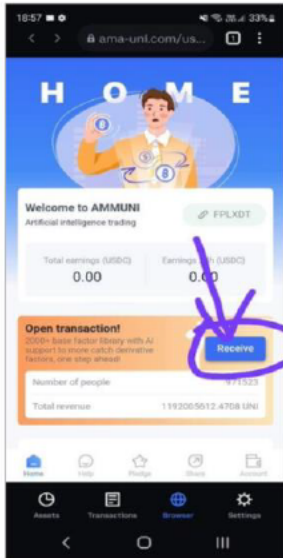
information on how your wallet was compromised.” Coinbase then suggested that if he has not done so already, Mr. Mokry “may want to report this incident to law enforcement.” Mr. Mokry filed an official complaint with the FBI Internet Crime Complaint Center.

jjjj. Morten Nilsen

1009. On August 7, 2022, a person using the name Hung Pham contacted Claimant Morten Nilsen through Facebook Messenger. After befriending Mr. Nilsen, Hung Pham informed Mr. Nilsen about a liquidity mining pool that Hung Pham insisted he join through the Coinbase Wallet application. Hung Pham directed Mr. Nilsen to visit and join Ammuni mining pool.

1010. Hung Pham directed Mr. Nilsen to download the Coinbase Wallet application and visit Ammuni’s URL at <https://www.ama-uni.com/usdc?d=3HAQLU> through the Wallet’s web browser. On August 21, 2022, following Hung Pham’s instructions, Mr. Nilsen registered for the pool through his Coinbase Wallet account. While registering, Hung Pham directed Mr. Nilsen to purchase a mining certificate to join the pool. Mr. Nilsen did as he was instructed.

Hung
As I told you yesterday, you need a coinbase wallet
Åpne
Hung
You need to download it from your mobile app store
Åpne
Hung
You’re in the middle of a session right now, I suggest you buy USDC after you finish the session, then download and register your Coinbase wallet and send the funds to your new wallet Contact me when you are done with the conference
Åpne



3LU

1011. During the process of joining the pool, which required him to press a button to connect, Mr. Nilsen received no warnings that he was giving Hung Pham or any third parties access to withdraw crypto from his Coinbase Wallet.

1012. To fund the pool, Mr. Nilsen deposited a total of \$155,888 USDC into his Coinbase Wallet.

1013. In August 2022, scammers withdrew all the USDC from Mr. Nilsen's Coinbase Wallet (approximately \$155,888). This withdrawal was done without Mr. Nilsen's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1014. On August 31, 2022, after becoming suspicious of the fraudulent mining pool, Mr. Nilsen attempted to contact Coinbase's customer support to complain about the unauthorized transfer but could not find a way to get help with his complaint. Mr. Nilsen later called Coinbase in Ireland, but customer support was not available at the time.

1015. On September 13, 2022, Mr. Nilsen contacted Coinbase's customer support after locating the appropriate contact to inform Coinbase that his Coinbase Wallet account had been drained. Coinbase denied liability or fault for the unauthorized transactions and told Mr. Nilsen that if he "did not confirm any outgoing transaction from your Wallet, we regret to inform you that this means the funds and the seed phrase are now compromised" and "Coinbase cannot recover the funds in these instances."

1016. Mr. Nilsen attempted to contact Coinbase's customer support as soon as he noticed the unauthorized transfer but was unable to locate the appropriate procedure to lodge his complaint. As a result, Mr. Nilsen called Coinbase in Ireland, but customer support was not available at the time. Mr. Nilsen then reported the unauthorized transfer to [reportfraud.ftc.gov](https://www.reportfraud.ftc.gov).

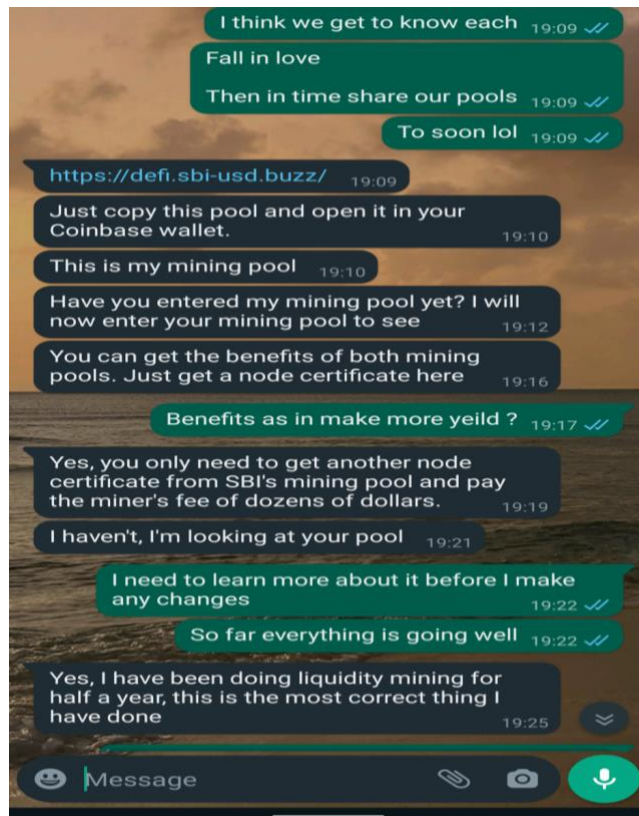
1017. On September 13, 2022, Mr. Nilsen notified Coinbase about the unauthorized transfer. Coinbase replied by informing Mr. Nilsen that if he "did not confirm any outgoing transactions from [his] Wallet, we regret to inform you that this means the funds and the seed phrase are now compromised." Moreover, Coinbase informed Mr. Nilsen that it was "unable to provide specific details on how your Wallet was compromised," because the transactions are part of an external

process, and due to that the transactions “cannot be reversed once they are confirmed on the blockchain, therefore Coinbase cannot recover the funds in these instances.” Coinbase then suggested that Mr. Nilsen contact the FBI Internet Crime Complaint Center to report the incident.

1018. Mr. Nilsen’s life has been devastated. He lost his life savings and his savings for his family. Mr. Nilsen also introduced his friends to the fraudulent liquidity mining pool, and they were also induced to deposit their money into the scam. Luckily his friends were able to retrieve their money before it was taken. Mr. Nilsen has gone from a very stable life to a life plagued by constant emotional stress due to this unauthorized transaction.

kkkk. Abdul-Azeez Oladapo

1019. On January 13, 2022, a person using the name Polly Naan contacted Claimant Abdul-Azeez Oladapo through the dating site Hinge. After befriending Mr. Oladapo, Ms. Naan informed Mr. Oladapo about a liquidity mining pool that she insisted he join through the Coinbase Wallet application. Ms. Naan directed Mr. Oladapo to visit and join her mining pool located at defi.sbi-usd.buzz and Defi-CTCS.com.



1020. After weeks of communication, on January 27, 2022, following Ms. Naan's instructions, Mr. Oladapo registered for the mining pool through his Coinbase Wallet account. While registering, Ms. Naan instructed Mr. Oladapo to purchase a mining certificate to join the mining pool. Mr. Oladapo did as he was instructed.

1021. During the process of joining the pool, Mr. Oladapo received no warnings stating that he was giving any third parties access to withdraw crypto from his Coinbase Wallet.

1022. To fund the fraudulent pool, Mr. Oladapo deposited a total of \$108,000 USDT into his Coinbase Wallet account.

1023. Between February 1, 2022, and February 11, 2022, the scammers, through unauthorized transactions, stole all of the USDT from Mr. Oladapo's Coinbase Wallet. This withdrawal was done without Mr. Oladapo's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1024. On February 13, 2022, Mr. Oladapo contacted Coinbase's customer support after realizing his Coinbase Wallet account had been drained. Coinbase denied liability or fault for the unauthorized transactions and told Mr. Oladapo that once his 12-word recovery phrase "is exposed to another party, they can use it to transfer funds without your authorization" and "due to the irreversible nature of cryptocurrency protocols, transactions can neither be canceled nor reversed once confirmed on the blockchain."

1025. After notifying Coinbase about the unauthorized transfers, on February 14, 2022, Coinbase responded to Mr. Oladapo and informed him that "once [his] recovery phrase is exposed to another party, they can use it to transfer funds without your authorization." Moreover, Coinbase did not immediately investigate the unauthorized transfer or provide Mr. Oladapo with any information regarding the wallet that his funds were transferred to. Coinbase never confirmed that Mr. Oladapo's seed phrase was actually compromised. Instead, Coinbase informed Mr. Oladapo that "[b]ecause your wallet is a user-controlled and non-custodial product, meaning that only you have full control/access (including the recovery phrase), we cannot provide any additional details about how it was compromised" and "[d]ue to the irreversible nature of cryptocurrency protocols, transactions can neither be canceled nor reversed once confirmed on the blockchain."

1026. On March 25, 2022, Mr. Oladapo filed a formal complaint with Coinbase concerning the unauthorized transfer from his account. On April 13, 2022, Coinbase responded to Mr. Oladapo's formal complaint and informed him that the "Disputes Team" is currently looking into his complaint and to please allow up to 20 business days for the Disputes Team to fully investigate his complaint. On April 29, 2022, Coinbase responded to Mr. Oladapo's formal complaint by informing him "[a]fter a review, we've determined that Coinbase cannot recover or reverse the transactions in question." At no time during Coinbase's investigation did it replenish Mr. Oladapo's account. Further, it appears that for at least a month after Mr. Oladapo reported the scam to Coinbase, the malicious dapp was still active.

1027. Mr. Oladapo lost his life savings and is no longer able to buy his mother a house because of these unauthorized transactions.

III. Mahmoud Osman

1028. On October 7, 2021, a person going by the name Lee Lena, who allegedly lived in the United States, contacted Claimant Mahmoud Osman through WhatsApp. After befriending Mr. Osman, Ms. Lena introduced him to Eth-Panda, a fraudulent liquidity mining pool.

1029. Ms. Lena directed Mr. Osman to download the Coinbase Wallet application and visit Eth-Panda's URL at <https://eth-panda.vip/#/> through the Wallet's web browser. On December 10, 2021, following Ms. Lena's instructions, Mr. Osman registered for the pool through his Coinbase Wallet account. While registering, Mr. Osman was required to pay a small fee in ETH to join the pool. Mr. Osman paid the fee as he was instructed to.

1030. During the process of joining the pool, Mr. Osman received no warnings that he was giving Ms. Lena or any third parties access to withdraw crypto from his Coinbase Wallet. Indeed, Ms. Lena, taking full advantage of Coinbase's security flaw, reassured Mr. Osman that as long as he kept his 12 word recovery phrase secure his crypto would be safe.

14/01/2022, 11:18 am – Lee Luna Number 3: I certainly believe unconditionally, you remember I told you, one of my beautiful BFF works in coinbase, I will know mining and understand so much because she shared with me, I am very grateful to her to let me know mining, I can get such a good reward
14/01/2022, 11:19 am – Lee Luna Number 3: My trust in them is unconditional trust, if I do not have enough trust in them I will not recommend them to you
14/01/2022, 11:22 am – Lee Luna Number 3: And as you have seen, the rewards are really paid to you four times a day and you can tell them to trust you and coinbase wallets just remember the 12 help words and no one can steal your funds as long as you protect the 12 help words and don't give them away.

1031. To fund the pool, Mr. Osman deposited a total of \$12,175 USDT into his Coinbase Wallet.

1032. In December 2021, scammers withdrew all the USDT from Mr. Osman’s Coinbase Wallet (approximately \$12,175). This withdrawal was done without Mr. Osman’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1033. On January 31, 2022, after becoming suspicious of the fraudulent mining pool, Mr. Osman contacted Coinbase’s customer support to confirm whether Coinbase was indeed partners with ETH-Panda. After several days and many emails later, Coinbase finally instructed Mr. Osman that ETH-Panda was a scam and that he should report it to his local law enforcement agency.

1034. After being contacted by the scammer to sign up for the fraudulent mining pool, on January 27, 2022, Mr. Osman emailed Coinbase’s customer support to specifically ask whether ETH-Panda was one of Coinbase’s partners and attached screenshots from the ETH-Panda mining pool. On January 27, 2022, Coinbase responded informing Mr. Osman that “DeFi Yield enables eligible Coinbase customers to receive variable interest rates on their crypto-assets by depositing them into third-party Defi protocols.” Mr. Osman replied to Coinbase’s email and informed them that he had been using ETH-Panda and was unsure if ETH-Panda is trustworthy and asked if Coinbase could confirm whether ETH-Panda is one of Coinbase’s partners.

1035. Based on Coinbase’s reply, Mr. Osman made additional deposits into Eth-Panda, one on January 27 and another on January 28, 2022.

1036. On February 2, 2022, Mr. Osman once again followed up with Coinbase to see whether ETH-Panda was indeed one of Coinbase’s partners. Coinbase responded by informing Mr. Osman that “Coinbase Wallet supports various networks such as Ethereum, Bitcoin, Litecoin, Stellar Lumens, and Ripple.” Coinbase did not confirm that ETH-Panda was one of its partners. Mr. Osman replied to

Coinbase’s response and specifically asked “Is coinbase a partner of (or in any type of way connected to) ETH-Panda?” Mr. Osman informed Coinbase that the question means quite a deal to him. Coinbase responded by stating “We’re always happy to help!”

