SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

ANDREW CHAIT, on behalf of himself and all others similarly situated, Plaintiff, -against- WENDY LEE, EILEEN BURBRIDGE, MARY SCOTT, VERNA, ETTIE LEE, KEIKO FUJIWARA and JOHN DOE NOS. 1-25, Defendants.	Index No. _____ **AFFIRMATION OF CHARLES ZACH**

I, Charles Zach, affirm under penalty of perjury as follows:

Introduction

1. I am employed as a Lead Illicit Finance Investigator by Inca Digital, a company that specializes in investigating cryptocurrency schemes, including "pig butchering." As part of my employment at Inca Digital, I have investigated matters related to Andrew Chait's ("Plaintiff") above-captioned action against Defendants Wendy Lee, Eileen Burbridge, Mary Scott, Verna, Ettie Lee, Keiko Fujiwara, and John Doe Nos. 1-25 (collectively "Defendants"). I am over 18 years of age, of sound mind, and am competent to make this Affirmation. The evidence set forth in this Affirmation is based on my personal knowledge unless expressly stated otherwise.

2. Inca Digital is a leading digital asset intelligence firm providing data, analytics, and expertise to cryptocurrency exchanges, financial institutions, regulators, and government agencies. Inca Digital's services are used to trace illicit financial activity and combat fraud, particularly in cases involving complex cryptocurrency schemes.

3. I hold a Master of Arts in Global Risk from Johns Hopkins University, School of Advanced International Studies (SAIS), where I specialized in Strategic Foresight for Political

Risk Analysis, Risk in International Politics and Economics, and Conflict and Risk in Cyberspace. I also earned a Bachelor of Arts in International Relations with a concentration in European Studies from the University of Arkansas. I am a Certified Cryptocurrency Tracing Examiner (CTCE) and hold certifications in Anti-Money Laundering and Transaction Monitoring. I am a member of the Association of Certified Anti-Money Laundering Specialists (ACAMS). Prior to my work at Inca Digital, I served as a Cleared American Guard with the United States Department of State and as a Marine Embassy Security Guard with the United States Marine Corps.

4. Inca Digital has been investigating "pig butchering" cases for over two years. "Pig butchering" is a fraudulent scheme in which victims are manipulated into investing in fake cryptocurrency platforms, often through social media or messaging applications. These scams have resulted in billions of dollars in losses and are under investigation by both state and federal authorities.[1] Based on my extensive experience in investigating such schemes, this case clearly involves a coordinated and large-scale "pig butchering" operation.

5. In this case, the fraudulent scheme revolves around several fake cryptocurrency trading and investment platforms. Defendants used these platforms to lure Plaintiff and other Class Members into transferring cryptocurrency to wallets they controlled. The goal of this class action is to freeze the wallets holding the converted funds and facilitate the return of these stolen assets to the defrauded Class Members.

[1] See FinCEN Alert of Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering," U.S. Treasury Financial Crimes Enforcement Network Sep. 8, 2023, https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf

6. Based on Inca's investigation to date, the Defendants' conversion scheme involved fraudulent transactions from January 2023 through at least July 2024. The scheme affected approximately 2,000 Class Members.

7. As detailed in Appendix A, Inca identified the specific cryptocurrency wallets in which the ill-gotten gains of Defendants' scheme are presently held. These wallets are linked to the common "pig butchering" scheme that centers around the fraudulent platforms mentioned above.

Summary of Inca's Investigation

8. Inca's investigation was based upon the review of communications between Plaintiff and Defendants, notes of interviews with Plaintiff, records from Plaintiff's financial institutions, analysis of transactions publicly available on various cryptocurrency blockchains, as well as the use of proprietary software tools and data, including Chainalysis, a tool commonly used by law enforcement to trace stolen crypto assets.

9. Inca's investigation confirmed that Defendants directed Plaintiff to transfer funds to fake versions of real platforms or wallets: CoinJar and SafePal—or to platforms that were completely fictitious: CoinExchange, Vbitex, and ICMarket—that were fraudulent and designed to deceive Class Members into believing their funds were being invested in legitimate cryptocurrency ventures. The purported profits and returns displayed to the victims were falsified to create the illusion of growing investments, while the Defendants had already misappropriated their cryptocurrency.

10. Inca's investigation further revealed that Defendants utilized these fake platforms to move and convert Class Members' assets, transferring the funds through a series of transactions designed to obscure their origins. Inca's tracing analysis followed these transactions, which led to

cryptocurrency wallets held on the exchanges Binance, OKX, and KuCoin. These wallets are listed in Appendix A.

11. Inca's investigation was conducted in two phases, both employing rigorous blockchain forensic techniques. In phase one, Inca performed a "forward trace," tracking the flow of Plaintiff's funds from their initial transfer to intermediary wallets and eventually to wallets hosted on exchanges and third-party platforms. This tracing uncovered the movement of Plaintiff's assets through multiple wallets, which culminated in deposits into the cryptocurrency wallets listed in Appendix A.

12. In phase two, Inca conducted a "reverse trace," which involved tracing funds flowing into the wallets identified during phase one. Through this analysis, Inca uncovered further wallet addresses involved in the same transaction patterns as Plaintiff's funds, thus revealing a broader network of wallets involved in the scam. This tracing methodology confirmed the involvement of exchange-controlled and privately held wallets in the misappropriation of Class Members' funds.

13. Through its forward tracing and reverse tracing analysis, Inca's investigation uncovered a network of cryptocurrency wallets through which Class Member funds were funneled. At least 82 of these wallets were previously associated with suspicious activity, including known scams, darknet-related activity, or are listed by the U.S. Office of Foreign Assets Control. The number of these wallets present in the network is highly indicative that the whole network is controlled by the perpetrators of a fraudulent crypto scheme.

14. Further, the interactions between the wallets in the network is highly indicative of fraudulent activity. Specifically, the network contains wallets engaging in behavior that is associated with cryptocurrency fraud schemes and is rarely if ever associated with legitimate

cryptocurrency transactions. Two types of wallets are present in scam networks: “Transport Addresses” and “Pivot Addresses.” “Transport Addresses” are designed to simply forward everything they receive, moving funds as far and as quickly as possible from the victim to frustrate tracing. Transport Addresses typically deal with a limited set of assets: USDC, USDT, DAI, and ETH, as these types of crypto are the easiest to move and convert from one type to another. Further, the wallets in this network mainly transact using stablecoins, which is typical of crypto scams like pig butchering because scammers are not interested in investing, staking, or farming--types of behavior associated with crypto that are not stablecoins. Funds are rarely held in these wallets for more than a few days, with the sum of inputs equaling the sum of outputs. Additionally, the number of nodes these addresses receive funds from will generally equal the number of nodes they send funds to.

15. The network also contains “Pivot Addresses,” which are known for mixing funds and serve as hubs for numerous transport channels. They accumulate funds from a large number of transport nodes and forward larger amounts to 3-4 other transport nodes. Typically, each scheme has only one Pivot Address, and the funds this address receives eventually end up on exchange wallets after passing through a few additional wallets in the network. This category of addresses actively uses decentralized exchanges to swap funds between USDT, USDC, and DAI, and frequently uses bridges and mixers to obscure funds in other networks. Additionally, sources of funds for these addresses often include wallets already flagged for scam activity, gambling, darknet involvement, or inclusion in sanction lists. Overall, these interactions between the different wallets in the network gives me a high degree of confidence that the entire network exists as part of the scam and is controlled by Defendants.

16. Inca uses a common tool called Etherscan to track transactions on the Ethereum blockchain. This tool shows all transactions at UTC+0 (Greenwich Mean Time). There are therefore often small discrepancies in date/time between the data that shows up in Inca's analysis based on the Etherscan tool and a cryptocurrency fraud victim's records of transactions, which normally are recorded in the time zone that the victim is in. In this case, Plaintiff's records generally record transactions in Eastern Time. Further, it takes time, sometimes up to several days, between the time a crypto transaction is initiated and the time a transaction is recorded on the blockchain.

17. When tracing cryptocurrency transactions, it is common for there to be slight discrepancies between the amount of funds the initiator of the transaction sends and the amount of funds received by the recipient. This is because most cryptocurrency transactions on the Ethereum blockchain require "gas," which is essentially a fee for engaging in the transaction, which is deducted from the amount that is received by the recipient. Further, some cryptocurrency, like the commonly traded cryptocurrency Ethereum, are highly volatile, so even a small delay between the transaction being initiated by the sender and the cryptocurrency being received by the recipient can lead to a difference in the dollar value of that cryptocurrency between when it is sent by the sender and when it is received by the recipient.

