

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

STEPHEN B. SHAYA, on behalf of)	
Himself and all others similarly situated,)	
)	Case No.
Plaintiff,)	
)	Hon.
-against-)	
)	<u>CLASS ACTION</u>
KYLIE NOFS, ZHU SHICAI, LUO)	
YANBING, LIN YIN, YANG ZHENLIN,)	
and JOHN DOE NOS. 1-25,)	
)	
Defendants.)	
)	

COMPLAINT

Class Plaintiff Stephen Shaya (“Plaintiff”), individually and on behalf of all others similarly situated, by and through his undersigned counsel, Altior Law, P.C., brings this Class Action Complaint against Defendants Kylie Nofs, Zhu Shicai, Luo Yanbing, Lin Yin, Yang Zhenlin, and John Doe Nos. 1-25, and alleges as follows:

INTRODUCTION

1. This case is about the theft of cryptocurrency using a scheme known as “pig butchering.”

2. The scheme is centered around a fake cryptocurrency trading platform composed of several websites that use the phrase “Coinbit,” including Coinbitjscz.top, Coinbitkgtf.top, and Coinbitqodf.com (collectively, “Coinbit” or

the “Coinbit Platform”). Defendants used the Coinbit Platform to lure a common class of victims (“Class Members,” or the “Class”) to transfer funds to cryptocurrency wallets controlled by Defendants. This class action is brought to freeze wallets containing Class Member funds that Defendants converted, and return these funds to Class Member victims.

3. On information and belief, the Coinbit Platform is unrelated to Coinbits Inc., a financial technology company incorporated in Delaware, or Coinbits Inc. affiliated individuals, entities, websites, and applications, including coinbits.app.

4. Plaintiff is a resident of Bloomfield Hills, Michigan. Like other similarly situated Class Members, Plaintiff was tricked by one or more individuals, including a person identifying herself as Kylie Nofs (“Nofs”); one or more persons or entities affiliated with the Coinbit Platform; and other unknown persons, John Does Nos. 1-25, as part of a common scheme to transfer funds to cryptocurrency wallets controlled by Defendants using the Coinbit Platform.

5. The scheme with Plaintiff began on or about July 24, 2023, when Nofs first contacted Plaintiff through Facebook. Nofs represented that she lived in San Francisco, California and traveled frequently between cities in the U.S. Nofs and Plaintiff engaged in regular text conversations, first on Facebook subsequently using Telegram, where Nofs stated that she engaged in cryptocurrency trading and could assist Plaintiff to invest through the Coinbit Platform. Nofs represented that she

would help Plaintiff, lend Plaintiff funds, and invest alongside Plaintiff using the Coinbit Platform.

6. Nofs assisted Plaintiff in accessing the Coinbit Platform and transferring funds from his accounts to accounts that Defendants represented were his accounts on the Coinbit Platform. As described below, on November 3, 2023, Plaintiff transferred \$14,000 to an account controlled by Defendants. During December 2023, Plaintiff transferred increasing amounts to accounts controlled by Defendants. In aggregate, Plaintiff transferred a total of nearly \$400,000.

7. Defendants represented that Plaintiff had invested his funds in cryptocurrency assets through the Coinbit Platform. Defendants subsequently blocked Plaintiff from accessing his Coinbit Platform accounts and transferring funds.

8. After Plaintiff could not recover his funds, he contacted Inca Digital (“Inca”), a cryptocurrency investigation firm, which traced his transactions and confirmed that Defendants were orchestrating a “pig butchering” scheme. As described below, Inca investigated other Coinbit Platform transactions and found that these transactions were part of a common scheme to convert Class Member funds.

9. Based on Inca’s investigation to date, Defendants’ conversion scheme involved transactions during the period from early November 2023 through at least

February 28, 2024, included approximately 200 to 250 Class Member victims, and involved the conversion by Defendants of approximately \$16 million of Class Member funds.

10. To date, the investigation has identified the wallet addresses set forth in Exhibit A as part of the common “pig butchering” allegations centered around the Coinbit Platform. Plaintiff requests that this Court issue an Order freezing these wallet addresses.

JURISDICTION AND VENUE

11. Plaintiff lives in Bloomfield Hills, Michigan. He is a family practice physician in Michigan and an officer of J&B Medical, a global health care solutions company, based in Wixom, Michigan. He also is an officer of Akkad Holdings, LLC, a family office based in Bloomfield Hills, Michigan.