1037. On February 10, 2022, Mr. Osman once again emailed Coinbase support and informed them that the “issue I am facing is that I did put a lot of money into ETH-Panda (<https://eth-panda.vip/#/?code=48740569>) and now they keep asking for me to put more and more money to release my funds. They keep insisting to be partnering with Coinbase and also show Coinbase as their official partner on their side.” Moreover, Mr. Osman informed Coinbase that he is “suspecting it is a scam. That is why I am asking for your confirmation on if you are working with them or if their claims of being an official partner with you is false.”

1038. Once again, Coinbase responded with an email asking Mr. Osman to “please elaborate what you meant by ETH-Panda and provide a screenshot of your issue, if applicable?” Mr. Osman replied to Coinbase’s email and reattached the screenshots he sent Coinbase in his initial complaint to the response.

1039. Finally, on February 10, 2022, Coinbase advised Mr. Osman to cease “any additional engagement with this scam” and recommended reporting it to law enforcement agencies in your own country and provided links to law enforcement agencies in the U.S., Canada, Europe, and the U.K. Coinbase then informed Mr. Osman that “Coinbase has no information or ownership of external cryptocurrency addresses, and because this is an external process, there is no way for Coinbase to cancel, reverse, or recover these funds-on your behalf.”

1040. When Mr. Osman responded to Coinbase’s email requesting a link to the government agency for “his” country, Malaysia, Coinbase did not provide a link to Malaysia’s government agency, instead it responded with an auto-generated message that informed Mr. Osman that “once [his] recovery phrase is exposed to another party, they can use it to transfer funds without your authorization” and because his “wallet is a user-controlled and non-custodial product, meaning that only you have full control/access (including the recovery phrase), we cannot provide any additional details about how it was compromised.”

1041. On February 11, 2022, Mr. Osman once again asked Coinbase for the website to report this scam to the law enforcement agency for his country. Coinbase once again responded with an auto-generated email informing Mr. Osman that “As previously mentioned, Coinbase Wallet is a user-controlled and non-custodial product which means that you – and only you – have access to your seed phrase and the ability to move your funds. Coinbase will never have access to you or any of our customers’ seed phrases. For this reasons, we cannot help recover any Coinbase Wallet or transfer funds on your behalf.”

1042. Coinbase’s customer support failed Mr. Osman on several fronts. First, Coinbase did not immediately inform Mr. Osman that it was not affiliated with Eth-Panda, which caused Osman to continue to invest in the fraudulent mining pool. Second, Coinbase failed to investigate Osman’s complaint that he may be involved in a scam mining pool. Finally, while Coinbase refused to investigate Mr. Osman’s claim, Coinbase would not provide Mr. Osman with information to the government agency that could assist with investigating the scam mining pool. Further, Coinbase did not take down the malicious dapp based on the information that Mr. Osman provided to Coinbase.

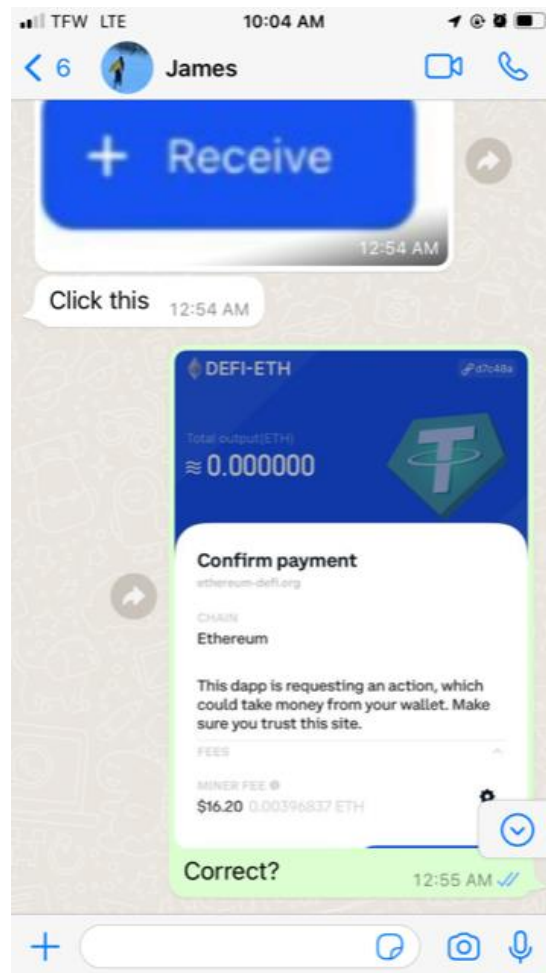
1043. Mr. Osman’s life has been devastated. He lost his life savings, his savings for his children, and is in debt to his friends and family. Mr. Osman introduced his friends to the fraudulent liquidity mining pool, and they were also induced to deposit their money into the scam. Mr. Osman now worries about how he will pay back the money he owes his friends and family, pay for his children’s education, pay for their health-related payments, and cover his family’s expenses. Mr. Osman has gone from a very stable life to a life plagued by constant emotional stress due to this unauthorized transaction.

mmmm. Jane Doe 4

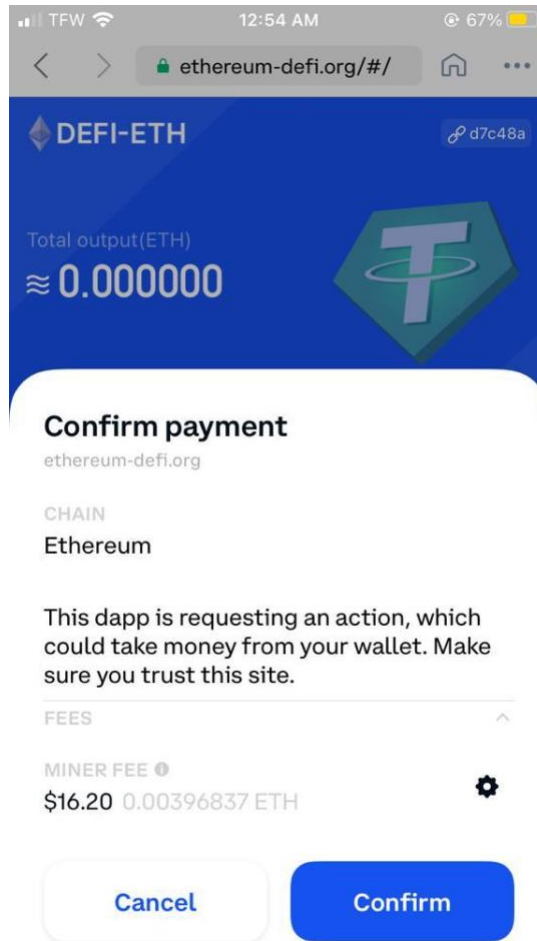
1044. On or around September 24, 2021, a person going by the name of James contacted Claimant Jane Doe 4 through Instagram. After befriending Jane Doe 4, James introduced her to a liquidity mining pool and directed Jane Doe 4 to download Coinbase Wallet.

1045. James directed Jane Doe 4 to the mining pool’s URL at www.ethereum-defi.org and instructed her to visit the website through her Coinbase Wallet browser. Jane Doe 4 did as she was instructed. James then directed Jane Doe 4 to click the Receive voucher button on the fraudulent

mining pool website. Jane Doe 4 did as she was instructed, and this action most likely initiated the fraudulent smart contract.



1046. During the process of joining the pool, Jane Doe 4 only received a warning that “This dapp is requesting an action, which could take money from your wallet” with a miner fee of \$16.20 listed below the warning. At no time did Jane Doe 4 believe that she had allowed James or anyone else access to the funds in her Wallet, and the Coinbase Wallet provided no warning to Jane Doe 4 that anyone could access her Wallet to take her funds. Jane Doe 4 believed she was only paying the “miner fee” and not giving scammers unlimited access to the funds in her wallet. To pay for the \$16.20 miner fee, James sent Jane Doe 4 \$81.42 ETH.



1047. To fund the fraudulent pool, Jane Doe 4 deposited a total of \$314,626 USDT into her Coinbase Wallet.

1048. Between December 11, 2021, and March 30, 2022, scammers withdrew all the USDT (approximately \$314,626) from Jane Doe 4's Wallet. This withdrawal was done without Jane Doe 4's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1049. On April 10, 2021, Jane Doe 4 tried to withdraw her funds from the liquidity mining pool. When she could not do so, she realized that the pool was fraudulent.

1050. Jane Doe 4 brought this matter to Coinbase's attention and Coinbase told her that there was nothing they could do, that they took no responsibility, and that "due to the irreversible nature of cryptocurrency protocols, transactions can neither be canceled nor reversed once confirmed on the blockchain."

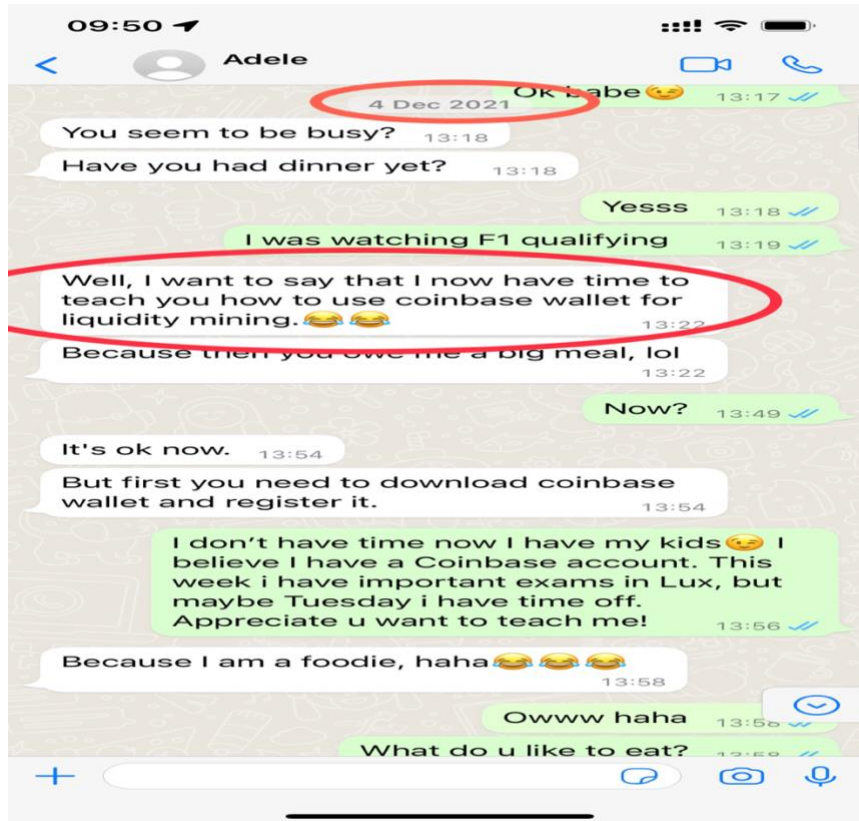
1051. On or about May 31, 2022, Jane Doe 4 notified Coinbase about the unauthorized transfers through Coinbase’s customer support chat option. Coinbase responded to Jane Doe 4 and informed her that “[i]t remains the customer’s responsibility to review the details of the dapps they interact with and understand the risk when interacting with them.” Coinbase did not immediately investigate the unauthorized transfer or provide Jane Doe 4 with any information regarding the wallet that her funds were transferred to. Instead, Coinbase informed Jane Doe 4 that “due to the irreversible nature of cryptocurrency protocols, transactions can neither be canceled nor reversed once confirmed on the blockchain.” Moreover, Jane Doe 4 asked Coinbase whether there should “be a security warning to indicate that by clicking a button to ‘receive’ a deposit from a dapp, I would be compromising my wallet for all future transactions?” Coinbase replied that “I completely understand how you feel right now and your frustration is valid, Sita” and then provided two links providing information on how to spot and avoid cryptocurrency scams. Neither link was relevant to the scam to which Jane Doe 4 fell victim. Moreover, despite the fact that Jane Doe 4 reported the specific malicious dapp to Coinbase, Coinbase did not block the app in the Wallet browser, even months later.

1052. Jane Doe 4 lost everything due to this unauthorized transaction. She has lost her life savings, her daughter’s education fund, and she owes \$110,000 in debts from loans she took out to fund the fraudulent pool. She is currently in a state of shock and has been socially withdrawn. It will take her years to recover from this devastating loss, if she is able to recover at all.

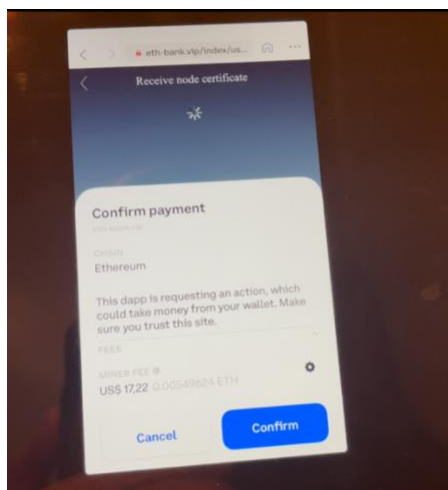
nnnn. Ivo van Reenen

1053. On December 3, 2021, a person using the name Adele, contacted Claimant Ivo van Reenen through the dating app Tinder. After befriending Mr. van Reenen, Adele introduced him to a high yield liquidity mining pool that she insisted he join through the Coinbase Wallet using the Dapp feature.

1054. Adele directed Mr. van Reenen to open the link to forethusdt.com through the Coinbase Wallet browser. Mr. van Reenen did as he was instructed and on December 7, 2021, Mr. van Reenen registered for the pool through his Coinbase Wallet account.