Inca's Tracing Analysis

Wendy Lee & Eileen Burbridge

Pivot Address 1: 0x63390bF7BD8c81809D69963D9d4b1E5F22844909; and

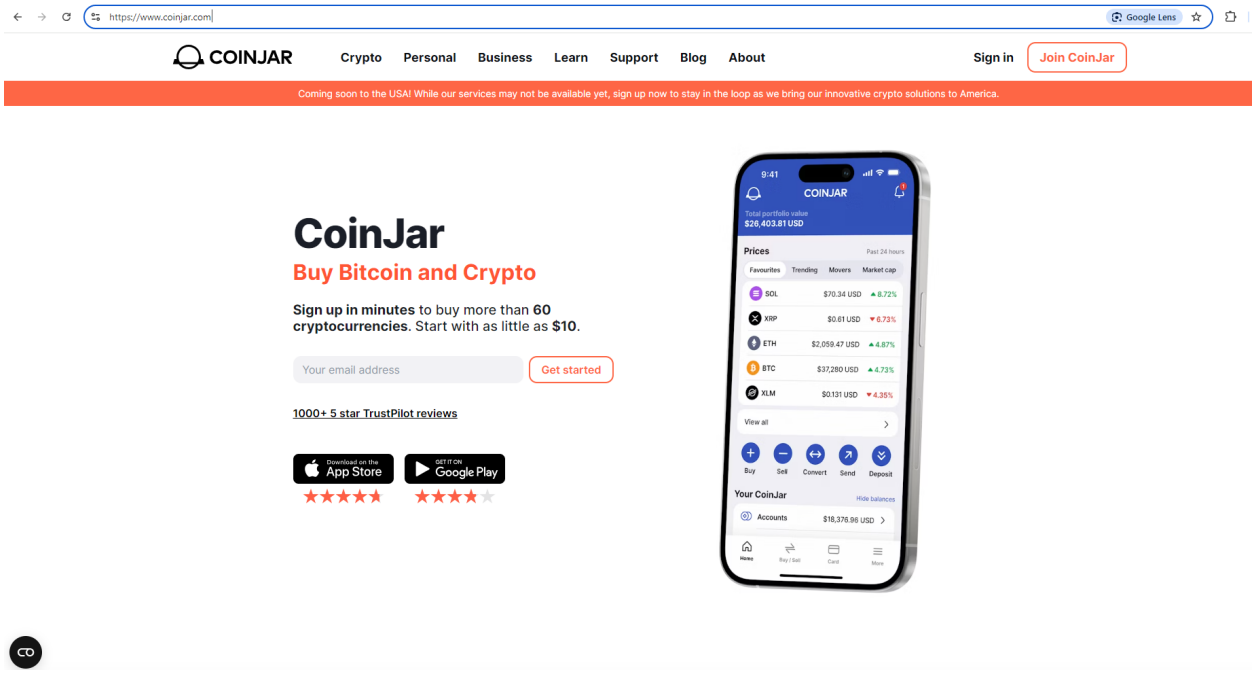
Pivot Address 2: 0x9f30654d708a2FD0C28855f8a5ee34a0Ce0b587c

18. This scheme is centered around a fake cryptocurrency investment strategy called "blockchain certification" and a fake cryptocurrency wallet that Defendants convinced Plaintiff

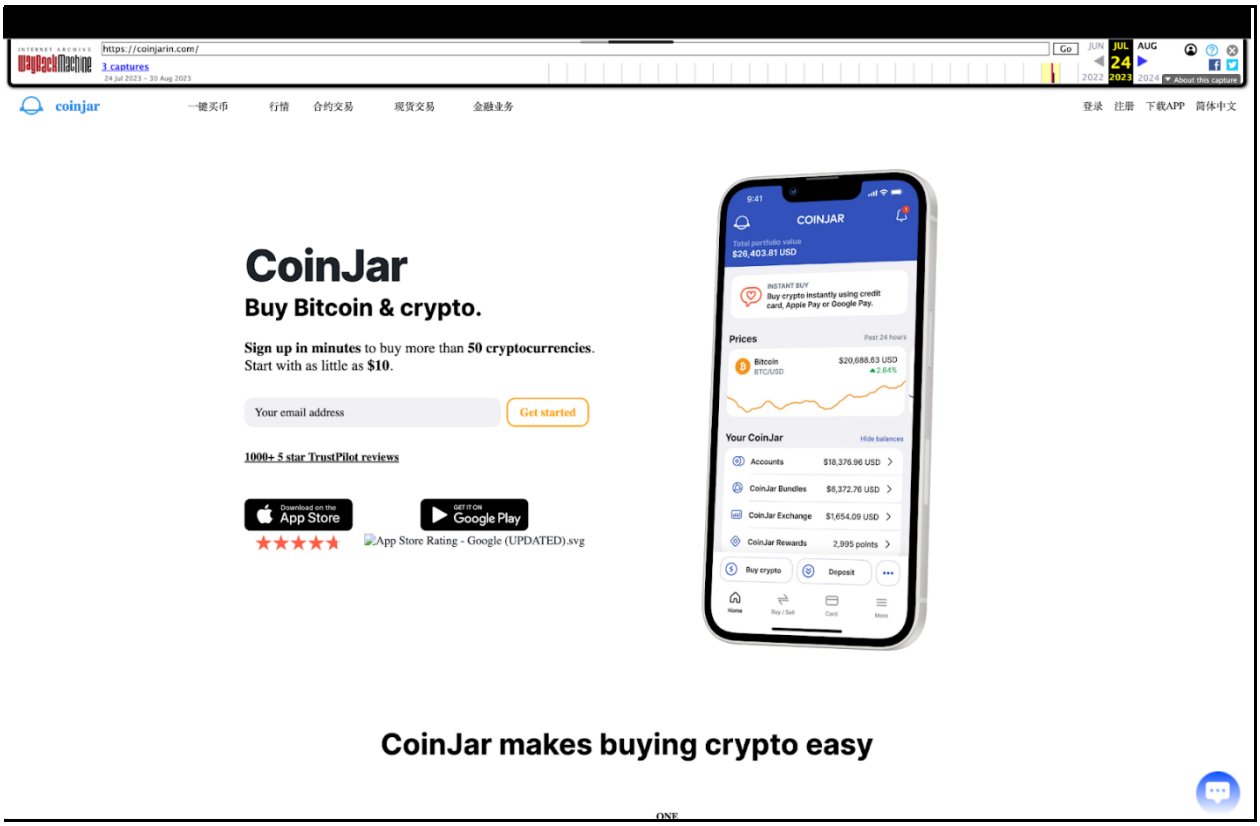
he controlled but which really was controlled by Defendants. The "blockchain certification" investment Defendants described to Plaintiff in the various communications I have reviewed, including communications described by or inserted into the Complaint, is nonsense. There is simply no cryptocurrency investment strategy that delivers returns that Defendants described or works in the way that Defendants described. Further, while SafePal's website can be accessed at the url https://www.safepal.com, Defendants directed Plaintiff to a website with a similar url of https://www.safepaladain.com.

19. Defendants similarly directed Plaintiff to a fraudulent version of a real crypto exchange called CoinJar. A comparison between the real CoinJar exchange, accessible at https://www.coinjar.com and an archived version of the fraudulent CoinJar website used by Defendants, accessible at the time at https://coinjarin.com, is below.

Real site:



Fraudulent site:



20. On November 16, 2023, following Defendants' instructions, Plaintiff initiated a wire transfer of $5,225 from his bank to what he believed was his SafePal wallet but was really a bank account controlled by Defendants. Plaintiff similarly initiated additional wire transfers on December 21, 2023, and January 12, 2024, in the amounts of $5,025 and $100,000, respectively, to what Plaintiff believed to be his CoinJar account but was actually a bank account controlled by Defendants. While Inca lacks the capacity to track funds after they arrive at a bank, based on my experience it is possible that Defendants used these funds to purchase cryptocurrency which would be transferred through the network controlled by Defendants.

21. Plaintiff, following Defendants' instructions, initiated two wire transfers—$25,025 on December 6, 2023, and $25,025 on December 11, 2023— to his Bitstamp crypto

exchange wallet. Continuing to follow Defendants' instructions, Plaintiff converted the funds to Ethereum and transferred 11 Ethereum (approximately $25,715 at the time) and 11.4 Ethereum (approximately $24,818 at the time) on December 7 and 11, respectively, to the to the address 0xd0FD2b2c038721CACa090E00f9529CA5312e16C0. Plaintiff believed this to be his SafePal account but it was really a crypto wallet controlled by Defendants. Once transferred, these funds were no longer within Plaintiff's control.

22. On December 8, 2023, Defendants exchanged the first 11 ETH transferred by Plaintiff for 25,715 USDT on the 1inch platform. Shortly thereafter, Defendants followed the same procedure to exchange the 11.4 ETH transferred by Plaintiff for 24,818 USDT.