12. Nofs represented to Plaintiff that she was a resident of San Francisco, California, and her Facebook profile stated, at the time of the wrongdoing alleged here, that she was a San Francisco, California resident. Nofs also provided Plaintiff with U.S. phone numbers and contact information. The true identity and residence of Nofs is currently unknown and is subject to ongoing investigation.

13. Defendants Zhu Shicai, Luo Yanbing, Lin Yin, Yang Shelin, and John Doe Nos 1-25 are persons of unknown citizenship who participated in the perpetration of the wrongdoing alleged herein. One or more of Defendants were

affiliated with Coinbit and the Coinbit Platform, which Class Members accessed through the “DeFi” application available through Crypto.com, a cryptocurrency exchange based in Singapore that, on information and belief, has customers, employees, and a physical presence in the U.S.

14. Plaintiff will attempt to identify Defendants through discovery served on third parties with whom Defendants interacted. The jurisdiction of incorporation and principal place of business of Coinbit and the Coinbit Platform also are unknown and are the subject of ongoing investigation.

15. This Court has subject matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest, fees, and costs, and Plaintiff, being a resident of Michigan and at least one Class member, is (a) a citizen of a state different from Defendant Nofs, and (b) upon information and belief, Defendants Zhu Shicai, Luo Yanbing, Lin Yin, and Yang Shelin are citizens or subject of a foreign state.

16. This Court has personal jurisdiction over Defendants because the claims asserted herein arise in substantial part from Defendants’ actions and scheme purposefully directed at Plaintiff in Michigan, and because the effects of Defendants’ actions and scheme were felt from within Michigan by Plaintiff as citizen and resident of Michigan.

17. Venue is proper in this Court under 28 U.S. Code § 1391, because a substantial part of the events giving rise to the claims occurred in this District, where the Plaintiff resides and was primarily targeted by the Defendants' scheme.

18. The Plaintiff reserves the right to amend this Complaint to include additional parties as Defendants, upon further investigation and discovery of their identities, roles, and residences.

STATEMENT OF FACTS

19. As detailed below, Defendants followed the "pig butchering" roadmap for cryptocurrency theft. "Pig butchering" victims in the United States have lost billions of dollars and "pig butchering" schemes have been the subject of state and federal government investigation and prosecution.¹

20. In a typical "pig butchering" scheme, scammers promise victims returns and then fabricate evidence of positive performance on fake websites made to look like functioning cryptocurrency trading venues or investment companies to entice victims to "invest" more money. When the victims have been sufficiently "fattened" with false profits, scammers steal the victims' cryptocurrency, and cover their tracks by moving the stolen property through a maze of subsequent transactions.

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.

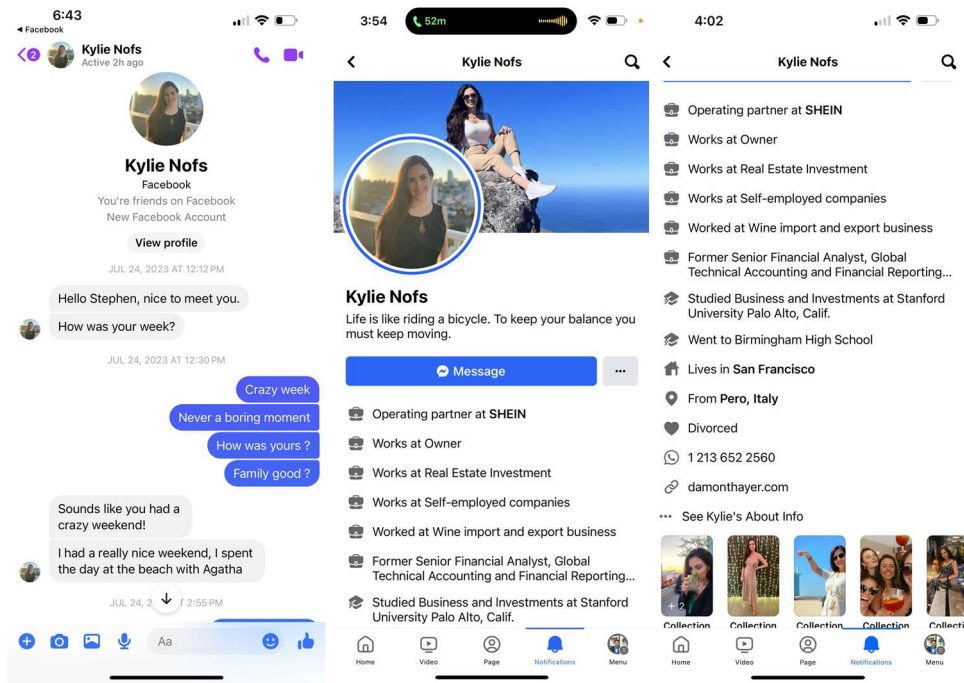
21. In this case, the illegal conversion of Class Members' assets centered around one fake cryptocurrency trading platform: the Coinbit Platform. Defendants used a systematized method to exploit Plaintiff and others similarly situated and steal their cryptocurrency by routing Class Member transactions through Coinbit websites and then to related cryptocurrency wallets controlled by Defendants. Class Members all used "accounts" established through one or more Coinbit websites.