1055. During the process of joining the pool, Mr. van Reenen only received a warning that “This dapp is requesting an action, which could take money from your wallet” with a miner fee listed below of \$17.22. At no time did Mr. van Reenen believe that he had allowed Adele or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to van Reenen that anyone could access his Wallet to take his funds. Mr. van Reenen believed he was only paying the “miner fee” and not giving scammers unlimited access to the funds in his Wallet.



1056. To fund the pool, Mr. van Reenen deposited a total of \$81,279 USDT into his Coinbase Wallet.

1057. Mr. van Reenen became suspicious of the fraudulent pool when the scammer asked him to deposit additional funds to earn additional rewards.

1058. Between December 7, 2021, and December 18, 2021, scammers withdrew all the USDT (approximately \$81,279) from Mr. van Reenen's Coinbase Wallet. These withdrawals were done without Mr. van Reenen's permission or consent. They were also done without any notification, warning, or substantive response from Coinbase.

1059. Mr. van Reenen brought this matter to Coinbase's attention and Coinbase told him that there was nothing they could do, that they took no responsibility, and that "[a]ll Coinbase Wallet users have agree [sic] on the Terms of Service when creating a wallet, stating that our users are responsible for all activities involved in their wallets."

1060. After notifying Coinbase about the unauthorized transfers from his Wallet, on December 24, 2021, Coinbase responded to Mr. van Reenen and informed him that "[w]e are unable to provide specific information on how your wallet was compromised." Moreover, Coinbase did not immediately investigate the unauthorized transfer or provide Mr. van Reenen with any information regarding the wallet that his funds were transferred to. Coinbase never confirmed that Mr. van Reenen's seed phrase was actually compromised. After Mr. van Reenen followed up with several emails, Coinbase informed Mr. van Reenen that "[b]ecause your wallet is a user-controlled and non-custodial product, meaning that only you have full control/access (including the recovery phrase), we

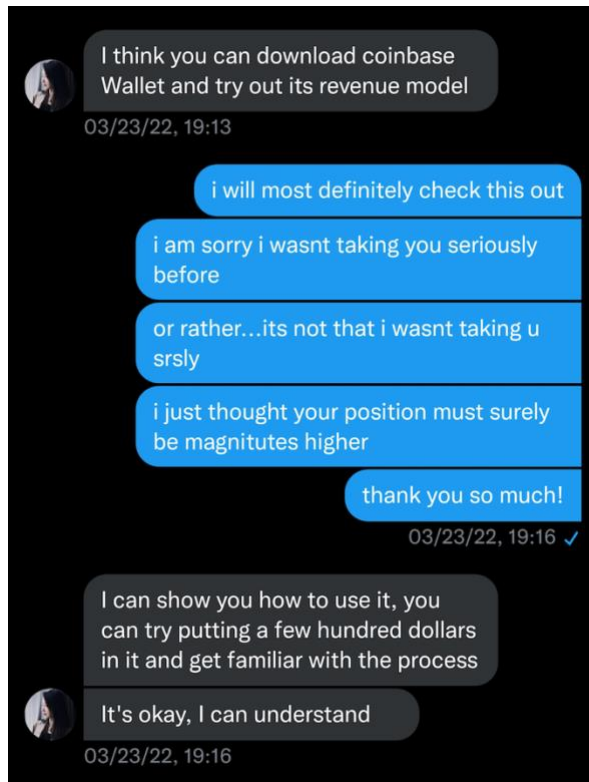
cannot provide any additional details about how it was compromised” and “[d]ue to the irreversible nature of cryptocurrency protocols, transactions can neither be canceled nor reversed once confirmed on the blockchain.”

1061. For weeks afterward, Coinbase did not take down or block the malicious dapp.

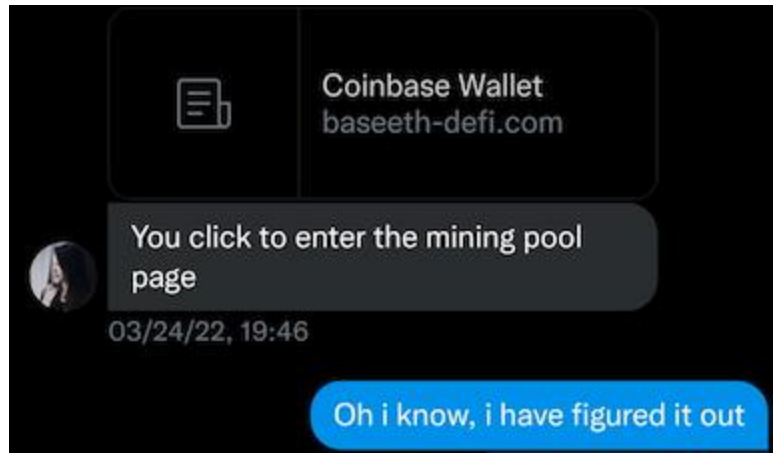
1062. These unauthorized transactions have devastated Mr. van Reenen. He lost his retirement fund and now suffers from depression. Mr. van Reenen is constantly concerned about how difficult it will be for him to make up for the loss of nearly \$82,000.

oooo. Miha Soršak

1063. On March 12, 2022, a person going by the name of Nicole contacted Claimant Miha Soršak through social media and introduced him to the idea of “loseless” liquidity mining through a liquidity mining pool. Nicole instructed Mr. Soršak to download the Coinbase Wallet app and deposit a few hundred dollars in it.



1064. Nicole then directed Mr. Soršak to open the baseeth-defi.com link through his Coinbase Wallet browser and click to enter the mining pool page. Mr. Soršak did as he was instructed.



1065. On March 25, 2022, Mr. Soršak purchased a “mining voucher” and registered for the pool through his Coinbase Wallet as he was instructed to do by Nicole, and this action most likely initiated the malicious smart contract.

1066. At no time did Mr. Soršak believe that he had allowed Nicole or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Mr. Soršak that anyone could access his Wallet to take his funds.

1067. To fund the pool, Mr. Soršak deposited a total of \$110,346 USDT into his Coinbase Wallet.

1068. In April 2022, scammers withdrew all the USDT (approximately \$110,346) from Mr. Soršak’s Wallet. This withdrawal was done without Mr. Soršak’s permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1069. On April 14, 2022, Mr. Soršak brought this matter to Coinbase’s attention and Coinbase told him that there was nothing they could do, that they took no responsibility, and that they could not reimburse or credit Mr. Soršak’s wallet.

1070. On or around April 14, 2022, Mr. Soršak contacted Coinbase’s customer support in an email titled “A dapp mining pool has frozen my funds and are threatening to take everything away from me in 9 days.” Coinbase responded to Mr. Soršak and informed him that it “remains the customer’s responsibility to review the details of the dapps they interact with and understand the risk when interacting with them. We recognize the difficult position this puts you in, but we cannot reimburse or credit your wallet” and that Coinbase will be flagging the malicious dapp to its security and investigation teams. After following up to Coinbase’s email, Coinbase informed Mr. Soršak that he

“may want to report this incident to law enforcement agencies in your jurisdiction“ and he could “submit a report to the FBI Internet Crime Complaint Center” because Coinbase “is willing to offer cooperation with law enforcement investigations pertaining to your compromised wallet.” Coinbase did not conduct its own investigation into the unauthorized transfer from Mr. Soršak’s Wallet or provide Mr. Soršak with any information regarding the wallet that his funds were transferred to.

1071. Mr. Soršak lost his entire life savings because of these unauthorized transactions. This experience has had a profoundly negative impact on Mr. Soršak’s life. Mr. Soršak had enormous difficulty eating and sleeping for several weeks after he was scammed. As a result, both his personal and professional life suffered. Mr. Soršak has been left with negative emotions such as shame, guilt, remorse, and unworthiness.

pppp. Paul Wilkinson

1072. On November 23, 2021, a person going by the name Jessica, who allegedly lived in the United States, contacted Claimant Paul Wilkinson through Instagram. After befriending Mr. Wilkinson through WhatsApp, Jessica informed Mr. Wilkinson about how he could earn passive income from a liquidity mining pool through the Coinbase Wallet application.

1073. Jessica directed Mr. Wilkinson to download the Coinbase Wallet application and visit the cbdefi.net link through the Wallet’s browser. On December 8, 2021, Mr. Wilkinson purchased the mining certificate or voucher, as directed by Jessica, and registered for the pool through his Coinbase Wallet account.

1074. During the process of joining the pool, Mr. Wilkinson received no warnings stating that he was giving Jessica or any third parties access to withdraw crypto from his Coinbase Wallet. Indeed, Jessica, taking full advantage of Coinbase’s security flaw, reassured Mr. Wilkinson that as long as he kept his 12 word recovery phrase secure “the world’s top hackers can’t steal your account funds.”

[05/12/2021, 16:17:38] Paul Wilkinson: No, this is great :) I'll start with this page and then do more research on how to create an account, set it up, pay into it etc. and what the risks are. :)

[05/12/2021, 16:22:22] Jessica: You only need to download the Coinbase wallet, register your account, and remember the twelve keys of the wallet. As long as you remember the twelve keys of your wallet, the world's top hackers can't steal your account funds.

[05/12/2021, 16:26:34] Jessica: You register your account, and I will teach you how to get the mining certificate. This mining certificate is a one-time charge. All you have to do is buy USDT from the exchange and transfer it into your wallet. Just like me, you can earn passive income every day, and you can earn ETH every day. You can choose a suitable price to sell the ETH you earn.

[05/12/2021, 16:31:35] Paul Wilkinson: You made it sound so simple. That's exactly what I wanted to know. I'll read the website later after I've walked the dog again. Thank you!!

1075. To fund the pool, Mr. Wilkinson deposited a total of \$70,843 USDT into his Coinbase Wallet.

1076. After informing Jessica that he had no more money to deposit into the pool, scammers withdrew all of the USDT (approximately \$70,843) from Mr. Wilkinson's Coinbase Wallet. This withdrawal was done without Mr. Wilkinson's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1077. Mr. Wilkinson brought this matter to Coinbase's attention and Coinbase told him that there was nothing they could do. Coinbase denied responsibility and told Mr. Wilkinson that Coinbase "users have agree [sic] on the Terms of Service when creating a wallet stating that our users are responsible for all activities involved in their wallets."

1078. After notifying Coinbase about the unauthorized transfers from his Wallet, on December 14, 2021, Coinbase responded to Mr. Wilkinson requesting additional information about the transfers from his account. Mr. Wilkinson replied by providing screenshots of the unauthorized transfers from his account and informed Coinbase that a total of \$70,699 USDT was illegally removed/stolen from his wallet without his knowledge.

1079. On December 16, 2021, Coinbase responded to Mr. Wilkinson's complaint and informed him that the "unauthorized activity you reported appears to have resulted from a signed transaction on (Dec-08-2021 01:54:57 PM +UTC) that approved a malicious third party to transfer funds from your Wallet." Mr. Wilkinson replied and described his interaction with the fraudulent liquidity mining pool and stated that his crypto being stolen is due to a security vulnerability within the Coinbase Wallet app. On December 20, 2021, Coinbase responded to Mr. Wilkinson and provided quotes from Coinbase Wallet's terms of service, including that "Coinbase does not warrant or endorse,

and is not responsible for the availability or legitimacy of, the content, products or services on or accessible from third party dApps” and since “users have agree on the Terms of Service when creating a wallet stating that our users are responsible for all activities involved in their wallets” that “Coinbase Wallet is not covered by our Insurance Policy.”

1080. On December 26, 2021, Mr. Wilkinson replied to Coinbase’s response and reiterated his position that his crypto was stolen due to a security vulnerability in Coinbase Wallet’s app and that he has lodged a formal complaint and would be referring his complaint to the Financial Ombudsman Service. On January 12, 2022, Coinbase closed Mr. Wilkinson’s case and offered no further response to Mr. Wilkinson.

1081. Mr. Wilkinson filed his formal complaint with Coinbase on December 21, 2021, and Coinbase responded on January 9, 2022, requesting an additional 20 business days to complete its investigation. At no time during Coinbase’s investigation did Coinbase replenish Mr. Wilkinson’s funds. On February 8, 2022, Coinbase provided a response to Mr. Wilkinson’s formal complaint and informed Mr. Wilkinson that “Coinbase cannot recover or reverse the transactions in question” and denied his complaint. On March 1, 2022, Mr. Wilkinson requested the full results from Coinbase’s investigation. Coinbase never replied to Mr. Wilkinson’s request for the results from its investigation into the unauthorized transfers from his account. Coinbase also did not take down or block the malicious app – cbdefi.net. As of mid-September 2022, that dapp was still active and fully accessible, with no warning signs from Coinbase.

1082. Mr. Wilkinson lost his entire life savings because of these unauthorized transactions. Mr. Wilkinson’s life has been wrecked due to this unauthorized transfer. He has sunken into a deep depression, and the loss has totally destroyed his confidence (in all aspects of his life including his professional career) as he is always questioning whether something nefarious is going on.