23. On December 20, 2023, Defendants sent 62,729 USDT from 0xd0FD2b2c038721CACa090E00f9529CA5312e16C0 to the address 0xED468E2AfC52B259f6aD913127522dEc631Fdab1. The following day, December 21, 2023, Defendants transferred 98,220 USDT to the address 0x43EF882F03FD2113979A45064fea5a3450cd961E, and within the hour, the entire sum was moved to the Class Victim Pivot Address 0x63390bF7BD8c81809D69963D9d4b1E5F22844909 ("Pivot Address 1").

24. On December 22, 2023, Defendants sent a total of 501,573 USDT from Pivot Address 1 to the address 0x9f30654d708a2FD0C28855f8a5ee34a0Ce0b587c ("Pivot Address 2").

25. Later that same day, Defendants exchanged this 501,573 USDT as part of a larger sum of 565,850 USDT via the 1inch contract 0x8571C129F335832F6BBC76D49414AD2B8371a422 for 565,876 DAI.

26. From Pivot Address 2 (0x9f30654d708a2FD0C28855f8a5ee34a0Ce0b587c), Defendants transferred funds to a number of other crypto wallets.

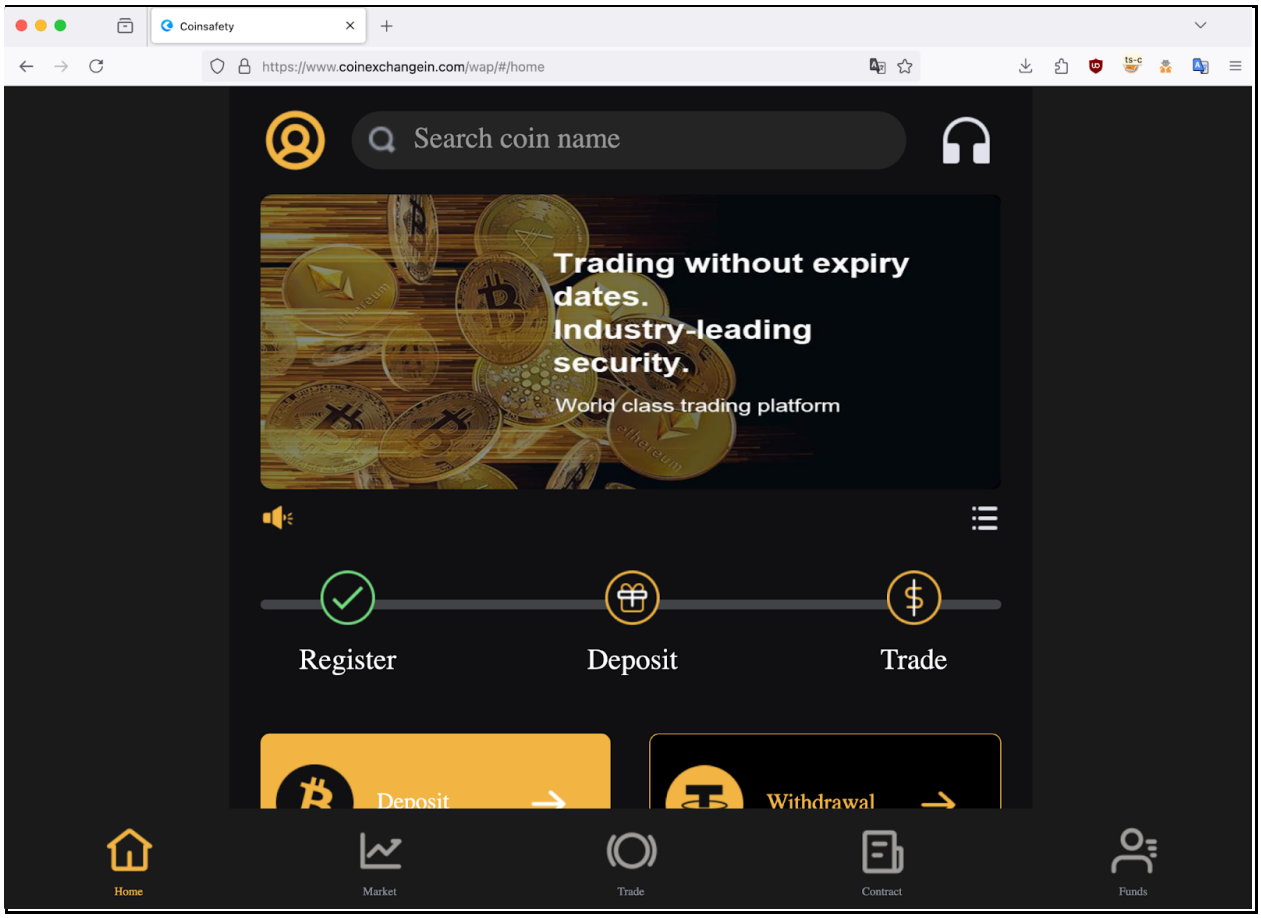
27. According to Inca's investigation, many of the wallets in the network of addresses identified by forward tracing Plaintiff's stolen funds through Pivot Addresses 1 and 2 to the wallets listed in Appendix A are associated with entities known among experts in the cryptocurrency community to be "scam entities" with 17 associated with Pivot Address 1 and 17 associated with Pivot Address 2.