22. On information and belief, the scheme perpetrated by Defendants involved facts common to Class Members, including the following:

- (i) conversations with Class Members to persuade them to invest using the common Coinbit Platform, including communications through social media and messaging apps, the use of fake identities, and false claims related to cryptocurrency investing through the Coinbit Platform;
- (ii) the common use of Coinbit websites and related applications by Class Members;
- (iii) the intentional and unlawful conversion of Class Members' cryptocurrency for Defendants' own use, including transactions conducted at Coinbit websites enabling such conversion;
- (iv) the common use of Defendants' cryptocurrency wallets; and
- (v) significant financial harm to Class Members from the conversion of their assets.

DEFENDANTS LURE PLAINTIFF TO “INVEST” VIA THE COINBIT PLATFORM

23. Nofs first contacted Plaintiff through Facebook on July 24, 2023. Nofs appeared to have common Facebook friends with Plaintiff, as well as relatives in Michigan. Nofs stated that she studied at Stanford University, lived in San Francisco, and had the U.S. telephone number +1-213-652-2560. The following are screenshots taken by Plaintiff:



24. Nofs subsequently communicated with Plaintiff via Telegram. She described investing and trading in cryptocurrency, and persuaded Plaintiff to download the “DeFi Wallet” app through Crypto.com and to use this app to access the Coinbit Platform using the website Coinbitjscz.top.

25. On November 3, 2023, Plaintiff transferred \$14,000 from his account at Akkad Holdings, LLC to account number 40286331681, recipient Lin Yin, at Standard Chartered Bank (Hong Kong) Limited. Defendants informed Plaintiff that these transactions involved transfers of cryptocurrency through his account, with User ID (“UID”) 18177.

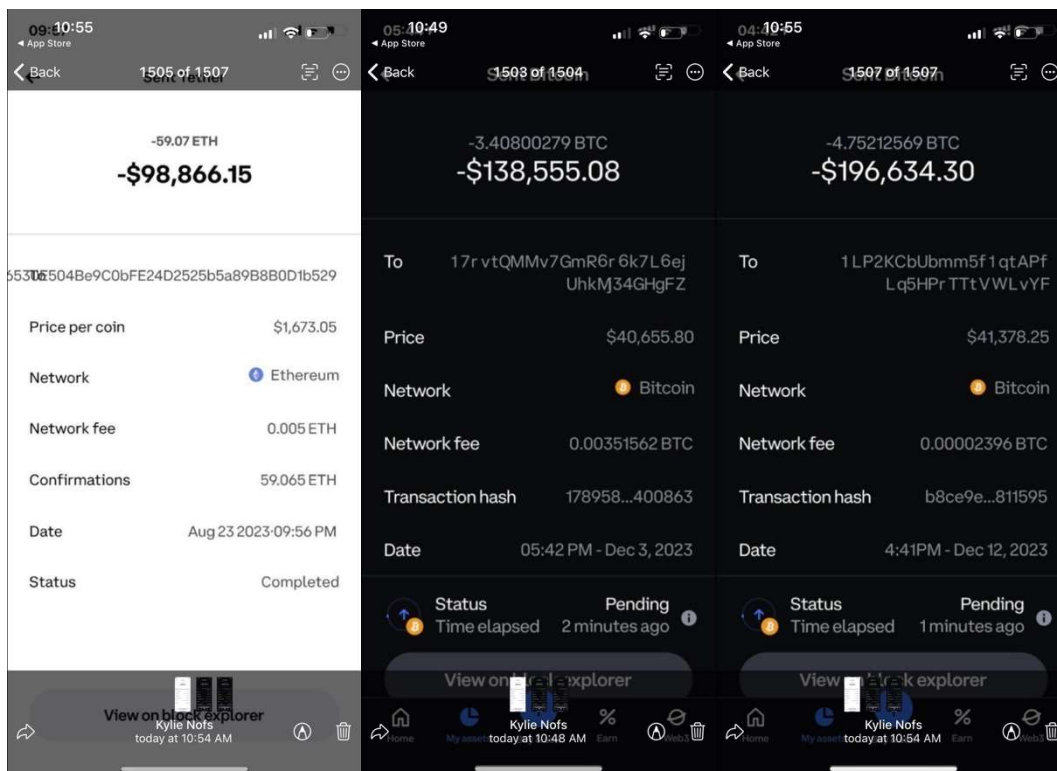
26. Plaintiff thereafter engaged in what Defendants represented were cryptocurrency transactions using the Coinbit Platform. During December 2023, Plaintiff transferred increasing amounts to accounts controlled by Defendants. In aggregate, Plaintiff transferred a total of nearly \$400,000.