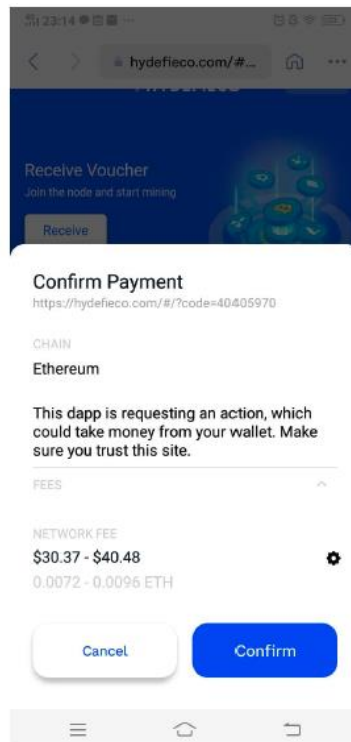
qqqq. Edmund Yeo

1083. On November 16, 2021, a person going by the name Juli Chua contacted Claimant Edmund Yeo through WhatsApp. After befriending Mr. Yeo, Ms. Chua introduced him to a liquidity mining pool and directed Mr. Yeo to join through the Coinbase Wallet application.

11/19/21, 10:53 - Edmund Yeo: Can I buy USDT and transfer to [coinbase](#)?
 11/19/21, 10:54 - Edmund Yeo: Using [Huobi](#)
 11/19/21, 10:54 - Juli Chua: This wallet can be purchased directly without USDT.
 11/19/21, 10:54 - Juli Chua: Yes, of course.
 11/19/21, 10:54 - Juli Chua: Do you have your own coin?
 11/19/21, 10:54 - Juli Chua: Do you have this trading platform?
 11/19/21, 10:55 - Edmund Yeo: I can open
 11/19/21, 10:55 - Juli Chua: OK, then you can open an account now.
 11/19/21, 10:55 - Edmund Yeo: So I buy USDT and transfer to [coinbase](#)
 11/19/21, 10:55 - Juli Chua: Yes,
 11/19/21, 10:56 - Juli Chua: Copy USDT's address to wallet
 11/19/21, 10:56 - Juli Chua: How much uSDT are you going to buy?
 11/19/21, 10:57 - Juli Chua: I suggest you buy 30000USDT T. I'll apply for an activity for you, and you can apply for an ETH.

1084. Ms. Chua directed Mr. Yeo to visit the [Hydefieco.com](#) liquidity mining pool through the Coinbase Wallet browser, and on November 23, 2021, Mr. Yeo, at the direction of Ms. Chua, registered for the pool through his Coinbase Wallet account and pressed “confirm” to purchase a “voucher,” and this action most likely initiated the malicious smart contract.

1085. During the process of joining the pool, Mr. Yeo only received a warning that “This dapp is requesting an action, which could take money from your wallet” with a Network Fee of \$30.37 - \$40.48 listed below the warning. At no time did Mr. Yeo believe that he allowed Ms. Chua or anyone else access to the funds in his Wallet, and the Coinbase Wallet provided no warning to Mr. Yeo that anyone could access his Wallet to take his funds. Mr. Yeo believed he was only paying a Network Fee and not giving scammers unlimited access to the funds in his Wallet.



1086. To fund the pool, Mr. Yeo deposited a total of \$346,652 USDT into his Coinbase Wallet.

1087. Between December 8, 2021, and January 7, 2022, scammers withdrew all of the USDT (approximately \$346,652) from Mr. Yeo's Coinbase Wallet. This withdrawal was done without Mr. Yeo's permission or consent. It was also done without any notification, warning, or substantive response from Coinbase.

1088. Mr. Yeo brought this matter to Coinbase's attention and was told there was nothing Coinbase could do. Coinbase denied responsibility, and told Mr. Yeo that Coinbase could not cancel, reverse, or recover these funds on his behalf.

1089. After contacting Coinbase to inquire about the fraudulent mining pool "hydefieco.com", on December 9, 2021, Coinbase responded to Mr. Yeo and informed him that a "liquidity pool is a group of funds locked in a smart contract that ensures liquidity of those funds for trading, borrowing, and lending. Liquidity pools provide the infrastructure for many decentralized exchanges (DEXes) like Uniswap, 1inch, and Sushiswap. Traders interact with liquidity pools by providing an equal value of two tokens to a pool to create a market. These traders are called liquidity providers (LPs) and earn trading fees for performing this service." Because of this, Mr. Yeo engaged with hydefieco.com and joined the fake liquidity mining pool. At no time did Coinbase inform Mr. Yeo that it was not associated with "Hydefieco.com."

1090. On January 4, 2022, after Mr. Yeo's funds were stolen, Mr. Yeo notified Coinbase about the unauthorized transfers. Coinbase responded asking for screenshots to show the trouble Mr. Yeo was having. Mr. Yeo responded by providing screenshots from the fraudulent mining pool and explaining the issues he was having. Coinbase then responded by informing Mr. Yeo that Coinbase "advise ceasing any additional engagement with this scam, and we recommend reporting it to law enforcement agencies in your country." Coinbase further explained that "[u]nless Coinbase announce an official partnership or affiliation with a 3rd party, any claims made detailing otherwise are not legitimate."

1091. Mr. Yeo lost his entire life savings and retirement fund because of these unauthorized transactions. This experience has brought a lot of financial, mental, and emotional stress into Mr. Yeo's life. In addition to losing his life savings, he devastatingly lost his mother's and sister's life

savings as well. Mr. Yeo is currently undergoing dialysis treatment for chronic kidney failure and desperately needs the funds for his daily survival.

* * *

As detailed above, each Claimant suffered enormous damages that Coinbase could and should have prevented.

H. Coinbase has failed to disclose the problems with its Wallet to investors through its SEC filings.

a. Coinbase’s SEC filings did not disclose the Wallet’s security flaws.

1092. In addition to the losses incurred by Claimants and other Coinbase Wallet customers, Coinbase failed to disclose the problems with its Wallet to investors through its SEC filings.

1093. Coinbase’s SEC filings reflect the importance of their Wallet functionality for the Company’s success. In addition, Coinbase has repeatedly informed investors that wallet security, both custodial and non-custodial, is a material issue that could affect the Company’s financial performance.

1094. Coinbase went public in a direct listing on or about April 14, 2021. In its publicly filed April 1, 2021 S-1, Coinbase stated that although their Wallet operates “separately” from Coinbase’s main platform, “wallet users are included in the following key business metrics: Verified Users and Monthly Transacting Users.”⁴³

1095. After going public, Coinbase was obligated to file quarterly 10-Q financial reports with the SEC. In its 10-Q filed on November 10, 2021, which represented results from third quarter of 2021 (July 1 to September 30, 2021), Coinbase bragged that the Wallet “enables users to participate in the cryptoeconomy, without intermediaries, including access to DeFi apps, NFT marketplaces, and sending and receiving crypto.”⁴⁴ The 10-Q also noted that in Q3 of 2021, Coinbase “expanded Wallet functionality through investments in deeplinking the Coinbase Wallet to our main Consumer app. This expanded software functionality provides our users access to DeFi to trade more than 2,000 crypto

⁴³ <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001679788/50ece2a0-8e87-4471-8df0-ff6fb8d1b19c.pdf>

⁴⁴ <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001679788/96565d20-f38b-49e3-a725-0e656b940b09.pdf>

assets.” Coinbase’s 10-Q also touted the company’s “enhanced security features,” stating that the Company was “committing to providing [their] customers with the highest levels of security to protect their crypto assets.” Coinbase noted that it provided two-factor authentication that provided “phishing-resistant security against bad actors.” With respect to theft from “Crypto asset wallets,” Coinbase, recognizing the importance of this issue, noted, with respect to the crypto that it held in its own custody:

The Company has committed to securely store all crypto it holds on behalf of users. As such, the Company may be liable to its users for losses arising from theft or loss of user private keys. The Company has no reason to believe it will incur any expense associated with such potential liability because (i) it has no known or historical experience of claims to use as a basis of measurement, (ii) it accounts for and continually verifies the amount of crypto assets within its control, and (iii) it has established security around custodial private keys to minimize the risk of theft or loss. Since the risk of loss is remote, the Company had not recorded a liability at September 30, 2021 or December 31, 2020.

1096. As noted above, the crypto mining liquidity scams began in the fourth quarter of 2021. To succeed, these scams relied on the Wallet’s poor user interface and incompetent customer service. In its February 25, 2022 10-K annual report (filed for the 2021 calendar year), however, Coinbase again repeatedly touted the company’s security and claimed that customers had “not lost funds due to a security” breach on Coinbase’s platform:

We have made significant investments in regulatory compliance and cybersecurity to earn the trust of our customers in over 100 countries. We work with regulators and law enforcement agencies around the world to drive policy and practices favorable to the cryptoeconomy, and to ensure we are licensed as appropriate under local law. **We are proud to be one of the longest-running crypto platforms where customers have not lost funds due to a security breach of the platform, and we secure our customers’ funds with multiple layers of protection by employing what we believe to be the largest hot wallet security program in the insurance market.**

1097. Additionally, the annual report, in disclosing risks faced by Coinbase, acknowledged that security, as well as the loss of customer assets, was one of the Company’s top concerns. The Company also explained that it understood the security risks associated with smart contracts. For example, Coinbase noted:

[I]n addition, assets held by the smart contract in reserves may be stolen, misused, burnt, locked up or otherwise become unusable and irrecoverable. These super users can also become targets of hackers and malicious attackers. If an attacker is able to access or obtain the super user privileges of a smart contract, or if a smart contract’s super-users or core community members take actions that adversely affects the smart

contract, our customers who hold and transact in the affected crypto assets may experience decreased functionality and value of the applicable crypto assets, up to and including a total loss of the value of such crypto assets. Although we do not control these smart contracts, any such events could cause customers to seek damages against us for their losses, result in reputational damage to us, or in other ways adversely impact our business.

1098. Further, Coinbase repeated the “crypto asset wallets” section that it had included in the 2021 Q3 10-Q filing. Coinbase assured its investors with respect to the crypto that the Company itself held:

The Company has committed to securely store all crypto assets it holds on behalf of users. As such, the Company may be liable to its users for losses arising from theft or loss of user private keys. The Company has no reason to believe it will incur any expense associated with such potential liability because (i) it has no known or historical experience of claims to use as a basis of measurement, (ii) it accounts for and continually verifies the amount of crypto assets within its control, and (iii) it has established security around custodial private keys to minimize the risk of theft or loss. **Since the risk of loss is remote**, the Company had not recorded a liability at December 31, 2021 or December 31, 2020.

1099. Coinbase also made clear that use of the Wallet was an important metric for Coinbase’s success. In its 2021 Q1 10-Q, filed on May 10, 2022, Coinbase stated: “During the first quarter of 2022, we made good progress on our product development, highlighted by the beta launch of Coinbase NFT in April 2022, **growing adoption of Coinbase Wallet**, expansion of our staking offering through the addition of Cardano, and hiring of over 1,200 full-time employees to help us build the future of crypto.”⁴⁵

1100. Coinbase made no mention of the significant security flaws in the Wallet. To the contrary, the company again touted its security with regards to its custodial “Crypto asset wallets” telling investors, in a paragraph copied nearly verbatim from prior filings, that:

The Company has committed to securely store all crypto assets it holds on behalf of users. As such, the Company may be liable to its users for losses arising from theft or loss of user private keys. The Company has no reason to believe it will incur any expense associated with such potential liability because (i) it has no known or historical experience of claims to use as a basis of measurement, (ii) it accounts for and continually verifies the amount of crypto assets within its control, and (iii) it

⁴⁵ <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001679788/89c60d81-41a2-4a3c-86fb-b4067ab1016c.pdf>

has established security around custodial private keys to minimize the risk of theft or loss. Since the risk of loss is remote, the Company had not recorded a liability at March 31, 2022 or December 31, 2021.

1101. In explaining business risks to investors, Coinbase noted that the Company has “built [its] reputation on the premise that [its] platform offers customers a secure way to purchase, store and transact in crypto assets. As a result, any actual or perceived security breach of us or our third-party partners may ... harm our reputation and brand [and] ... lead to theft or irretrievable loss of our or our customers’ fiat currencies or crypto assets.” The 10-Q then continued on to explain how the company has developed systems and processes designed to protect its own security and that of its customers, while at the same time ignoring the significant security flaws in the Wallet.

1102. The 10-Q did, however, acknowledge the risk of supporting smart contracts “deployed on a third-party blockchain”:⁴⁶

In addition, assets held by the smart contract in reserves may be stolen, misused, burnt, locked up or otherwise become unusable and irrecoverable. These super users can also become targets of hackers and malicious attackers. If an attacker is able to access or obtain the super user privileges of a smart contract, or if a smart contract’s super-users or core community members take actions that adversely affects the smart contract, our customers who hold and transact in the affected crypto assets may experience decreased functionality and value of the applicable crypto assets, up to and including a total loss of the value of such crypto assets. Although we do not control these smart contracts, any such events could cause customers to seek damages against us for their losses, result in reputational damage to us, or in other ways adversely impact our business.

1103. Thus, Coinbase clearly understood the risk that smart contracts posed to customer assets. And, when speaking to investors about these risks, Coinbase chose to conceal that Coinbase

⁴⁶ Coinbase, in its Q1 2022 10-Q (p. 80) continued to acknowledge the risk that its outsourced customer service posed: “We rely on third parties in connection with many aspects of our business, including payment processors, banks, and payment gateways to process transactions; cloud computing services and data centers that provide facilities, infrastructure, website functionality and access, components, and services, including databases and data center facilities and cloud computing; as well as third parties that provide outsourced customer service, compliance support and product development functions, which are critical to our operations. Because we rely on third parties to provide these services and to facilitate certain of our business activities, we face increased operational risks.”