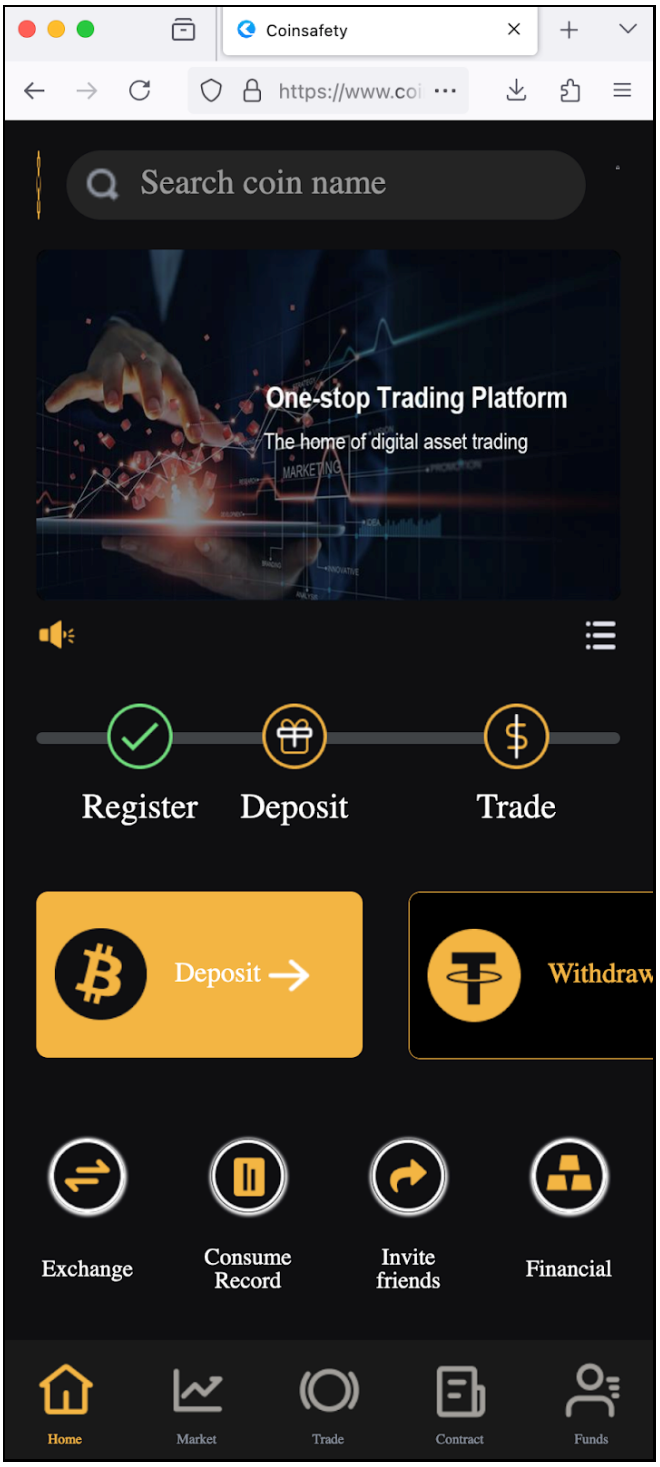
Mary Scott

Pivot Address 3: 0x9a3642A0C6D95485d3a5dF9cA25Ddc8971Be122b; and

Pivot Address 4: 0x1Ee69c435fd024DD639110C00059e0904bc2905E

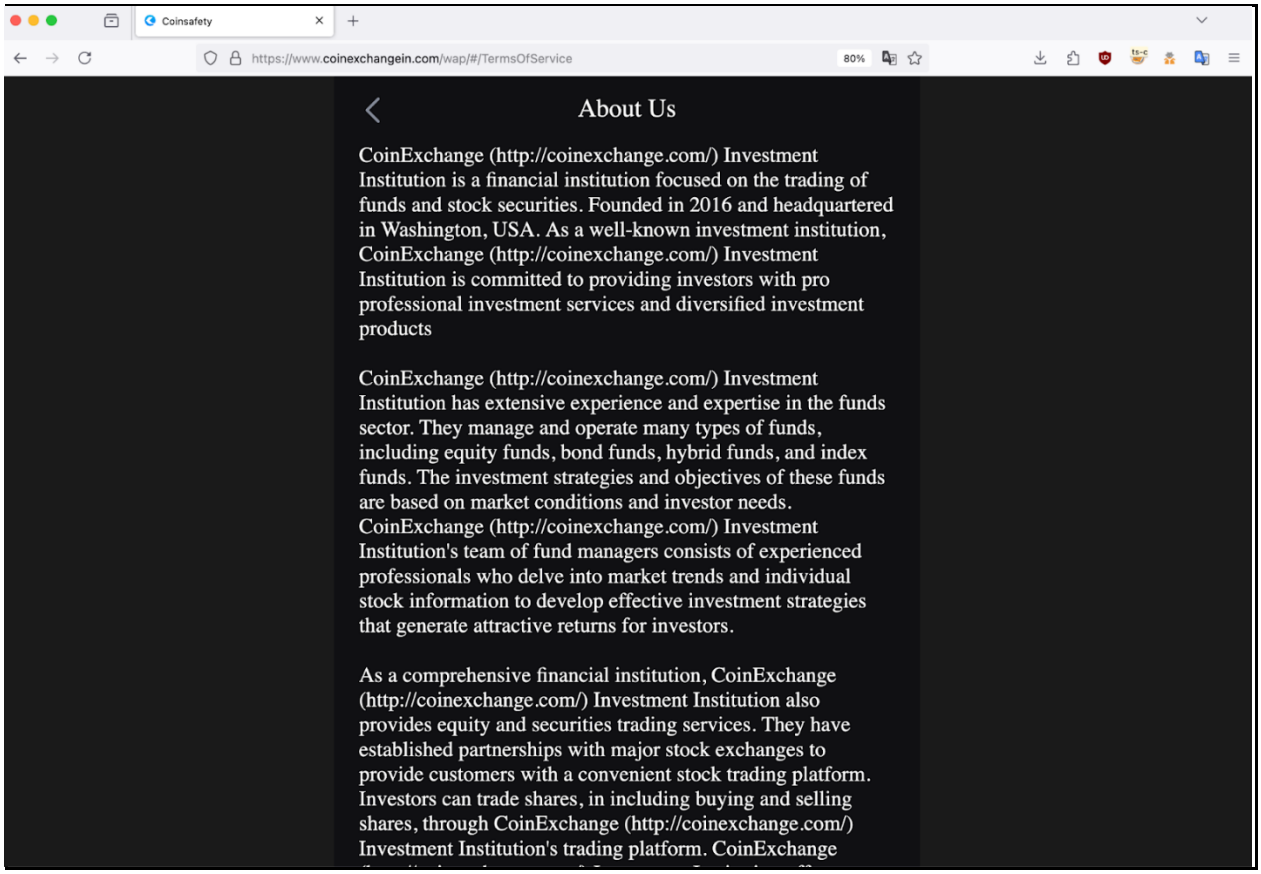
28. This scam is centered around the fictitious trading platform CoinExchange. Defendants directed Plaintiff to the web address https://www.coinexchangein.com/wap. This website contains realistic looking graphics supposedly related to a trading platform—but the platform does not really exist. Pictures of the website are below.


Coinsafety
https://www.coinexchangein.com/wap/#/home
Search coin name
Trading without expiry dates.
Industry-leading security.
World class trading platform
Register
Deposit
Trade
Deposit
Withdrawal
Home
Market
Trade
Contract
Funds



29. Eleven security vendors have flagged this domain as malicious. Inca's investigation uncovered several additional indications that the platform is fraudulent. First, the "About Us" section (reproduced below) contains clearly false information, and includes the

wrong web address (http://coinexchange.com/) instead of http://www.coinexchangein.com/wap. Similar to other fraudulent websites that Defendants used, the url ended with in.com/wap.



30. Second, the "About Us" page links to the website http://www.coinexchangeit.com, a domain registered at the same time and by the same registrar as https://www.coinexchangein.com/, which displays a Colorado Secretary of State Certificate of Fact of Good Standing for Aetem LLC, against which a customer complaint was filed to the Better Business Bureau for being a cryptocurrency scam.

31. Plaintiff initiated several wire transfers from his bank account to what he believed to be his CoinExchange account, but was really a bank account controlled by Defendants: $50,050 on January 11, 2024; $50,025 on January 25; $50,015 on January 26; and $10,801.18 on

February 8. While Inca lacks the capacity to track funds after they arrive at a bank, based on my experience it is possible that Defendants used these funds to purchase cryptocurrency which would be transferred through the network controlled by Defendants.

32. On May 7, 2024, following instructions of Defendant Mary Scott, Plaintiff transferred 5 USDC from his Coinbase account to the fake CoinExchange address 0x70B63e1F650CE252304c9E7f825fc4d68177706D. At that point the funds were no longer within Plaintiff's control.

33. On June 12, 2024, Defendants transferred 1,005 USDC from the initial address 0x70B63e1F650CE252304c9E7f825fc4d68177706D to the Class Victim Pivot Address 0x9a3642A0C6D95485d3a5dF9cA25Ddc8971Be122b (Pivot Address 3), which, based on its transaction history, acts as an intermediary address for mixing stolen funds for the Defendant.

34. On June 21, 2024, Defendants swapped 3,299 USDC for 3,299 USDT via the decentralized exchange Tokenlon (address 0x4a14347083B80E5216cA31350a2D21702aC3650d).

35. Later that day, Defendants transferred 41,846 USDT from Pivot Address 3 to the address 0x86f250A03BD182D022d48C1664a38d8aD102AE75.

36. On June 22, 2024, Defendants transferred 244,160 USDT from 0x86f250A03BD182D022d48C1664a38d8aD102AE75 to 0x8E7B486160f9A4c94A850A3F3254AD98734E3608.

37. Shortly thereafter, Defendants transferred 244,160 USDT from 0x8E7B486160f9A4c94A850A3F3254AD98734E3608 to 0xec641A117b7BB421e578e0857893Cc16738dC556. Following this, the stolen funds were split into several branches.

38. Branch 1. On June 22, 2024, Defendants sent 42,500 USDT from 0xec641A117b7BB421e578e0857893Cc16738dC556 to the OKX deposit wallet 0x5d8814d1268d70d89c2EE8cdF9e14fF64902fcE6.

39. Branch 2. On June 25 Defendants sent 134,482 USDT from wallet address 0xec641A117b7BB421e578e0857893Cc16738dC556 to wallet address 0xCbD158bf619EEC521BcE7582529Dc5CDe404D073. 3 minutes later, Defendants sent 134,580 USDT from wallet address 0xCbD158bf619EEC521BcE7582529Dc5CDe404D073 to OKX Deposit Address 0x0eC4E0303897a8E8b477Fdce43e577B3981b5617.

40. Additionally, Defendants made further transfers from 0x8E7B486160f9A4c94A850A3F3254AD98734E3608 to several other deposit addresses, including 0xdA22870E0Bd87133250fbC319476E278D7af93c2 (OKX).

41. On May 9, 2024, following the instructions of the Defendant Mary Scott, Plaintiff sent 0.00334134 ETH from his Coinbase account to the to the fake CoinExchange address 0xe978a33aA86529dA089F5C1EEfDDcC17939Ebc88. At the time of the transaction, the asset's value was approximately 10 USD. Once transferred, these funds were no longer within Plaintiff's control.

42. Then, on May 24, 2024, Defendants transferred 1.2357 ETH from 0xe978a33aA86529dA089F5C1EEfDDcC17939Ebc88 to the Class Victim Pivot Address 0x1Ee69c435fd024DD639110C00059e0904bc2905E (Pivot Address 4), which, based on its transaction history, acts as an intermediary address for mixing stolen funds for the Defendant. This amount was swapped for 4,624 USDT on the decentralized exchange Tokenlon (0x4a14347083B80E5216cA31350a2D21702aC3650d).

43. On June 1, 2024, Defendants transferred 15,251 USDT from Pivot Address 4 to 0xdbc72fCbd56B1481A6EF27Ab247c71f7fB87eA66.