27. The details of Plaintiffs’ wires to accounts controlled by Defendants are set forth below. As noted above, Plaintiff’s first wire transfer, for \$14,000 was on November 3, 2023, to an account at the receiving bank Standard Chartered Bank (Hong Kong) Limited. Plaintiff made three additional international wire transfers, during December 2023, all to accounts at the receiving bank Hang Seng Bank Limited. These wires referenced UID 18177, Plaintiff’s purported account on the Coinbit Platform. All of the above wires were sent from Akkad Holdings, LLC.

<u>Date</u>	<u>Amount (US\$)</u>	<u>Recipient Name</u>	<u>Account Number</u>
11/3/23	14,000.00	Lin Yin	40286331681
12/8/23	65,000.00	Yang Zhenlin	273819581888
12/12/23	146,000.00	Zhu Shicai	794648808888
12/22/23	171,621.30	Luo Yanbing	923154785888
Total	396,621.30		

28. On information and belief, based on Inca’s investigation, the funds Plaintiff wired were converted to Bitcoin (“BTC”) and Ethereum (“ETH”), two popular cryptocurrencies, which are traded on separate “blockchains.” According to Inca’s investigation, as described below, Plaintiff’s funds later were sent as follows: Plaintiff’s BTC transactions were sent to BTC address 1KNcYeWbmKJtFXTNDL7PNdohm4s7D6rfn1, and his ETH transactions were sent to ETH address 0xaE99d33B3ddeAf6328B328F82176D1f0939E4188.

29. Nofs represented to Plaintiff that she would lend money to Plaintiff and invest alongside Plaintiff in cryptocurrency transactions using the Coinbit Platform. Nofs sent Plaintiff “confirmations” indicating that she had invested funds.