Wallet users had already repeatedly complained to Coinbase that these smart contracts had resulted in the complete depletion of their assets.

b. Coinbase executives dumped stock while their customers suffered massive and financially catastrophic losses.⁴⁷

1104. Despite the fact that Coinbase Wallet’s customers essentially lost their life savings without reimbursement for Coinbase’s porous security in the Wallet, Coinbase executives, while touting their products, sold off enormous quantities of Coinbase stock, resulting in high paydays.

1105. On April 14, 2021, the very first day of Coinbase’s direct listing, Surojit Chatterjee, Coinbase’s Chief Product Officer, sold nearly \$62 million in Coinbase stock.⁴⁸ Square Ventures, a major shareholder, sold nearly \$1.5 billion; Jennifer Jones, the Chief Accounting Officer sold \$43 million, Emilie Choi, Coinbase’s President, sold nearly \$100 million; Brian Armstrong, Coinbase’s CEO, sold nearly \$300 million; Alesia Haas, Coinbase’s CFO, sold \$100 million.

1106. These sales continued throughout the fall and winter of 2021. For example, Chief Legal Officer Paul Grewal sold nearly \$12 million in stock on August 31, 2021, and another \$10 million in stock on September 23. As the crypto liquidity scam picked up speed, Grewal sold nearly \$8 million in stock on October 21, 2021, \$1.4 million in stock on November 22, 2021, and more than \$200,000 in stock on February 25, 2022. Chatterjee, the product designer, made repeated huge dollar volume sales through this time-period as well, selling nearly \$6 million in October 2021, \$20 million in November 2021, \$9 million in December 2021, and \$2.5 million in January 2022. Other insiders, such as Jones and Choi also made major stock sales.

1107. Outside of shares issued in options grants, not a single major executive purchased any Coinbase shares from April 14, 2021 through at least August 1, 2022.

⁴⁷ Last updated on or about August 1, 2022.

⁴⁸ <https://web.archive.org/web/20220822030153/https://blog.coinbase.com/welcome-surojit-chatterjee-coinbases-chief-product-officer-c611d156610a?gi=bb73bb662666> (Coinbase notes in a blog post announcing his arrival that Surojit would “play a critical role in making the cryptoeconomy accessible to millions more people through Coinbase’s suite of products.”). This did not end well for many individuals who relied on the purported security of the Coinbase Wallet. Despite having a Twitter feed that announces to his followers the addition of many new products, and generally touts the Company, Chatterjee has dumped hundreds of thousands of shares on the public markets, while not purchasing a single share on the open market himself.

1108. In short, instead of investing in competent customer service, Coinbase executives touted their company’s commitment to security,⁴⁹ drew in customers to use their products through these empty promises, and then dumped their stock as the stock price climbed higher in the fall of 2021. As noted, the Wallet’s customers did not fare so well.

CLAIMS FOR RELIEF

COUNT 1

Violations of Section 1693g of the Electronic Funds Transfer Act and Section 1005.6(b) of Federal Regulation E With Respect to Unauthorized Transfers from Claimants’ Accounts (Against All Respondents)

1109. Claimants reallege and incorporate by reference the allegations in the preceding paragraphs as if fully alleged herein.

A. Legal Framework of the EFTA

1110. The EFTA and its corresponding regulations implemented by the Consumer Financial Protection Bureau (“CFPB”), 12 C.F.R. § 1005.1, *et seq.* were designed with the “primary objective” of “the provision of individual consumer rights.” 15 U.S.C. § 1693; 12 C.F.R. § 1005.1(b) (the “primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers and remittance transfers.”). The primary purpose of the EFTA and Federal Regulation E is the protection of individual consumers engaging in electronic fund transfers and remittance transfers.

1111. Relevant definitions:

a. A “financial institution” means “a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services”;

b. The term “account” means “a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes.”

⁴⁹ See, e.g., <https://blog.coinbase.com/how-coinbase-responds-to-industry-wide-crypto-security-threats-ad2c8a5da1f5>; <https://www.youtube.com/watch?v=G5B9Bwc5q5s>

- c. The term “consumer” means a “natural person”;
- d. The term “Access device” means a “card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers.”
- e. An access device becomes an “accepted access device” when the consumer: i) Requests and receives, or signs, or uses (or authorizes another to use) the access device to transfer money between accounts or to obtain money, property, or services; (ii) Requests validation of an access device issued on an unsolicited basis; or (iii) Receives an access device in renewal of, or in substitution for, an accepted access device from either the financial institution that initially issued the device or a successor.
- f. The term “electronic fund transfer” means any “transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account”;
- g. The term “Unauthorized electronic fund transfer” means an “electronic fund transfer from a consumer’s account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit.” The term does not include, as relevant here, “a person who was furnished the access device to the consumer’s account by the consumer.”

B. Factual Allegations

1112. Coinbase is a “financial institution” as defined by the EFTA and Federal Regulation E because it is a company that directly or indirectly holds accounts belonging to consumers, including Claimants’ accounts, and because Coinbase issues an access device and agrees with a consumer to provide electronic fund transfer services. 15 U.S.C. § 1693a(9); 12 C.F.R. § 1005.2(i).

1113. Claimants are “consumers” as defined by the EFTA and Federal Regulation E because they are natural persons. 15 U.S.C. § 1693(a)(6); 12 C.F.R. § 1005.2(j).

1114. Claimants’ Coinbase Wallet accounts are “accounts” as defined by the EFTA and Federal Regulation E because they are consumer asset accounts held directly or indirectly by Coinbase and established primarily for personal, family, or household purposes. 15 U.S.C. § 1693a(2); 12 C.F.R.

§ 1005.2(b)(1). Claimants' accounts were used for such personal purposes – *i.e.*, intended to earn income from appreciating assets – and not for business purposes. Further, in the Terms and Conditions attached as Exhibit 1, Coinbase refers to the Wallets as an “Account” and requires customers to notify Coinbase as to “any unauthorized use of [their] Account.” Coinbase also reserved the right, in its Terms and Conditions, to “suspend or terminate” the Accounts, thereby confirming that the Accounts are held and controlled by Coinbase.

1115. The Coinbase Wallet is an “access device” as defined by Federal Regulation E because it is used by consumers to initiate electronic fund transfers to or from a consumer account. The Wallet holds a private key that allows consumers to initiate electronic fund transfers.

1116. The electronic funds that were transferred from the Claimants' Coinbase Wallets are “unauthorized electronic fund transfers” because they were initiated by a person other than the owner of the Coinbase Wallet by fraud and without consent, and without actual authority to initiate such transfer, from which Claimants received no benefit. The primary purpose of the electronic transfers were for the scammers to steal the Claimants' crypto-assets and not for investment in a liquidity pool. Further, as directly applicable here, an “unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery.” *See* 12 CFR 1005.2 Comment 2(m). That is what happened here.

1117. Pursuant to the EFTA, the liability of a consumer, such as Claimants, for unauthorized electronic funds transfers is limited to the *lesser* of \$50.00, or the amount of money or value of property or services obtained in such unauthorized electronic fund transfer prior to the time that the financial institution is notified of, or otherwise becomes aware of, circumstances which lead to the reasonable belief that an unauthorized electronic fund transfer involving the consumer's account has or may be effected.

1118. Pursuant to Federal Regulation E, a consumer's liability for an unauthorized electronic fund transfer or series of related unauthorized transfers if timely notice is given shall not exceed the lesser of \$50 or the amount of unauthorized transfers that occurred before notice to the financial institution. If timely notice is not given then the consumer's liability shall not exceed the lesser of \$500 or the sum of \$50 or the amount of unauthorized transfers that occur within the two business

days, whichever is less; and the amount of unauthorized transfers that occur after the close of two business days and before notice to the institution, provided the institution establishes that these transfers would not have occurred had the consumer notified the institution within that two-day period.

1119. As alleged above, Coinbase received notice from Claimants that there were unauthorized electronic transfers from Claimants' Coinbase Wallet accounts. Section 1693g(a)(2) of the EFTA provides that: Notice under this paragraph is sufficient when such steps have been taken as may be reasonably required in the ordinary course of business to provide the financial institution with the pertinent information, whether or not any particular officer, employee, or agent of the financial institution does in fact receive such information. Similarly, Section 1005.6(b)(5) provides that: Notice to a financial institution is given when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information.

1120. After receiving notice from Claimants of the unauthorized electronic transfers, Coinbase failed to refund Claimants Coinbase Wallets for the unauthorized transfers as required by the EFTA and Federal Regulation E.

1121. In addition, Coinbase failed to timely investigate the unauthorized electronic transfers from Claimants' accounts as required by 15 U.S. Code § 1693f(a)(3) and 15 U.S. Code § 1693f(d) by failing to conduct a reasonable review of its own records. See 12 C.F.R. § 205.11(c)(4); see also Supp. I to § 205 at 11(c) 4–5. Indeed, an adequate investigation would have easily led Coinbase to the conclusion that fraud had occurred given that Claimants did not authorize the transfers at issue, that there were security flaws with the Coinbase Wallet, and that these fraudulent transfers had been widely reported as a common issue to Coinbase.

1122. Instead, Coinbase denied liability for the unauthorized electronic transfers by responding to Claimants' complaints with auto-generated form messages, for example:

“According to our records, the funds you asked about were successfully sent out of your Coinbase Wallet. If you did not authorize this, then it means that your Coinbase Wallet has been compromised. We could not provide any information as to why your Coinbase Wallet was compromised since Coinbase Wallet is user-controlled and non-custodial product. Only

our users have full control of their wallets and solely responsible for taking care of their wallets' security.”

1123. Coinbase's limitation of liability provision in its Terms of Service is inapplicable because pursuant to § 1693l of the EFTA: “No writing or other agreement between a consumer and any other person may contain any provision which constitutes a waiver of any right conferred or cause of action created by this subchapter.”

1124. Based on the foregoing, and pursuant to the EFTA and Federal Regulation E, Coinbase is required to refund Claimants for all of their losses due to unauthorized electronic transfers from their Coinbase Wallet, including interest thereon, an additional amount not less than \$100, and the costs of the action, together with reasonable attorneys' fees.

1125. In the alternative, if Coinbase is not deemed to either directly or indirectly hold the Claimants' accounts, Coinbase is still, pursuant to 12 C.F.R. § 1005.14, liable for the unauthorized electronic transfers because they provided the electronic fund transfer service to Claimants from other financial institutions without an agreement with the account-holding institution.

COUNT II

Violations of Section 1693c of the Electronic Funds Transfer Act and Section 1005.6 of Federal Regulation E With Respect to Failure to Make Required Disclosures (Against All Respondents)

1126. Claimants incorporate the allegations above.

1127. Pursuant to § 1693c of the EFTA, Coinbase is required to disclose, amongst others, at the time the consumer contracts for an electronic fund transfer service: (i) the consumer's liability for unauthorized electronic fund transfers; (ii) the telephone number and address of the person or office to be notified in the event the consumer believes that an unauthorized electronic fund transfer has been or may be effected; (iii) a summary, in a form prescribed by regulations of the Bureau, of the error resolution provisions of section 1693f and the consumer's rights thereunder; and (iv) under what circumstances the financial institution will in the ordinary course of business disclose information concerning the consumer's account to third persons.

1128. Similarly, pursuant to § 1005.7 of Federal Regulation E, Coinbase is required to disclose, among others: (i) a summary of the consumer's liability for unauthorized electronic fund transfers; (ii) the telephone number and address of the person or office to be notified when the consumer believes that an unauthorized electronic fund transfer has been or may be made; and (iii) notice of the error resolution provision.

1129. Coinbase failed to make the proper disclosures as required by the EFTA and Federal Regulation E.

1130. Coinbase's Terms of Service and Privacy Policy did not disclose the consumer's liability for unauthorized electronic fund transfers as required by the EFTA and Federal Regulation E. Instead, Coinbase included a limitation of liability provision, as detailed *supra* ¶127, which discharged any liability from it under any circumstances for damages arising out of or in any way related to software, products, services, and/or information offered or provided by third parties and accessed through the app, site or services.

1131. Coinbase did not include a telephone number and address for the person or office Claimants should notify if they believed an unauthorized electronic fund transfer occurred as required by the EFTA and Regulation E. Instead, Claimants were put in an endless loop of automated responses through email when they used the support@coinbase.com email address to notify Coinbase of the unauthorized electronic transfer.

1132. Coinbase failed to disclose the error resolution provision, as detailed *infra* ¶¶1135-1144, as required by the EFTA and Federal Regulation E.

1133. Coinbase failed to disclose that it would share Claimants' private key with third parties to establish the fraudulent smart contracts.

1134. Based on the foregoing, and pursuant to the EFTA and Federal Regulation E, Coinbase is required to refund Claimants for their losses due to the unauthorized electronic transfers from their

Coinbase Wallet, including interest thereon, an additional amount not less than \$100, and the costs of the action, together with reasonable attorney's fees.

COUNT III
**Violations of Section 1693f of the Electronic Funds Transfer Act and Section 1005.11 of
Federal Regulation E With Respect to Procedures for Resolving Errors
(Against All Respondents)**

1135. The procedures for resolving errors of Federal Regulation E and the EFTA provides, in relevant part, that if a financial institution receives notice of an error within sixty days after having sent the periodic statement or transmitted to a consumer documentation of an electronic funds transfer, receives oral or written notice in which the consumer (i) enables the institution to identify the consumer's name and account number; (ii) indicates why the consumer believes an error exists; and (iii) includes to the extent possible the type, date, and amount of the error, the financial institution must promptly investigate the alleged error, determine whether an error has occurred, and report or mail the results of such investigation and determination to the consumer within ten business days.⁵⁰ 15 U.S.C. § 1693f(a)(3); 12 C.F.R. § 1005.11(b)(1).