44. Later, on June 9, 2024, Defendants sent 130,000 USDT from 0xdbc72fCbd56B1481A6EF27Ab247c71f7fB87eA66 to the address 0x3CFB55D880BF8ca2295eD0fB25AA70852E7075a3.

45. On June 25, 2024, Defendants transferred 100,000 USDT from 0x3CFB55D880BF8ca2295eD0fB25AA70852E7075a3 to 0x0027F85Daffd156Fa4d501bf1c0482b328bB8A33.

46. Shortly after, on June 25, 2024, Defendants sent 100,000 USDT from 0x0027F85Daffd156Fa4d501bf1c0482b328bB8A33 to the Binance Deposit Address 0xb4B44239Bc9B5c4c810A181Cb5aFE2b15F1C7087.

47. Inca's investigation as set forth above determined that the following deposit addresses are controlled by Defendants and contain crypto assets that were stolen from class members:

0xb4B44239Bc9B5c4c810A181Cb5aFE2b15F1C7087 (Binance)

0xdA22870E0Bd87133250fbC319476E278D7af93c2 (OKX)

0x5d8814d1268d70d89c2EE8cdF9e14fF64902fcE6 (OKX)

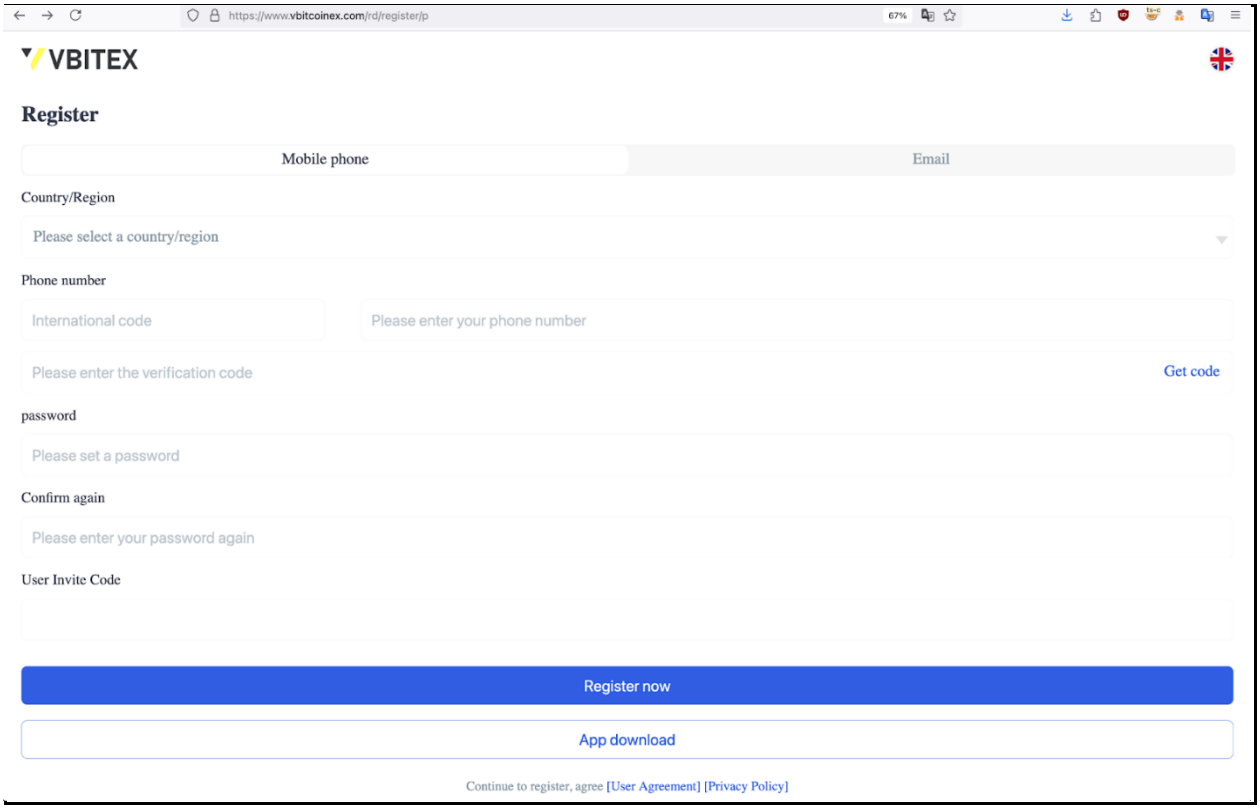
0x0eC4E0303897a8E8b477Fdce43e577B3981b5617 (OKX)

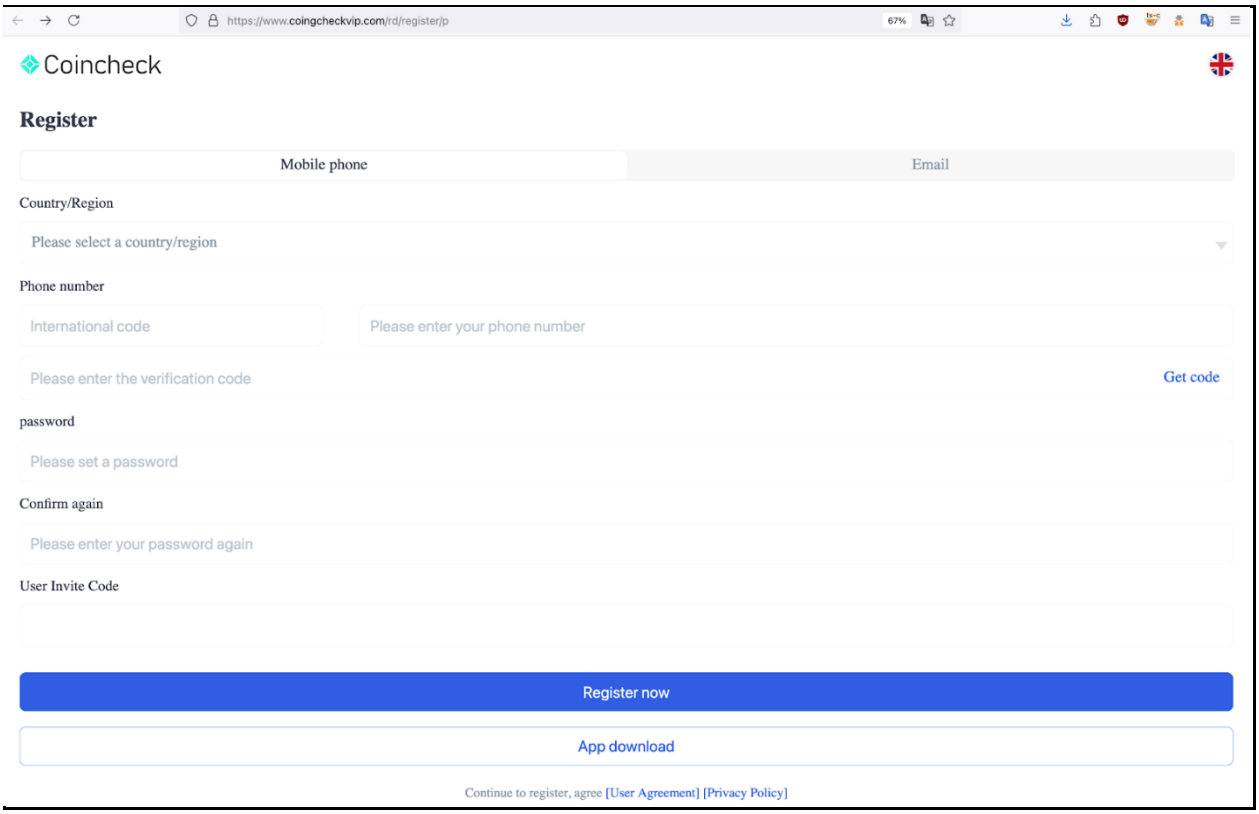
48. According to Inca's investigation, many of the wallets in the network of addresses identified by forward tracing Plaintiff's stolen funds through Pivot Addresses 3 and 4 to the wallets listed in Appendix A are associated with entities known among experts in the cryptocurrency community to be "scam entities," with 1 associated with Pivot Address 3 and 21 associated with Pivot Address 4.

Verna

Pivot Address 5: 0xd2b57f175E2CBb1B561d6109CbAAF17B09AcEcE2

49. This scheme is centered around a fictitious gold trading platform called Vbitex. Defendants directed Plaintiff to the web address https://www.vbitcoinex.com/p/m and https://www.vbitcoinex.com/p/app. Inca's investigation determined this website to be fraudulent. One indication that the platform is fraudulent is that the website https://www.vbitcoinex.com has an interface identical to and shares the same IP address as coingcheckvip.com. A comparison between the two websites is below.