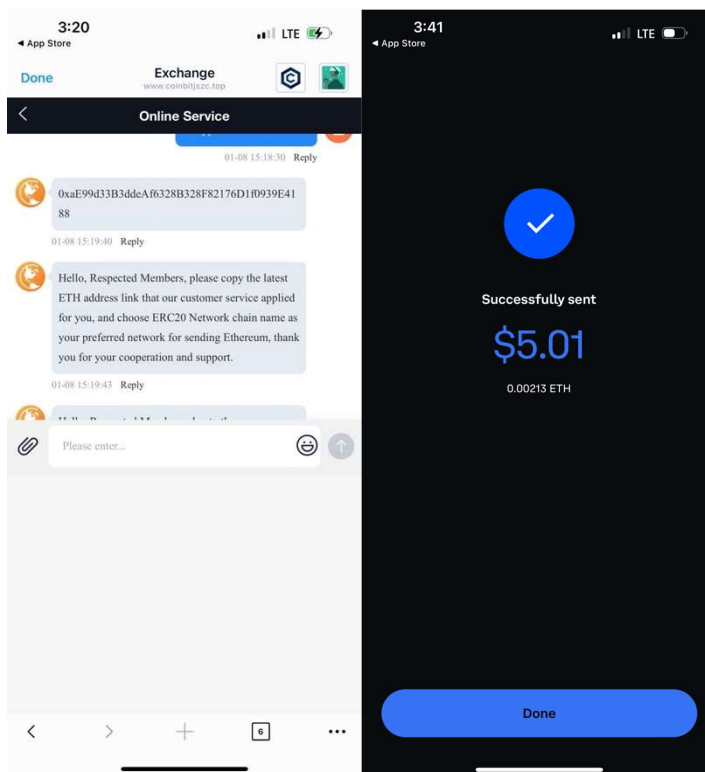



30. After Plaintiff transferred funds to the Coinbit Platform, Defendants represented that he had earned significant profits from cryptocurrency trading, but that he would need to deposit additional funds in order to withdraw his money. For example, Defendants communicated to Plaintiff that his total profit as of December 18, 2023 was more than \$3.4 million, but that he would need to pay a “handling fee” of 5 percent in order to withdraw funds. Plaintiff’s final wire, on December 22, 2023, was sent in response to the request to pay this “handling fee,” as instructed by Defendants.

31. On December 30, 2023, Defendants informed Plaintiff that his account was involved in money laundering, that his “trading account is shown as red red [sic] flag user”, and that he would need to pay an additional 10 percent “risk deposit” to confirm that his account “is a normal account.” Nofs subsequently informed Plaintiff that he would have to pay additional deposits to access his funds, and that she would lend him money to make these payments. Through the Coinbit Platform, Defendants informed Plaintiff on December 30, 2023 and subsequently in early 2024 that this additional required deposit was 421,059.08 of USDT (USDT is a cryptocurrency traded on the ETH blockchain).

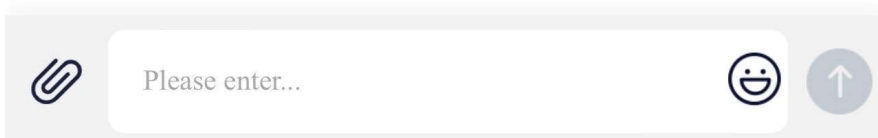
32. On January 8, 2024, Defendants provided Plaintiff with account address information for him to send a test transfer of \$5 from his account at

Coinbase. Plaintiff sent these funds, and Defendants confirmed receipt, as indicated in Plaintiff's January 8, 2024 screenshots.



 Hello, dear user 18177. After inquiry, you need to pay a risk deposit of 421,059.08 USDT. Our company received your ETH worth 4.92 USDT on January 8th today. You also need to pay a risk deposit of 421,054.16 USDT to restore your account. The deadline is before 00:00 on January 20. Extra fees will be incurred if you exceed the deadline. Please be sure to pay all funds within the specified time. Also wish you a happy life!

01-08 16:05:47 Reply



33. Plaintiff did not transfer the additional hundreds of thousands of dollars of funds. Instead, he and Inca began an investigation of Defendants' use of the Coinbit Platform as the common center of a scheme to lure Plaintiff and others to "invest" in cryptocurrency.

THE COINBIT PLATFORM AND NOFS PROVE TO BE FAKE

34. The investigation by Plaintiff and Inca established that Coinbit is a fake cryptocurrency trading platform and Defendant Nofs is a fake identity. The "results" and "statements" provided to Class Members that purported to be from the Coinbit Platform were also false.