1136. If the financial institution determines that an error did occur, it has the option to either (1) timely correct the error, including the crediting of interest where applicable; or (2) timely provisionally recredit the consumer's account for the amount alleged to be in error pending the conclusion of the institution's investigation of the error within ten business days of being notified of the error. 15 U.S.C. § 1693(f)(c); *see also* 12 C.F.R. § 1005.11.

1137. In no circumstance can an investigation be concluded more than forty-five days after receipt of the notice of error, and during the pendency of the investigation, the consumer must be allowed full use of funds provisionally recredited. *Id.*

⁵⁰ The definition of "error" includes an unauthorized electronic fund transfer to or from the consumer's account. 12 C.F.R. § 1005.11(a)(1)(i).

1138. Since Coinbase failed to disclose the error resolution procedures, Claimants, pursuant to 15 U.S.C. § 1693g and/or 12 C.F.R. § 1005.6, are not liable for any amount of the unauthorized transfers.

1139. Moreover, Coinbase failed to timely investigate the unauthorized transfers from Claimants' accounts as required by 15 U.S.C. § 1693f(a)(3) and 15 U.S.C. § 1693d by failing to conduct a timely and reasonable review of its own records. Indeed, an adequate investigation would have easily revealed that Claimants were the victims of a widespread liquidity mining pool scam. In fact, in the rare cases that Coinbase did conduct an investigation, they arrived at the conclusion that "[a]fter an extensive review of the transaction details, your Wallet's history, and the addresses associated with it, the unauthorized activity you reported appears to have resulted from a signed transaction dated Oct-10-2021 that approved a malicious third-party transfer funds from your wallet."

1140. Instead, Coinbase sought to avoid liability by claiming that only Claimants had full control/access to their wallet, so Coinbase could not provide any further details about how Claimants' wallets were compromised nor assist with helping to recover the funds.

1141. However, if Coinbase actually conducted a reasonable investigation, it would have concluded that Claimants did not authorize the transfers at issue, the fraudulent transfers were made to accounts other than those Claimants used to fund their Coinbase Wallet accounts, and that these fraudulent transfers had been widely reported as common problems on the Coinbase platform.

1142. Indeed, for example, this is what Coinbase's untimely investigation revealed in the case of Claimant David Evdokimow. In the case of Evdokimow, Coinbase failed to timely correct the "error" in Claimant's account by timely crediting or provisionally recrediting his account after it had been breached and drained of funds. This failure, separately, results in any outstanding damages owed to Claimants pursuant to 15 U.S.C. § 1693m(a).

1143. Since Coinbase failed to provisionally recredit Claimants' account within the ten-day period, and did not make a good faith investigation of the unauthorized transfer, pursuant to §

1693f(e)(1), Claimants are entitled to treble damages. Moreover, pursuant to 1693f(e)(2), Claimants are entitled to treble damages because Coinbase knowingly and willfully concluded that Claimants' accounts were not in error when no other reasonable conclusion could have been drawn from the evidence available to Coinbase at the time it should have been investigating Claimants' claims.

1144. Accordingly, Claimants are entitled to actual damages, treble damages, attorneys' fees, and costs for Coinbase's violation of the error procedures pursuant to the EFTA and Federal Regulation E.

COUNT IV
Negligence
(Against All Respondents)

1145. Claimants reallege and incorporate by reference the allegations in the preceding paragraphs as if fully alleged herein.

1146. Coinbase owed duties to Claimants, including to exercise reasonable care in safeguarding Claimants' funds, through the use of reasonable and adequate security and fraud detection practices, procedures and technologies, and otherwise, and to take action to promptly inform Claimants of and otherwise address fraud once it had occurred.

1147. Coinbase knew or should have known of the likelihood of potential security breaches that resulted in Claimants' accounts being drained by unauthorized electronic fund transfers.

1148. As a company that advertises that consumers can "protect your digital assets with industry-leading security," Coinbase had a duty to develop, design, test, and warn their consumers when they were accessing fraudulent sites through the Coinbase Wallet browser, as well as to create and maintain procedures that would alert their consumers that there was a risk that scammers could drain their account before allowing their consumers to enter into the liquidity mining pool scam smart contracts. But Coinbase breached its duty by failing to create and enforce an adequate plan to prevent unauthorized transfers from Claimants' wallet. Coinbase also breached its duty by failing to provide customer service that recognized that funds were being lost due to the security breaches.

1149. Coinbase further breached its duties to Claimants by not providing warnings similar to other industry leaders in the non-custodial crypto wallet space, such as Metamask and Trust Wallet. Indeed, scammers induce victims to download the Coinbase Wallet app specifically because the Coinbase Wallet app fails to provide these warnings, unlike its competitors. Coinbase's failure to protect its customers' funds is an extreme departure from industry standard, which is why it is the preferred platform for scammers to use to induce victims to sign up for their fake liquidity mining pools.

1150. Coinbase also breached its duties by intentionally and/or negligently failing to provide an adequate and timely resolution to replenish Claimants' accounts and intentionally and/or negligently failing to respond in a timely fashion to the complaints of the Claimants.

1151. As a direct and proximate cause of Coinbase's acts and omissions, Claimants sustained damages as alleged herein. Claimants are entitled to damages, pre-judgement interest, attorneys' fees and costs pursuant to California Civil Code Section 1021.5, or as otherwise provided by statute or contract.

COUNT V
Gross Negligence
(Against All Respondents)

1152. Claimants reallege and incorporate by reference the allegations in the preceding paragraphs as if fully alleged herein.

1153. Coinbase owed duties to Claimants, including to exercise reasonable care in safeguarding Claimants' crypto, through the use of reasonable and adequate security and fraud detection practices, procedures and technologies, and otherwise, and to take action to promptly inform Claimants of and otherwise address fraud once it had occurred.

1154. As alleged, Coinbase's conduct constitutes a want of even scant care and an extreme departure from the ordinary standard of care. This grossly negligent conduct resulted in the theft of Claimants' funds from their Wallets. Specifically:

- a. To attract users, Coinbase advertised to customers its industry-leading security, and further advertised that its Wallet would protect consumers from crypto “scammers”;
- b. Coinbase customer service even told customers that the only way their funds could be compromised is their seed phrase was stolen. This lured customers into a false sense of security;
- c. Coinbase created a user interface in its Wallet that, unlike other wallets such as MetaMask, did not warn customers that malicious smart contracts had access to the funds in their Wallets;
- d. Scammers recognized this significant and serious security flaw, which is why scammers directed consumers to the Coinbase Wallet (as opposed to other non-custodial wallets);
- e. Once scammers began stealing customers’ funds through these liquidity pool scams, the victims, from at least October 2021, contacted Coinbase about the security flaw in the Wallet. Because Claimants and others repeatedly contacted Coinbase, Coinbase knew or should have known that there were security flaws in the Wallet that resulted in Claimants’ accounts being drained by unauthorized electronic fund transfers in the manner described herein.
- f. For months, Coinbase was repeatedly warned about the security flaws in its Wallet;
- g. Yet Coinbase employed customer service agents and “bots” that were inept and incapable of properly handling customer funds and accounts;
- h. Coinbase customer service largely ignored customers’ repeated warnings, and instead told customers (falsely) that their security seed phrases had been compromised;
- i. Coinbase customer service told victims that they would “flag” the scam dApps so that they would be blocked, but Coinbase did not do so, exposing many other people to the scams and likely resulting in the loss of significant funds;

- j. Even months after being told about the scams, Coinbase published videos regarding Wallet security that neglected to tell customers about the significant flaws in the Wallet or about the liquidity pool scams;
- k. Coinbase took no action to fix the flaws in the Wallet;
- l. Coinbase, for nearly six months, took no action to warn other customers about the security flaws in its Wallet;
- m. When Coinbase did eventually warn customers in March 2022 about the liquidity mining scams, Coinbase falsely told customers that Coinbase only recently learned of the scams and that the scams applied to all non-custodial wallets.
- n. Coinbase's gross negligence in creating the security flaws in the Wallet, responding to customer complaints and queries, and in covering up its negligence, collectively amounted to an extreme departure of care for a public company that touted the security features of its Wallet and actively told customers that it was working to keep out scammers.

1155. Coinbase was aware of the Wallet's security flaw by at least October 2021, but instead of warning its users about the flaw and the liquidity mining pool scam, Coinbase actively concealed the fact that scammers could withdraw all of a user's assets from their Wallet without having access to the User's 12-word recovery phrase. As a result of Coinbase's concealment of this glaring defect, additional users fell victim to this scam and lost their life savings.

1156. As a direct and proximate cause of Coinbase's acts and omissions, Claimants sustained damages as alleged herein. Claimants are entitled to damages, pre-judgment interest, attorney's fees and costs pursuant to California Civil Code Section 1021.5, or as otherwise provided by statute or contract.

COUNT VI
Breach of Contract
(Toshi Holdings Pte. Ltd.)

1157. Claimants reallege and incorporate by reference the allegations in the preceding paragraphs as if fully alleged herein.

1158. Claimants entered into a written agreement with Toshi Holdings, specifically the Coinbase Wallet Terms upon their registration for a Coinbase Wallet account. *See* Exhibit 1. Claimants were presented with this agreement on a take-it-or-leave it basis, or slightly modified versions thereof, when opening their Coinbase Wallet accounts.

1159. Claimants, as part of their agreement to open a Coinbase Wallet account, were responsible for the retention and security of their 12-word recovery phrase.

1160. As part of Coinbase Wallet’s Terms, Toshi Holdings guaranteed that its users’ “Recovery Phrase is the only way to access the cryptocurrency associated with your account.” (underline added). As detailed *supra* ¶164, Coinbase’s customer support agents informed users that “no third party or even Coinbase could have access to the funds in your wallet account” without the 12-word recovery phrase.

1161. Coinbase nevertheless breached the contractual guarantee provided to the Claimants by failing to provide proper security to Claimants’ Coinbase Wallet accounts and funds by allowing scammers to withdraw Claimants’ crypto from their Wallets without the scammers having access to Claimants’ 12-word Recovery Phrase. As detailed *supra* ¶966, Coinbase, while describing how the liquidity mining pool generally works, acknowledged that the liquidity mining pool scam does not need a user’s Recovery Phrase to drain the user’s Wallet: “[w]hile the user thinks that he/she approved a one-off transaction (the amount they wish to invest into the project) untrustworthy projects work with manipulated smart contracts, that grants them the permission to remove all your funds you’re [sic] your wallet, once you submitted a transaction to them. For this type of scam, the project does not need your seed-phrase.”

1162. As a result of Toshi Holding's breach of the Coinbase Wallet Terms, Claimants were harmed, including but not limited to the loss of the crypto that was stolen from their Wallets. Claimants are entitled to damages, pre-judgment interest, attorneys' fees and costs pursuant to California Civil Code section 1021.5, or as otherwise provided by statute or contract.

COUNT VII
Breach of Implied Covenant of Good Faith and Fair Dealing
(Against Toshi Holdings Pte. Ltd.)

1163. Claimants reallege and incorporate by reference the allegations in the preceding paragraphs as if fully alleged herein.

1164. Every contract, including the Coinbase Wallet Terms, contains an implied duty of good faith and fair dealing. Toshi Holdings entered into and is bound by the Coinbase Wallet Terms with Claimants, which are valid and enforceable contracts that contain an implied duty of good faith and fair dealing.

1165. Toshi Holdings breached the Coinbase Wallet Terms and the implied covenant of good faith and dealing by, among other things, failing to discharge their obligations and provide the services they promised in exchange for the transaction fees they charged Claimants for transactions in their Coinbase Wallet.

1166. Specifically, Toshi Holdings breached the Coinbase Wallet Terms and the implied covenant of good faith and fair dealing by choosing profits over providing sufficient security over Claimants' Coinbase Wallet accounts.

1167. Toshi Holdings breached the Coinbase Wallet Terms and the implied covenant of good faith and fair dealing by failing to timely notify Claimants of security threats, hacking, malicious smart contracts, and technological issues that allowed scammers to access Claimants' crypto assets without Claimants' 12-word recovery phrase.

1168. Toshi Holdings breached the Coinbase Wallet Terms and the implied covenant of good faith and fair dealing by failing to meet their obligation to timely and properly resolve Claimants' complaints about unauthorized transfers from their Coinbase Wallets.

1169. Toshi Holdings breached the Coinbase Wallet Terms and the implied covenant of good faith and fair dealing by failing to properly investigate Claimants' claims that their crypto assets were transferred out of their Wallets without their authorization.

1170. Toshi Holdings breached the Coinbase Wallet Terms and the implied covenant of good faith and fair dealing by failing to return Claimants' account funds and cryptocurrency assets.

1171. Toshi Holdings breached the Coinbase Wallet Terms and the implied covenant of good faith and fair dealing by failing to hire efficient customer service personnel and instead provided customer service that simply sent autogenerated replies when Claimants complained about losing life changing sums of money.

1172. As a result of Toshi Holdings's breach of their contractual duties, obligations and/or promises arising under the Terms of Service and the implied covenant of good faith and fair dealing, Claimants were damaged by, including but not limited to, the loss of their crypto assets, their payment of transaction fees, and the inability to access the funds and crypto assets in their account and the loss of value of those assets, all in an amount to be proven at trial.

1173. In addition to Claimants' actual contract damages, Claimants seek recovery of their attorneys' fees, costs to the extent provided by the Terms of Service and pre-judgement interest.