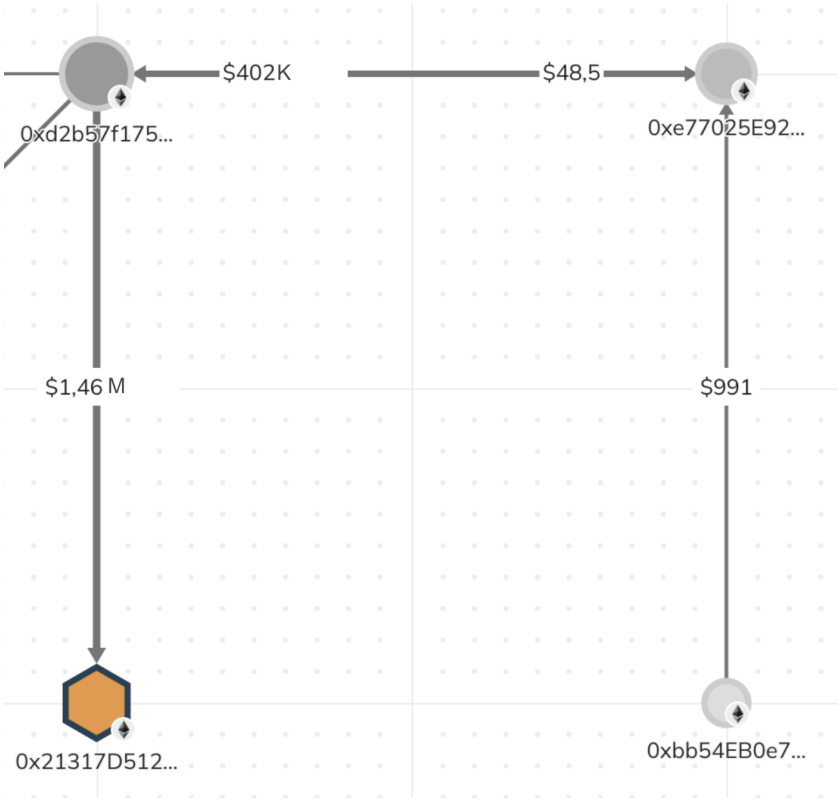


50. Further, the user agreement for Vbitex is identical to the user agreement for https://payotc365.com. It is common for the perpetrators of pig butchering schemes to copy parts of legitimate websites or reuse parts of websites across various scams.

51. On March 5, 2024, following the instructions of Defendant Verna, Plaintiff sent 0.133 ETH from his MetaMask wallet (a legitimate software cryptocurrency wallet) to wallet address 0x19cBE2012d79f28065cD3005Ab8Cbc12A301c82B, which he believed to be his Vbitex account, but was really a wallet controlled by Defendants. At the time of the transaction, the asset's value was approximately 470 USD. Once transferred, these funds were no longer within Plaintiff's control.

52. That same day, Defendants transferred these funds to the Class Victim Pivot Address 0xd2b57f175E2CBb1B561d6109CbAAF17B09AcEcE2 (Pivot Address 5). Just half an

hour later, the funds were transferred to the KuCoin Deposit Address 0x21317D512417c31a5CEA75Fb6A57f6206F02c0e6. Based on the transaction history of Pivot Address 5, Defendants use the wallet as an intermediary for mixing stolen funds. A visual representation of these transactions is below.



53. On March 29, 2024, following the instructions of Defendant Verna, Plaintiff sent 0.138 ETH, which was approximately equal to 480 USD at the time of the transaction, to wallet address 0xe77025E924346A3F140a24d2B92c5b8449605235, another fake Vbtex wallet. Once transferred, these funds were no longer within Plaintiff's control. That same day Defendants transferred these funds to Pivot Address 5 and from there to the KuCoin Deposit Address.

54. On April 5, 2024, following the instructions of Defendant Verna, Plaintiff sent 0.151 ETH, worth approximately $490 at the time of the transaction, to the same fake Vbtex wallet. Once transferred, these funds were no longer within Plaintiff's control. Defendants

followed the same procedure and transferred these funds the same day to Pivot Address 5 and from there to the KuCoin Deposit Address.

55. Inca's investigation as set forth above determined that the KuCoin Deposit Address (0x21317D512417c31a5CEA75Fb6A57f6206F02c0e6) is controlled by Defendants and contains crypto assets that were stolen from class members.

56. According to Inca's investigation, 12 of the wallets in the network of addresses identified by forward tracing Plaintiff's stolen funds through Pivot Address 5 to the wallets listed in Appendix A are associated with entities known among experts in the cryptocurrency community to be "scam entities."

Ettie Lee

Pivot Address 4: 0x1Ee69c435fd024DD639110C00059e0904bc2905E

57. This scheme is centered around the legitimate crypto platform Alpha Homora. Defendants showed Plaintiff the Alpha Homora platform and then instructed him to send crypto to what they told him was the Alpha Homora platform but was really a crypto wallet controlled by Defendants. It is clear that the wallets Defendants directed Plaintiff to send funds to were not associated with the Alpha Homora platform because all wallets associated with the Alpha Homora platform are "smart contracts" and none of the wallets that Plaintiff actually transferred crypto to as part of this scheme were "smart contracts."

58. On May 24, 2024, following the instructions of Defendant Ettie Lee, Plaintiff transferred 0.01084736 ETH, worth approximately $30 at the time, from his Coinbase wallet to the address 0xEEAb811232873c3e7777A78868FE222F45766206, which Plaintiff believed to be Alpha Homora, but was really a wallet controlled by Defendants. Once transferred, these funds were no longer within Plaintiff's control.

59. On May 30, 2024, Defendants transferred 5.19 ETH from 0xEEAb811232873c3e7777A78868FE222F45766206 to the ChangeNOW Deposit Address 0xcA2DB3Fe31046CCaA71F25AD1FBA6F874094030E.

60. On May 24, 2024, following the instructions of Defendants, Plaintiff made two payments of 798 USDC and 6,696 USDC from his Coinbase wallet to the address 0xEEAb811232873c3e7777A78868FE222F45766206. Plaintiff similarly transferred 4,997 USDC on May 29 to the same wallet. Once transferred, these funds were no longer within Plaintiff's control.

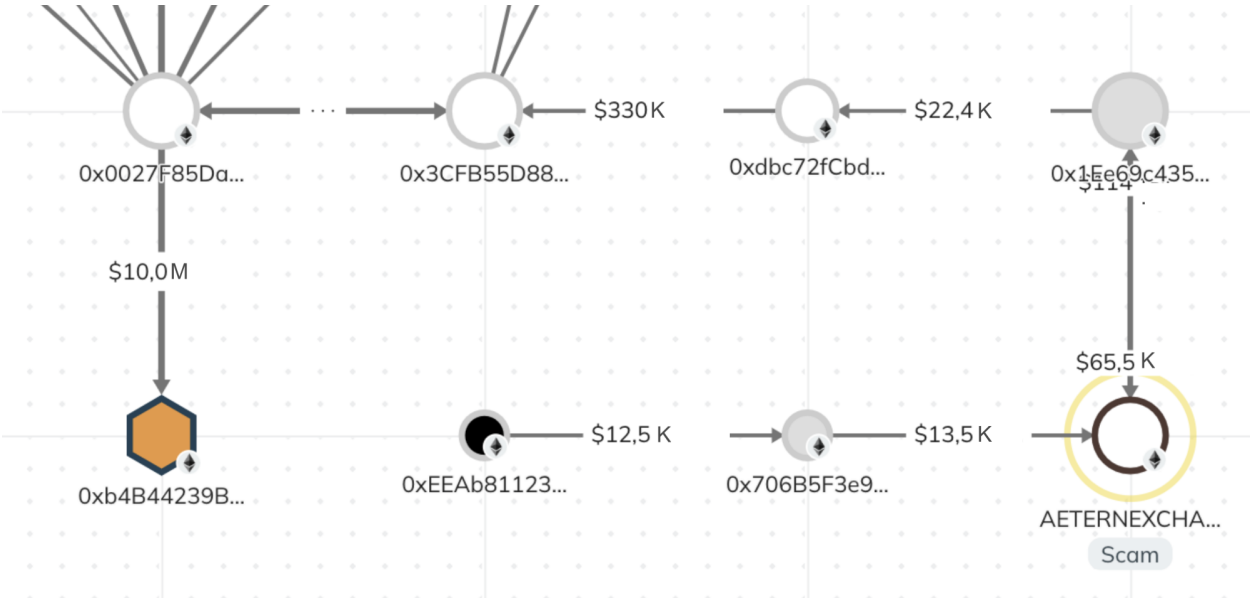
61. By the evening of May 29, 2024, the total amount accumulated at the initial address was 12,491 USDC. At that time Defendants transferred the 12,491 USDC from the initial address to 0x706B5F3e94F8EaA4a06005Ff297DBF8eAf718e2f and then a few minutes later to address 0x18818Bd9b3c16394E64499994319Bd436f0134A8. The same amount of USDC (12,491) was then sent from wallet address 0x18818Bd9b3c16394E64499994319Bd436f0134A8 to Pivot Address 4, 0x1Ee69c435fd024DD639110C00059e0904bc2905E.