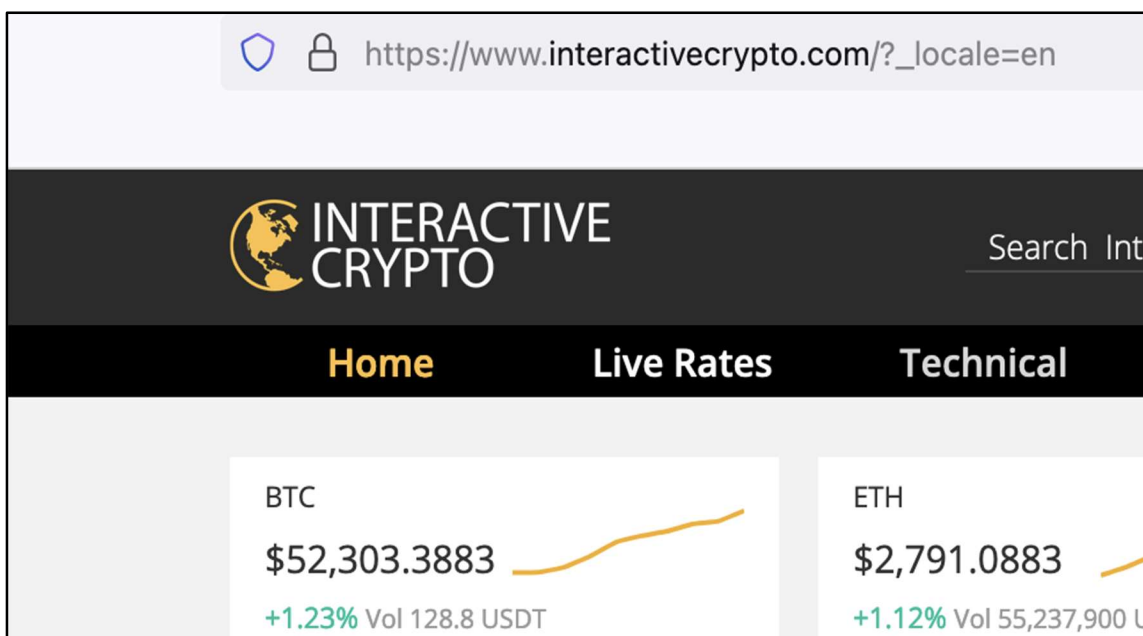
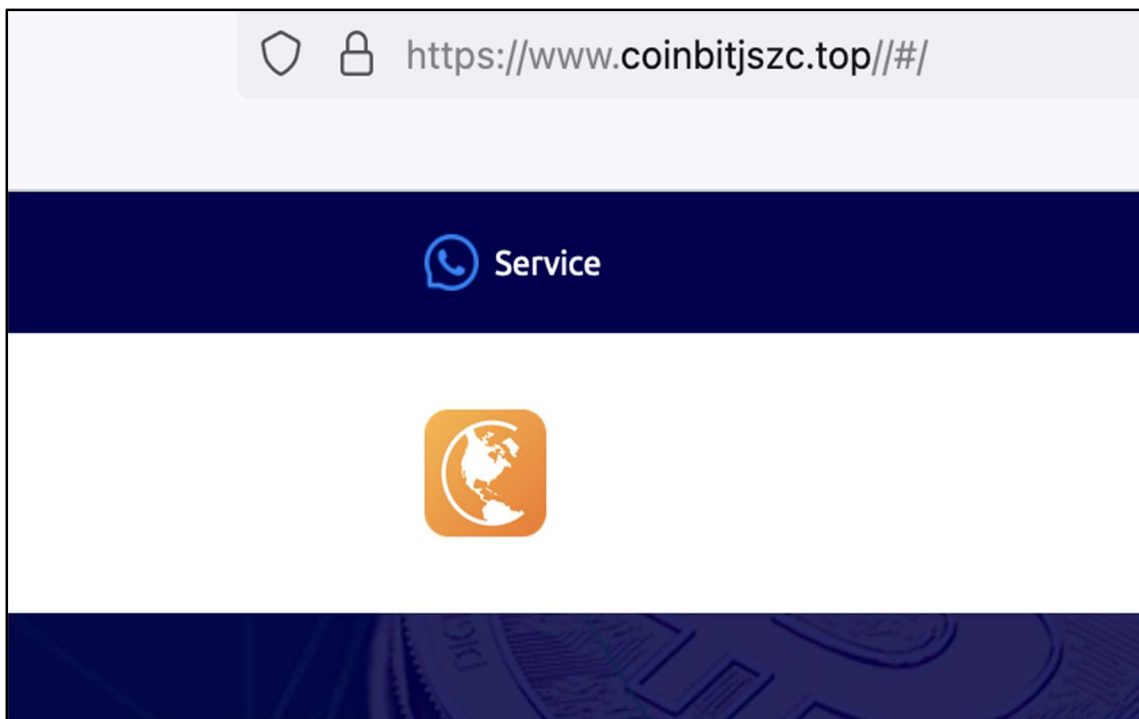
35. Inca's investigation determined that Class Member transactions were part of two "clusters" controlled by Defendants, one on the BTC blockchain and one on the ETH blockchain. A "cluster" refers to a collection of wallet addresses deemed to be controlled by the same entities or users based on a clustering algorithm designed to establish the relationships among various cryptocurrency transactions.