COUNT VIII
Unjust Enrichment
(Against All Respondents)

1174. Claimants reallege and incorporate by reference the allegations in the preceding paragraphs as if fully alleged herein, excluding Paragraphs 1158 through 1163.

1175. Claimants bring this claim in the alternative to their claim for breach of contract.

1176. As part of Coinbase's Coinbase Wallet Terms entered into by Coinbase and Claimants, Coinbase "may charge fees for some or part of the Services we make available to you. We reserve the right to change those fees at our discretion with notice. We will disclose the amount of fees we will charge you for the applicable Service at the time that you access the Service." Coinbase did charge such fees, and thereby received a money benefit from its relationship with Claimants.

1177. Coinbase was unjustly enriched, at the expense of Claimants, by collecting fees for the transfer of fiat currency into Tether through Coinbase.com, as well as from fees paid by Claimants through the use of the Wallet. As a result of Coinbase's acts and omissions as alleged herein, Coinbase has unjustly received and retained benefits at the expense of Claimants. Under principles of equity and good conscience, Coinbase should not be permitted to retain valuable funds belonging to Claimants and should disgorge the benefits and profits gained as a result of its acts and omissions.

1178. Claimants are entitled to restitution of, disgorgement of, and/or the imposition of a constructive trust upon all profits, benefits, and other compensation obtained by Coinbase, attorney's fees and costs pursuant to California Civil Code section 1021.5, or as otherwise provided by statute or contract and for such other relief that this Court deems just and proper.

COUNT IX
Violation of the California Unfair Competition Law
(Business and Professions Code Section 17200, *et seq.*)
(Against All Respondents)

1179. Claimants reallege and incorporate by reference the allegations in the preceding paragraphs as if fully alleged herein.

1180. Coinbase has engaged in unfair business acts and practices by inducing consumers to use its Wallet without warning them of the significant security risks inherent in doing so, and taking no action to mitigate those risks. As discussed above, Claimants have suffered substantial injury, which injury is not outweighed by any countervailing benefits to consumers or to competition. Nor was the injury reasonably avoidable by the consumer. To the contrary, Coinbase was in the best position to mitigate the risk of fraud because it was repeatedly warned, over a multi-month period, of the precise security risks that led to the Claimants' loss, but took no actions to mitigate this loss. To the contrary, Coinbase repeatedly assured its customers that the Wallet was the most secure non-custodial wallet in the market, even though scammers directed customers to the Coinbase Wallet *because of its terrible security.*

1181. Likewise, Coinbase’s acts and omissions as alleged herein serve as unlawful predicate acts and practices for purposes of Business and Professions Code sections 17200, *et seq.*, and are not outweighed by any countervailing benefits to consumers.

1182. Moreover, Coinbase’s business acts and practices are fraudulent because they are likely to deceive members of the public. Coinbase claims that a user’s recovery phrase is the only way to access the cryptocurrency associated with their account, however, scammers are able to drain user’s Wallet without the user’s 12-word recovery phrase being compromised. Coinbase offers its non-custodial wallet to consumers without any warning that it contains a glaring security flaw, which allows scammers to drain the Wallets.

1183. California Business and Professions Code section 17204 allows “any person who has suffered injury in fact and has lost money or property as a result of such unfair competition” to prosecute a civil action for violation of the UCL.

1184. As a result of these actions, including not refunding Claimants’ accounts after the unauthorized transfers, Coinbase is able to unfairly compete with other comparable companies in violation of Business and Professions Code sections 17000, *et seq.* and 17200, *et seq.* Due to these unlawful, unfair, and fraudulent business practices, Coinbase has gained a competitive advantage over other comparable companies—including over similar companies who have *better* security features.

1185. The victims of these unlawful, unfair, and fraudulent business practices include, but are not limited to, Claimants, competing cryptocurrency wallets providing similar services as Coinbase, and the general public. Upon information and belief, Coinbase performed the alleged acts with the intent of gaining an unfair competitive advantage and thereby injuring Claimants, other competitors, and the general public.

1186. Claimants’ success in this action will enforce important rights affecting the public interest and public policy. In this regard, Claimants sue on behalf of themselves and the public.

1187. Business and Professions Code Section 17203 provides that a court may make such orders or judgments as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition. Injunctive relief is necessary and appropriate to prevent Coinbase from repeating their unlawful, unfair, and fraudulent business acts and business practices alleged above.

1188. Business and Professions Code section 17203 provides that the Court may restore to any person in interest, any money or property that may have been acquired by means of such unfair competition. Claimants are entitled to restitution pursuant to Business and Professions Code section 17203 for the unauthorized transfers draining Claimants' accounts and/or funds, and the fair value of other losses alleged herein.

1189. Claimants request injunctive relief pursuant to Business and Professions Code section 17203 to enjoin Coinbase from continuing the unfair/unlawful business practices alleged herein.

1190. Claimants herein take upon enforcement of these laws and lawful claims. There is a financial burden involved in pursuing this action. The action is seeking to vindicate a public right, and it would be against the interests of justice to penalize Claimants by forcing Claimants to pay attorneys' fees from the recovery in this action. Attorneys' fees are appropriate pursuant to Code of Civil Procedure Section 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Claimants respectfully pray for relief as follows:

- a. A judgment for actual damages;
- b. A judgment for compensatory damages;
- c. A judgment for disgorgement of profits;
- d. A declaratory judgment that Coinbase violated the UCL;
- e. A judgment for injunctive relief enjoining Coinbase from engaging in future unlawful activities complained of herein, including violations of the UCL; ordering Coinbase to engage in a

corrective notice campaign, and requiring Coinbase to refund to Claimants and others similarly situated any funds lost;

f. An accounting of all amounts that Coinbase unjustly received, retained, and/or collected as a result of its unlawful acts and omissions;

g. A list of all victims of the liquidity pool scams as described above;

h. A judgment for exemplary and punitive damages for Coinbase's knowing, willful, and intentional conduct;

i. Treble damages pursuant to the EFTA, 15 U.S.C. § 1693(f);

j. Statutory damages pursuant to the EFTA, 15 U.S.C. § 1693(m);

k. Costs of litigation pursuant to EFTA, 15 U.S.C. § 1693(m);

l. Pre-judgment interest pursuant to federal law;

m. Post-judgment interest pursuant to 28 U.S.C. § 1961(a);

n. A judgment for reasonable attorney fees and costs of this suit, pursuant to contract, the EFTA, the UCL, California Civil Code Section 1021.5, and any other applicable statute; and

o. Any other relief that is proper.

Dated: October 14, 2022

Respectfully submitted,

/s/ Eric S. Rosen

Eric Rosen

Amos Friedland

Jordana Haviv

Constantine Economides

Kelvin Goode

Maya S. Jumper

ROCHE FREEDMAN LLP

99 Park Avenue, 1910

New York, NY 10016

Tel.: (646) 350-0527

erosen@rochefreedman.com

afriedland@rochefreedman.com

jhaviv@rochefreedman.com

ceconomides@rochefreedman.com

kgoode@rochefreedman.com

mjumper@rochefreedman.com

Counsel for Claimants

EXHIBIT 1

Coinbase Wallet Terms of Service

Last Updated: October 21, 2021

Toshi Holdings Pte. Ltd (“**Toshi Holdings**” or “**we**” or “**us**” or “**our**”) makes available to users certain software services accessible via a mobile device application, including the Toshi Wallet (commonly known as Coinbase Wallet) (the “**Wallet Application**” or “**App**”). Toshi Holdings is a wholly owned subsidiary of Coinbase Global, Inc. The Wallet Application enables users to (i) self custody digital assets; (ii) access a digital asset browser and link to decentralized applications and decentralized exchanges (“**Dapp(s)**”); (iii) view addresses and information that are part of digital asset networks and broadcast transactions; and (iv) additional functionality as Toshi Holdings may add to the App from time to time (collectively the “**Services**”). Toshi Holdings developed these Terms of Service (these “**Terms**”) to describe the terms that govern your use of all versions of the Wallet Application. These terms and additional information about the Wallet Application can be found on the Coinbase website located at <https://wallet.coinbase.com> (the “**Site**”).

Agreement to Terms

By clicking “I Agree” or by accessing the Wallet Application or using any or all of the Services, you agree to be bound by these Terms. If you don’t agree to be bound by these Terms, you may not access or use the Services.

Privacy Policy

Please refer to our [Coinbase Wallet’s Privacy Policy](#) for information on how we collect, use and disclose information from our users. You acknowledge and agree that your use of the Services is subject to, and that we can collect, use and/or disclose your information (including any personal data you provide to us) in accordance with, our Privacy Policy.

Changes to Terms or Services

We may modify the Terms at any time at our sole discretion. If we do so, we’ll let you know either by posting the modified Terms on the Site, by providing you a notice through the App, or through other methods of communication which we deem reasonable. The modified Terms will be effective at the time they are posted on the Site. It’s important that you review the Terms whenever we modify them because if you continue to use the Services after we have modified the Terms, you are agreeing to be bound by the modified Terms. If you don’t agree to be bound by the modified Terms, then you may not use the Services. Because our Services are evolving over time we may change or discontinue all or any part of the Services, at any time and without notice, at our sole discretion.

ARBITRATION NOTICE : THESE TERMS CONTAIN AN ARBITRATION CLAUSE FOR USERS IN CERTAIN JURISDICTIONS. IF YOU ARE A USER LOCATED IN THE UNITED STATES OR CANADA YOU AGREE THAT DISPUTES BETWEEN YOU AND TOSHI HOLDINGS WILL BE RESOLVED BY BINDING, INDIVIDUAL ARBITRATION IN THE UNITED STATES OR CANADA AS APPLICABLE, AND YOU ARE WAIVING YOUR RIGHT TO A TRIAL BY JURY OR TO PARTICIPATE AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS ACTION OR REPRESENTATIVE PROCEEDING.

Who May Use the Services

Eligibility

You may use the Services if you are 18 years or older and are not barred from using the Services under applicable law.

Registration and Your Information

If you want to use the Services you’ll have to create an account (“**Account**”) via the App. You agree that you won’t disclose your Account credentials to anyone and you’ll notify us immediately of any unauthorized use of your Account. You’re responsible for all activities that occur under your Account, or are otherwise referable to your Account credentials, whether or not you know about them. We reserve the right to suspend or terminate your Account if you provide inaccurate, untrue, or incomplete information, or if you fail to comply with the Account registration requirements or these terms.

You are solely responsible for the retention and security of your twelve word recovery phrase (“**Recovery Phrase**”). Your Recovery Phrase is the only way to access the cryptocurrency associated with your Account. Anyone that has access to your Recovery Phrase can access your cryptocurrency. If you lose your Recovery Phrase, you will not be able to access your cryptocurrency. You acknowledge that Toshi Holdings does not store and is not responsible in any way for the security of your Recovery Phrase and you agree to hold Toshi Holdings and/or Coinbase harmless and that Toshi Holdings and/or Coinbase shall not be liable in any way in the event you lose your Recovery Phrase and cannot access your cryptocurrency.

Feedback

We welcome feedback, comments, ideas, and suggestions for improvements to the Services (“**Feedback**”). You can submit Feedback by contacting us at <https://help.coinbase.com/en/more/coinbase-wallet>. You grant to us a non-exclusive, worldwide, perpetual, irrevocable, fully-paid, royalty-free, sublicensable and transferable license under any and all intellectual property rights that you own or control to use, copy, modify, create derivative works based upon and otherwise exploit the Feedback for any purpose. **If you lose your Recovery Phrase, you will not be able to access your cryptocurrency. You acknowledge that Toshi Holdings does not store and is not responsible in any way for the security of your Recovery Phrase and you agree to hold Toshi Holdings and/or Coinbase harmless and that Toshi Holdings and/or Coinbase shall not be liable in any way in the event you lose your Recovery Phrase and cannot access your cryptocurrency.**

Content Ownership, Responsibility and Removal

For purposes of these Terms: (i) “**Content**” means text, graphics, images, music, software, audio, video, works of authorship of any kind, and information or other materials that are posted, generated, provided or otherwise made available through the Services; and (ii) “**User Content**” means any Content that Account holders (including you) make available through the Services. Content includes without limitation User Content.

We do not claim any ownership rights in any User Content and nothing in these Terms will be deemed to restrict any rights that you may have to use and exploit your User Content.

Subject to the foregoing, Toshi Holdings and its licensors exclusively own all right, title and interest in and to the Services and Content, including all associated intellectual property rights. You acknowledge that the Services and Content are protected by copyright, trademark, and other laws of the United States and foreign countries. You agree not to remove, alter or obscure any copyright, trademark, service mark or other proprietary rights notices incorporated in or accompanying the Services or Content.

Rights in User Content Granted by You

In order to operate and provide our Services, you grant us a worldwide, non-exclusive, royalty-free, sublicensable, and transferable license to use, copy, distribute, create derivative works of, display, and perform the User Content that you upload, submit, store, send, or receive on the App or through our Services. The rights you grant in this license are for the limited purpose of operating and providing our Services. Additional information about your privacy and how we use User Content is available in the Privacy Policy.

You warrant and represent that you have the right and authority to submit your User Content and that the User Content or any part thereof does not infringe the intellectual property rights or any other rights of any third party.

You acknowledge that, in certain instances, where you have removed your User Content by specifically deleting it, some of your User Content (such as posts or comments you make) may not be completely removed and copies of your User Content may continue to exist on the Services. We are not responsible or liable for the removal or deletion of (or the failure to remove or delete) any of your User Content.