62. On May 30, 2024, Defendants swapped 12,491 USDC for 12,501 USDT using the decentralized exchange Tokenlon.

63. On June 1, 2024, Defendants transferred 12,501 USDT, as part of a larger sum totaling 15,251 USDT, to address 0xdbc72fCbd56B1481A6EF27Ab247c71f7fB87eA66. Then, on June 9, Defendants transferred the funds to address 0x3CFB55D880BF8ca2295eD0fB25AA70852E7075a3 as part of a total 130,000 USDT.

64. On June 25, 2024, Defendants transferred 100,000 USDT from 0x3CFB55D880BF8ca2295eD0fB25AA70852E7075a3 to address

0x0027F85Daffd156Fa4d501bf1c0482b328bB8A33 and then to the Binance Deposit Address 0xb4B44239Bc9B5c4c810A181Cb5aFE2b15F1C7087. On June 26, 2024, Defendants sent the remaining 30,000 USDT from 0x3CFB55D880BF8ca2295eD0fB25AA70852E7075a3 to 0x0027F85Daffd156Fa4d501bf1c0482b328bB8A33 as part of a larger sum totaling 273,673 USDT. Within an hour Defendants transferred the entire amount of 273,673 USDT to the same Binance Deposit Address 0xb4B44239Bc9B5c4c810A181Cb5aFE2b15F1C7087. A visual representation of these transactions is below.



65. Inca's investigation as set forth above determined that the Binance deposit address 0xb4B44239Bc9B5c4c810A181Cb5aFE2b15F1C7087 is controlled by Defendants and contains crypto assets that were stolen from class members.

Keiko Fujiwara

Pivot Address 6: 0xb28B13e4a88316bDa38675C0BFC23c974a7fb5e4

66. This scheme is centered around a fictitious cryptocurrency trading platform called ICMarket. Inca's investigation determined the ICMarket website to be fraudulent. One indication that the platform is fraudulent is that the Terms and Conditions include no contact information,

but rather a placeholder for contact information that was apparently inadvertently left in from a template. Further, the SSL for the website is undefinable, a significant red flag suggesting fraudulent activity.

67. On June 4, 2024, following instructions from Defendant Keiko Fujiwara, Plaintiff transferred 1,074 USDC from his Coinbase wallet to the fake cryptocurrency exchange ICMarket, associated with the initial address 0xdCEc886f0D82074F4D5d03657d95D3aCbE05c8b1, which Plaintiff believed to be his ICMarket account, but which was really a wallet controlled by Defendants. Once transferred, these funds were no longer within Plaintiff's control.

68. Following Defendant's further instructions, Plaintiff transferred an additional 1,219 USDC from his Coinbase wallet to the same initial address On June 21, 2024, bringing the total amount sent to 2,293 USDC. Once transferred, these funds were no longer within Plaintiff's control.

69. On June 21, 2024, at 05:25 UTC, Defendants moved the total of 2,294 USDC from the initial address to the Pivot Address 3 (0x9a3642A0C6D95485d3a5dF9cA25Ddc8971Be122b). This pivot address acts as an intermediary for mixing stolen funds.

70. At 05:26 UTC on the same day, the pivot address swapped 3,299 USDC for 3,301 USDT using the decentralized exchange Tokenlon.

71. Later on June 21, 2024, at 14:39 UTC, Defendants transferred 41,846 USDT from Pivot Address 3 to the address 0x86f250A03BD182D022d48C1664a38d8aD102AE75.

72. On June 22, 2024, at 06:01 UTC, Defendants sent 244,160 USDT from 0x86f250A03BD182D022d48C1664a38d8aD102AE75 to the address 0x8E7B486160f9A4c94A850A3F3254AD98734E3608.

73. Immediately thereafter, the same amount of 244,160 USDT was transferred from 0x8E7B486160f9A4c94A850A3F3254AD98734E3608 to the address 0xec641A117b7BB421e578e0857893Cc16738dC556.

74. Subsequently, on June 22, 2024, the following transfers were made from 0xec641A117b7BB421e578e0857893Cc16738dC556 to the OKX deposit address 0x5d8814d1268d70d89c2EE8cdF9e14fF64902fcE6:

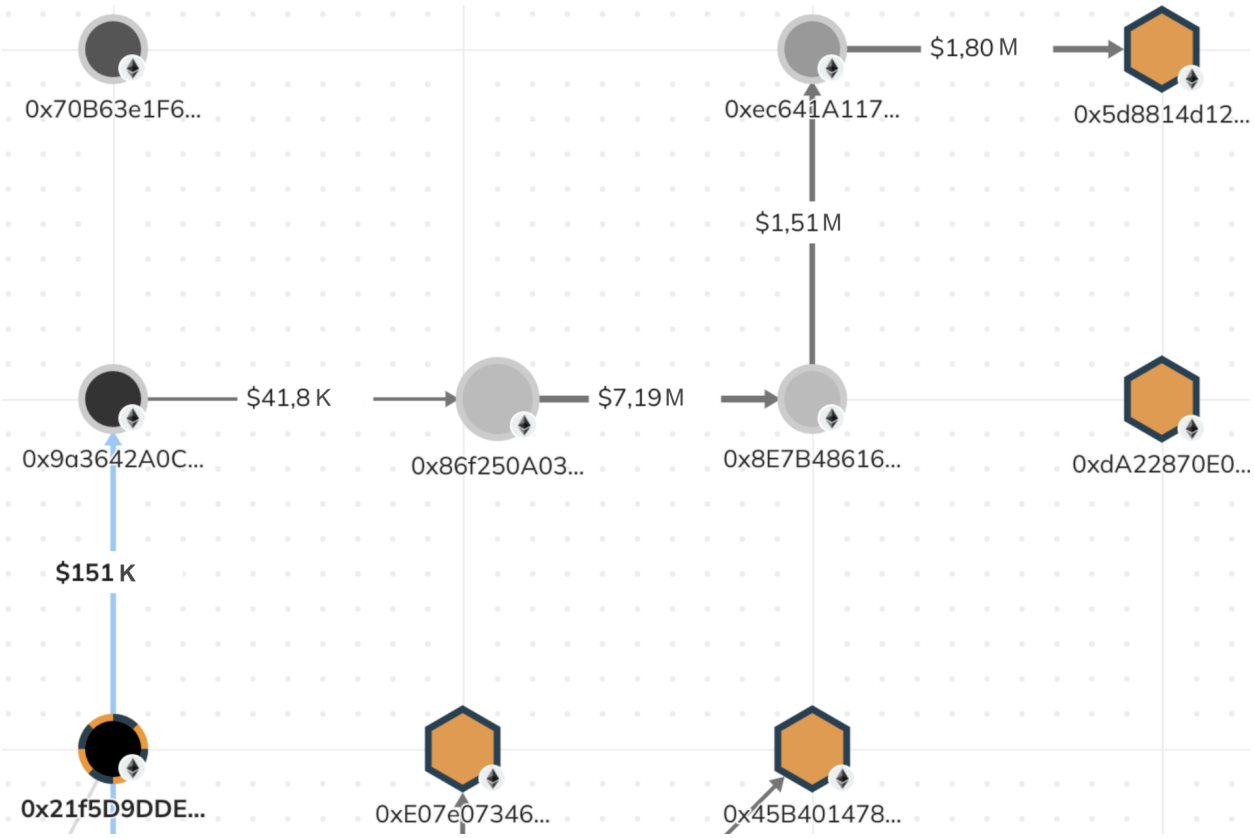
06:03 UTC: 42,500 USDT

06:32 UTC: 62,584 USDT

07:04 UTC: 63,852 USDT

07:41 UTC: 75,220 USDT

A visual representation of these transactions is below:



75. On July 17, 2024, following Defendants' instructions, Plaintiff transferred 3,597 USDC from his Coinbase account to the fake ICMarket address (0xdCEc886f0D82074F4D5d03657d95D3aCbE05c8b1). The following day, on July 18, 2024, Plaintiff transferred 4,415 USDC to the same address. Once transferred, these funds were no longer within Plaintiff's control.