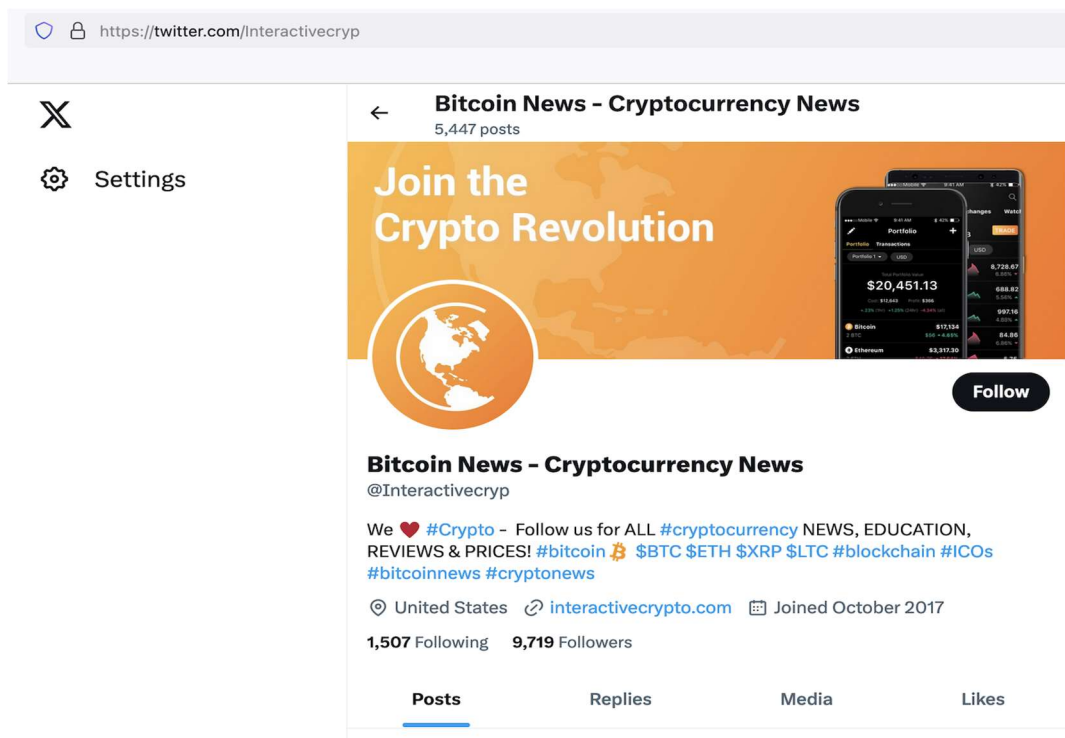
36. With respect to BTC, Inca has determined that Plaintiff's BTC transactions sent to bitcoin address 1KNcYeWbmKJtFXTNDL7PNdohm4s7D6rfn1 were part of cluster address 19PDCExbTskJMk6DC4m7ffsybYNThnCxyE (the "BTC Cluster"), and included 11 wallet addresses controlled by Defendants, set forth in Exhibit A. The BTC Cluster received 96 transactions totaling approximately

35 BTC between January 4, 2024 and February 22, 2024. This amount of BTC was worth approximately \$1.5 million during this time.

37. With respect to ETH, Inca has determined that Plaintiff's ETH transactions sent to ETH address 0xaE99d33B3ddeAf6328B328F82176D1f0939E4188 were part of cluster address 0xf99218cac4d4a1b6bf334d55152937240bafd8a0 (the "ETH Cluster"), which included 176 wallet addresses controlled by Defendants, also set forth in Exhibit A. The ETH Cluster received 935 transactions totaling approximately 6,100 ETH and approximately 1.4 million USDT between November 4, 2023 and January 14, 2024. This amount of ETH and USDT was worth an estimated \$14.8 million during this time.

38. In addition, the investigation established that the Coinbit Platform was fake. The website www.coinbitjszc.top has a logo that is taken from a separate website, interactivecrypto.com. There are no statements or indications that either site is related. Note that the screenshots below, from (1) www.coinbitjszc.top, (2) interactivecrypto.com, and (3) the Twitter/X page of interactivecrypto.com have near-identical logos:







39. The investigation also revealed that Nofs was a fake identity. Reverse image searches of images sent by Nofs to Plaintiff established that the same photos were used widely across various social media platforms, including two different Twitter accounts, two different LinkedIn accounts, and various Russian language dating app accounts. Examples of these photos are set forth below, with captions indicating the sources of the photos.