Rights in Content Granted by Toshi Holdings

Subject to your compliance with these Terms, we grant you a limited, non-exclusive, non-transferable, non-sublicensable license to download, view, copy, display and print the Content solely in connection with your permitted use of the Services.

Rights in App, Site and Services Granted by Toshi Holdings

The App, Site and Services are proprietary to Toshi Holdings and its licensors and must not be used other than strictly in accordance with these Terms. Toshi Holdings grants to you a limited, non-exclusive, non-transferable, non-sublicensable right to use the App and Site for the purposes of accessing and using the Services in accordance with these Terms.

Fees

We may charge fees for some or part of the Services we make available to you. We reserve the right to change those fees at our discretion with notice. We will disclose the amount of fees we will charge you for the applicable Service at the time that you access the Service.

You may incur charges from third parties for use of linked services. For example, you may be charged fees via the Dapps and/or DEXs that you may access via the App. You may also be charged fees by Coinbase, Inc. if you elect to link the Wallet App to your Coinbase account and transact in your Coinbase account. Third party fees are not charged by Toshi Holdings and are not paid to Toshi Holdings.

Acceptable Use and Coinbase Wallet Holding's Enforcement Rights

You agree not to use the Services in ways that:

- Violate, misappropriate, or infringe the rights of Toshi Holdings, our users, or others, including privacy, publicity, intellectual property, or other proprietary rights;
- Are illegal, defamatory, threatening, intimidating, or harassing;
- Involve impersonating someone;
- Breach any duty toward or rights of any person or entity, including rights of publicity, privacy, or trademark;
- Involve sending illegal or impermissible communications such as bulk messaging, auto-messaging, auto-dialing, and the like;
- Avoid, bypass, remove, deactivate, impair, descramble or otherwise circumvent any technological measure implemented by us or any of our service providers or any other third party (including another user) to protect the Services or Content;
- Disguise your location through IP proxying or other methods;
- Interfere with, or attempt to interfere with, the access of any user, host or network, including, without limitation, sending a virus, overloading, flooding, spamming, or mail-bombing the Services;
- Violate any applicable law or regulation; or
- Encourage or enable any other individual to do any of the foregoing.

Although we have no obligation to monitor any User Content, we have absolute discretion to remove User Content at any time and for any reason without notice. You understand that by using the Services, you may be exposed to User Content that is offensive, indecent, or objectionable. We take no responsibility and assume no liability for any User Content, including any loss or damage to any of your User Content.

You agree to comply with all applicable U.K. and non-U.K. export control and trade sanctions laws ("**Export Laws**"). Without limiting the foregoing, you may not download the App or use the Services if 1) you are in, under the control of, or a national or resident of Cuba, Iran, North Korea, Sudan, or Syria or any other country subject to United States embargo, UN Security Council Resolutions ("UNSCR"), HM Treasury's financial sanctions regime, or if you are on the U.S. Treasury Department's Specially Designated Nationals List or the U.S. Commerce Department's Denied Persons List, Unverified List, Entity List HM Treasury's financial sanctions regime; or (2) you intend to supply any Services to Cuba, Iran, North Korea, Sudan or Syria or any other country subject to United States embargo or HM Treasury's financial sanctions regime (or a national or resident of one of these countries), or to a person on the Specially Designated Nationals List, Denied Persons List, Unverified List, Entity List, or HM Treasury's financial sanctions regime.

Third Party Materials

The Services and App may contain links to third-party services and/or Dapps ("**Third Party Materials**"). The Services enable you to access Dapps via a Dapp browser and WalletLink by navigating away from the App to the Dapp or by enabling a native frontend software link within the App. When using a Dapp or other Third Party Materials, you understand that you are at no time transferring your assets to us. We provide access to Third Party Materials only as a convenience, do not have control over their content, do not warrant or endorse, and are not responsible for the availability or legitimacy of, the content, products or services on or accessible from those Third Party Materials (including any related websites, resources or links displayed therein). We make no warranties or representations, express or implied, about such linked Third Party Materials, the third parties they are owned and operated by, the information contained on them or the suitability of their products or services. You acknowledge sole responsibility for and assume all risk arising from your use of any third-party websites, applications, or resources.

You may be able to link Wallet to your Coinbase account to enable access to your Coinbase account from Wallet. IN doing so, you understand and agree that all transactions made when accessing your Coinbase account from Wallet is subject to the terms of use for the Coinbase account and the Coinbase privacy policy.

Termination

We may terminate your access to and use of the Services, at our sole discretion, at any time and without notice to you. You may cancel your Account at any time by following the account closure instructions in the App. Upon any termination, discontinuation or cancellation of Services or your Account, (i) all rights and/or licences granted to you under these Terms shall immediately cease and terminate and you shall forthwith cease the use and/or access of the App, Site, Services and Content in any way whatsoever; and (ii) notwithstanding the foregoing, the following provisions will survive: Feedback, Content and Content Rights, Content Ownership, Responsibility and Removal (save for the subsection "Rights in Content Granted by Toshi Holdings"), Termination, Warranty Disclaimers, Indemnity, Limitation of Liability, Dispute Resolution, and General Terms.

Warranty Disclaimers

YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE SERVICES (INCLUDING ANY PRIVATE KEY STORAGE SERVICE OFFERED AS PART OF THE SERVICES, WHETHER CLOUD OR HARDWARE-BASED) AND CONTENT IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. THE APP, SITE AND SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT ANY REPRESENTATION OR WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TOSHI HOLDINGS SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND/OR NON-INFRINGEMENT. TOSHI HOLDINGS DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES THAT ACCESS TO THE SERVICES OR ANY OF THE MATERIALS CONTAINED THEREIN WILL BE CONTINUOUS, UNINTERRUPTED, TIMELY, OR ERROR-FREE.

USE OF ANY PRIVATE KEY STORAGE SERVICE INCLUDED AS PART OF THE SERVICES IS OFFERED TO YOU AS A CONVENIENCE, SUBJECT TO THE LIMITATIONS ABOVE. TO BE SAFE, YOU SHOULD ALWAYS BACKUP YOUR PRIVATE ACCESS KEY VIA SECONDARY MEANS.

Indemnity

You will indemnify and hold harmless Toshi Holdings and its officers, directors, employees and agents, from and against any claims, disputes, demands, liabilities, damages, losses, and costs and expenses, including, without limitation, reasonable legal and accounting fees arising out of or in any way connected with (i) your access to or use of the Services or Content, (ii) your User Content, (iii) Third Party Materials, or (iv) your violation of these Terms.

Limitation of Liability

TO THE MAXIMUM EXTENT NOT PROHIBITED BY LAW, TOSHI HOLDINGS SHALL NOT BE LIABLE FOR DAMAGES OF ANY TYPE, WHETHER DIRECT OR INDIRECT, ARISING OUT OF OR IN ANY WAY RELATED TO YOUR USE OR INABILITY TO USE THE SERVICES, INCLUDING BUT NOT LIMITED TO DAMAGES ALLEGEDLY ARISING FROM THE COMPROMISE OR LOSS OF YOUR LOGIN CREDENTIALS OR FUNDS, OR LOSS OF OR INABILITY TO RESTORE ACCESS FROM YOUR BACKUP PHRASE, OR FOR MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, DEFECTS AND/OR ERRORS IN THE TRANSMISSION OF TRANSACTIONS OR MESSAGES TO THE ETHEREUM NETWORK, OR THE FAILURE OF ANY MESSAGE TO SEND OR BE RECEIVED BY THE INTENDED RECIPIENT IN THE INTENDED FORM, OR FOR DIMINUTION OF VALUE OF ETHER OR ANY OTHER DIGITAL TOKEN OR DIGITAL ASSET ON THE ETHEREUM NETWORK. TOSHI HOLDINGS SHALL NOT BE LIABLE UNDER ANY CIRCUMSTANCES FOR ANY LOST PROFITS OR ANY SPECIAL, INCIDENTAL, INDIRECT, INTANGIBLE, OR CONSEQUENTIAL DAMAGES, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH AUTHORIZED OR UNAUTHORIZED USE OF THE SERVICES, EVEN IF AN AUTHORIZED REPRESENTATIVE OF TOSHI HOLDINGS HAS BEEN ADVISED OF OR KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES. TOSHI HOLDINGS SHALL NOT BE LIABLE UNDER ANY CIRCUMSTANCES FOR DAMAGES ARISING OUT OF OR IN ANY WAY RELATED TO SOFTWARE, PRODUCTS, SERVICES, AND/OR INFORMATION OFFERED OR PROVIDED BY THIRD-PARTIES AND ACCESSED THROUGH THE APP, SITE OR SERVICES.

SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. IN NO EVENT SHALL TOSHI HOLDINGS' TOTAL LIABILITY TO YOU FOR ALL DAMAGES (OTHER THAN AS MAY BE REQUIRED BY APPLICABLE LAW IN CASES INVOLVING PERSONAL INJURY) EXCEED THE AMOUNT OF ONE HUNDRED U.S. DOLLARS (\$USD100.00) OR ITS EQUIVALENT IN THE LOCAL CURRENCY OF THE APPLICABLE JURISDICTION.

Dispute Resolution

Governing Law, Forum and Venue

These Terms and any action related thereto will be governed by the laws of the state of California in the United States, without regard to its conflict of laws provisions, If you are a user located in the United States or Canada, the terms in the "Special Arbitration Provision for United States or Canada Users" section below apply to you.

If you are not located in the United States or Canada, you agree that you will resolve any claim you have with us relating to, arising out of, or in any way in connection with our Terms, us, or our Services (each, a "Dispute," and together, "Disputes") exclusively in the state courts located in the City and County of San Francisco, California, or federal court for the Northern District of California and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such Disputes.

Special Arbitration Provision for United States or Canada Users

If you are a user located in the United States or Canada, you and Toshi Holdings agree that any Dispute **shall be finally settled in binding arbitration, on an individual basis, in accordance with the American Arbitration Association's rules for arbitration of consumer-related disputes (accessible at <https://www.adr.org/Rules>) and you and Toshi Holdings hereby expressly waive trial by jury and right to participate in a class action lawsuit, private attorney general actions, or class-wide arbitration**, except that each party retains the right: (i) to bring an individual action in small claims court and (ii) to seek injunctive or other equitable relief in a court of competent jurisdiction to prevent the actual or threatened infringement, misappropriation or violation of a party's copyrights, trademarks, trade secrets, patents or other intellectual property rights (the action described in the foregoing clause (ii), an "IP Protection Action"). The exclusive jurisdiction of an IP Protection Action shall be the courts of San Francisco, California and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating IP Protection Actions.

The Federal Arbitration Act, 9 U.S.C. §§ 1-16, fully applies to the arbitration. The arbitration will be conducted by a single, neutral arbitrator and shall take place in the county or parish in which you reside, or another mutually agreeable location, in the English language. The arbitrator may award any relief that a court of competent jurisdiction could award, including attorneys' fees when authorized by law, and the arbitral decision may be entered as a judgement and enforced in any court of law. At your request, hearings may be conducted in person or by telephone and the arbitrator may provide for submitting and determining motions on briefs, without oral hearings. The prevailing party in any action or proceeding to enforce this agreement shall be entitled to costs and attorneys' fees.

If the arbitrator(s) or arbitration administrator would impose filing fees or other administrative costs on you, we will reimburse you, upon request, to the extent such fees or costs would exceed those that you would otherwise have to pay if you were proceeding instead in a court. We will also pay additional fees or costs if required to do so by the arbitration administrator's rules or applicable law. Apart from the foregoing, each Party will be responsible for any other fees or costs, such as attorney fees that the Party may incur. If a court decides that any provision of this Special Arbitration Provision is invalid or unenforceable, that provision shall be severed and the other parts of this Special Arbitration Provision shall still apply. In any case, the remainder of this User Agreement, will continue to apply.

General Terms

These Terms constitute the entire and exclusive understanding and agreement between Toshi Holdings and you regarding the Services and Content, and these Terms supersede and replace any and all prior oral or written understandings or agreements between Toshi Holdings and you regarding the Services and Content. If any provision of these Terms is held invalid or unenforceable (either by an arbitrator appointed pursuant to the terms of the "Special Arbitration Provision" section above or by a court of competent jurisdiction, that provision will be enforced to the maximum extent permissible and the other provisions of these Terms will remain in full force and effect. You may not assign or transfer these Terms, by operation of law or otherwise, without our prior written consent. Any attempt by you to assign or transfer these Terms, without such consent, will be null. We may freely assign or transfer these Terms without restriction. Subject to the foregoing, these Terms will bind and inure to the benefit of the parties, their successors and permitted assigns.

Any notices or other communications provided by us under these Terms, including those regarding modifications to these Terms, will be given by posting to the Services and/or through other electronic communication. You agree and consent to receive electronically all communications, agreements, documents, notices and disclosures (collectively, "Communications") that we provide in connection with your Account and your use of the Services.

Our failure to enforce any right or provision of these Terms will not be considered a waiver of such right or provision. The waiver of any such right or provision will be effective only if in writing and signed by a duly authorized representative of Toshi Holdings. Except as expressly set forth in these Terms, the exercise by either party of any of its remedies under these Terms will be without prejudice to its other remedies under these Terms or otherwise.

These Terms are written in English (U.S.). Any translated version is provided solely for your convenience. To the extent any translated version of our Terms conflicts with the English version, the English version controls.

Contact Information

If you have any questions about these Terms or the Services, please contact us at wallet.support@coinbase.com.