76. On July 20, 2024, Defendants moved 8,012 USDC from the ICMarket address to the Class Victim Pivot Address 0xb28B13e4a88316bDa38675C0BFC23c974a7fb5e4 (Pivot Address 6), which, based on its transaction history, acts as an intermediary address for mixing stolen funds for the Defendants. After that the amount of 8,012 USDC was swapped for 8,004 USDT via the decentralized exchange Tokenlon (address 0x4a14347083B80E5216cA31350a2D21702aC3650d). Following this, the stolen funds were split into several branches.

77. Branch 1. On August 17, 2024, Defendants transferred 73,485 USDT from Pivot Address 6 to the address 0xfD4A4df5A4969857AebC8366373b364945d5756f. After a period of accumulation, on September 9, 144,192 USDT was sent to the address 0x631458eb3B175A0a7784Bc9d0C94cC3BbD1B2D8D, and the next day, 143,262 USDT was transferred to the address 0xE11126aFC596d9489a0Fc16a9bccb2C3c587D119.

78. Finally, on September 10, three transactions of 40,000 USDT, 30,000 USDT, and 29,997 USDT were sent to the OKX Deposit Address 0x03A080f0763E53A2304e98A4f9bC663f66ad1B26, and another transaction of 30,000 USDT was sent to the OKX Deposit Address 0x5594c5ECA2B8CF2CD3A2c0FbA172F1dF2C15645F.

79. Branch 2. On August 17, Defendants transferred 73,485 USDT from Pivot Address 6 to the address 0xfD4A4df5A4969857AebC8366373b364945d5756f. Then, on August 28, 230,000 USDT was sent from the address 0xfD4A4df5A4969857AebC8366373b364945d5756f to the address 0x5945e98956C5EF29731a52E2fA4Fa8d0b53df314. On August 30, Defendants transferred 36,000 USDT from address 0x5945e98956C5EF29731a52E2fA4Fa8d0b53df314 to the address 0x049be558d72B1747C05c63EaA42e08471D34E3D5.

80. On September 4, Defendants sent 35,000 USDT from address 0x049be558d72B1747C05c63EaA42e08471D34E3D5 to the address 0xBA39f73fA46D4Dc2B4c3Fb7e81598A3F10beAe87, and just two minutes later, 35,719 USDT was transferred to the Binance Deposit Address 0xE025Fcc2D58CA09852DEd8d0FCdb9db4355f4a8F.

81. Branch 3. On August 3 and August 9, Defendants sent transactions of 57,307 USDT and 57,471 USDT, respectively, from Pivot Address 6 to wallet address 0x194bD7543A786561510ca7fCAE82caEAa6DE625d.

82. On August 10, Defendants sent a transaction of 127,479 USDT from wallet address 0x194bD7543A786561510ca7fCAE82caEAa6DE625d to wallet address 0x9AFa19B223dEEC9e2352D17c495a48854bb1748C. Two minutes later, Defendants sent 273,130 USDT from wallet address 0x9AFa19B223dEEC9e2352D17c495a48854bb1748C to wallet address 0x827BA7f9A58c3631AEEA9e3Fd9d5ff5bC70B00D5.

83. On August 12, Defendants sent a transaction of 257,995 USDT from wallet address 0x827BA7f9A58c3631AEEA9e3Fd9d5ff5bC70B00D5 to wallet address 0xACf7417bd53dc79FD12E6601f10138Cfa1413546.

84. On August 15, Defendants sent a transaction of 721,000 USDT from wallet address 0xACf7417bd53dc79FD12E6601f10138Cfa1413546 to wallet address 0x97E64512dcbdc8Ec9b78F7b4d1DC10eDf5630527.

85. That same day, Defendants sent two transactions of 360,500 USDT each from wallet address 0x97E64512dcbdc8Ec9b78F7b4d1DC10eDf5630527 to Binance Deposit Address 0xa3364D012dA0E925b908cfE98008418D4d145573.

86. Branch 4. On July 26, Defendants sent 100,000 USDT from Pivot Address 6 to the address 0xDeB6176f6Ef069569a0e499eAD40C59B42f2BcE7. Then, on July 31, these funds were transferred in two transactions of 5,000 USDT and 95,000 USDT to the address 0xC1916b7D03247CcB29A25E91847EB80c9494989c.

87. Ten minutes later, the entire amount of 100,000 USDT was sent to the address 0xB2d50D047C585BF65D62e66D51abD45E9E774155. One hour later, 60,000 USDT was

transferred to the address 0x7ca3E3Bce128a7A24A9F01ecD5F6E96c38140B2f, from which the full amount was immediately sent to the Binance Deposit Address 0x8E670D1d6993413Ce7B23FCEB4e26101D2b816e0.

88. Branch 5. On July 23, Defendants sent 30,000 USDT from the address 0xB2d50D047C585BF65D62e66D51abD45E9E774155 to the address 0x7ca3E3Bce128a7A24A9F01ecD5F6E96c38140B2f and a few minutes later, the entire amount was sent to the Binance Deposit Address 0x8E670D1d6993413Ce7B23FCEB4e26101D2b816e0.

89. Inca's investigation as set forth above determined that the following deposit addresses are controlled by Defendants and contain crypto assets that were stolen from class members:

0x5d8814d1268d70d89c2EE8cdF9e14fF64902fcE6 (OKX)

0x03A080f0763E53A2304e98A4f9bC663f66ad1B26 (OKX)

0x5594c5ECA2B8CF2CD3A2c0FbA172F1dF2C15645F (OKX)

0xE025Fcc2D58CA09852DEd8d0FCdb9db4355f4a8F (Binance)

0xa3364D012dA0E925b908cfE98008418D4d145573 (Binance)

0x8E670D1d6993413Ce7B23FCEB4e26101D2b816e0 (Binance)

90. According to Inca's investigation, 19 of the wallets in the network of addresses identified by forward tracing Plaintiff's stolen funds through Pivot Address 6 to the wallets listed in Appendix A are associated with entities known among experts in the cryptocurrency community to be "scam entities."

Conclusion

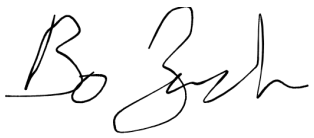
91. In summary, Inca's analysis demonstrates that the cryptocurrency assets belonging to Class Members, including Plaintiff Andrew Chait, were systematically misappropriated by the Defendants through the use of fraudulent platforms. The wallets that now hold the stolen funds are identified in Appendix A.

92. Based upon my expertise in blockchain forensics and my substantial experience investigating "pig butchering" schemes similar to this one, if Plaintiff is required to wait until after the Defendants receive notice of this action, it is highly likely that Defendants will transfer cryptocurrency at issue beyond the reach of discovery or recovery.

93. I am familiar with the process of providing notice via the Input Data Message process, whereby a message with a link to a website containing documents is sent using the Input Data field on a transaction on the Ethereum blockchain. In my experience, the method of notice proposed in the Proposed Order to Show Cause and Temporary Restraining Order is reasonably calculated to and would likely result in actual notice of those documents to the individuals or entities that control those wallets, and the existence and contents of those service tokens would be readily apparent to the owners.

94. I affirm this 23rd day of October, 2024, under the penalties of perjury under the laws of New York, which may include a fine or imprisonment, that the foregoing is true, and I understand that this document may be filed in an action or proceeding in a court of law.

Dated: October 23, 2024



By: _____
Charles Bo Zach

Inca Digital
1100 15th St. NW
Washington, D.C. 20005
Phone: (908) 219-7750
Email: charles.zach@inca.digital

APPENDIX A

Binance
0x8E670D1d6993413Ce7B23FCEB4e26101D2b816e0
0xE025Fcc2D58CA09852DEd8d0FCdb9db4355f4a8F
0xa3364D012dA0E925b908cfE98008418D4d145573
0xb4B44239Bc9B5c4c810A181Cb5aFE2b15F1C7087

OKX
0x5d8814d1268d70d89c2EE8cdF9e14fF64902fcE6
0x0eC4E0303897a8E8b477Fdce43e577B3981b5617
0xdA22870E0Bd87133250fbC319476E278D7af93c2
0x03A080f0763E53A2304e98A4f9bC663f66ad1B26
0x5594c5ECA2B8CF2CD3A2c0FbA172F1dF2C15645F

KuCoin
0x21317D512417c31a5CEA75Fb6A57f6206F02c0e6

Certification Pursuant to 22 NYCRR § 202.8-b

I, Rishi Bhandari, at attorney duly admitted to practice law before the courts of the State of New York, hereby certifies that this Affirmation contains 4,894 words, excluding the parts exempted by § 202.8-b(b), and therefore complies with the word count limit set forth in 22 NYCRR § 202.8-b(a).

Dated: New York, New York
October 23, 2024

By: /s/ Rishi Bhandari
Rishi Bhandari, Esq.