(Twitter profile “Elena Helen”)



(Photo received from “Nofs”)



La Perla Jeanne
@LaPerlaJeanne

I enjoy my life, I'm a dermatologist, internal medicine, gynecologist, hobbies, golf, skiing, horseback riding, being a romantic woman

📍 Los Angeles 📅 Joined July 2012

9,487 Following 13.3K Followers

Not followed by anyone you're following

⋮ Follow



La Perla Jeanne @LaPerlaJeanne · 20h

God will not favor you because you are weak. #happy



🗨️ 1 🔄 📄 2 📊 86 📌 📤

(Twitter profile “La Perla Jeanne”)



(Photo received from “Nofs”)


A screenshot of Eileen Thomas's XING profile page. The page features the XING logo at the top left. Below it is a large blue header area with a profile picture of Eileen Thomas in a red top. To the right of the profile picture, the name "Eileen Thomas" is displayed with a "Basic" badge, followed by a "See whole profile" button and a three-dot menu icon. Below the name, it says "forscht zu einem Thema." and "Partnerin / Gesellschafterin, Präsident für Operations, Pure Health consultancy". A link "Log in now to view all entries. →" is also present. The "Skills" section is titled "Skills" and includes a link "Log in now to view their full profile. →". Below this, there are several skill tags: "Interimsmanagement", "Kraft", "Mergers & Acquisitions", "Technologie", "Branding", "Werbung", "Produkt", and "Coaching". The "Timeline" section is titled "Timeline" and contains the heading "Professional experience for Eileen Thomas". Below this, it shows "Current 8 years and 6 months, since Sep 2015" and "Präsident für Operations" at "Pure Health consultancy".

(Resume website profile for “Eileen Thomas”)



(Photo received from “Nofs”)

Matchmaker App Encounters Search Sign in Sign up




Bella, 34
From Moscow

Wink Message Add to Favourites

Give her a compliment
Attract more attention to your profile

Interested in: Guy
Age: 40 - 60
Goal: flirt and dating
Languages: Русский
Russian Federation



(Russian Dating Profile)

5:56

LTE



Kylie Nofs is in Tucson, AZ.

5h · 🌐



The most precious thing for man is life, and life is only once for man. A person's life should be spent like this: when he looks back on the past, he will not feel regret for wasting his years by doing nothing, nor will he feel guilty for being despicable and living a mediocre life. The most precious thing for man is life, and life is only once for man. A person's life should be spent like this: when he looks back on the past, he will not feel regret for wasting his years by doing nothing, nor will he feel guilty for being despicable and living a mediocre life. --Ostrovsky



Comment as Stephen Shaya



(Photo on "Nofs" Facebook Page)

DEFENDANTS CONVERT CLASS MEMBERS' ASSETS

40. Inca's investigation also revealed that Defendants used the fake Coinbit Platform to convert Class Members' assets, and then sent those assets through a web of transactions designed to hide their trail. Inca has traced and connected Defendants' transactions, found and followed a trail of transactions, and identified the cryptocurrency wallets that held Class Members' funds. Inca's investigation found that Class Members sent funds from accounts at the following cryptocurrency exchanges: Crypto.com, Coinbase, Kraken, Robinhood, OKX, BitFlyer, Paxos, CashApp, and Binance.

41. Inca's investigation involved two phases, each of which is precise, reliable, and replicable. In phase one, Inca "forward traced" the flow of funds from Plaintiff's investment to other cryptocurrency wallets. Inca traced Plaintiff's transactions forward to one BTC Blockchain wallet and one ETH Blockchain wallet, each of which were involved in transactions originating with Class Member wallets. Inca also traced Plaintiff's transactions to a "Pivot Address," 0x32c6Ffd39e5FdD2e1c0a56307fD62dB45Cddf9f8, on the ETH Blockchain and found that this Pivot Address was common to transactions with other Class Member wallets.

42. In phase two, Inca "reversed traced" the flow of funds to the above addresses and determined that additional addresses matched Plaintiff's flow of funds

as part of a common scheme involving other Class Members. Through this tracing, Inca was able to confirm the identity of wallets involved in cryptocurrency transactions that were part of the common scheme, including the identity of Defendants' wallets that received Class Member funds and accordingly should be frozen. A summary of Inca's analysis is set forth below, separated into the analysis of the Defendants' conversion of assets using (1) the BTC Blockchain, and (2) the ETH Blockchain.

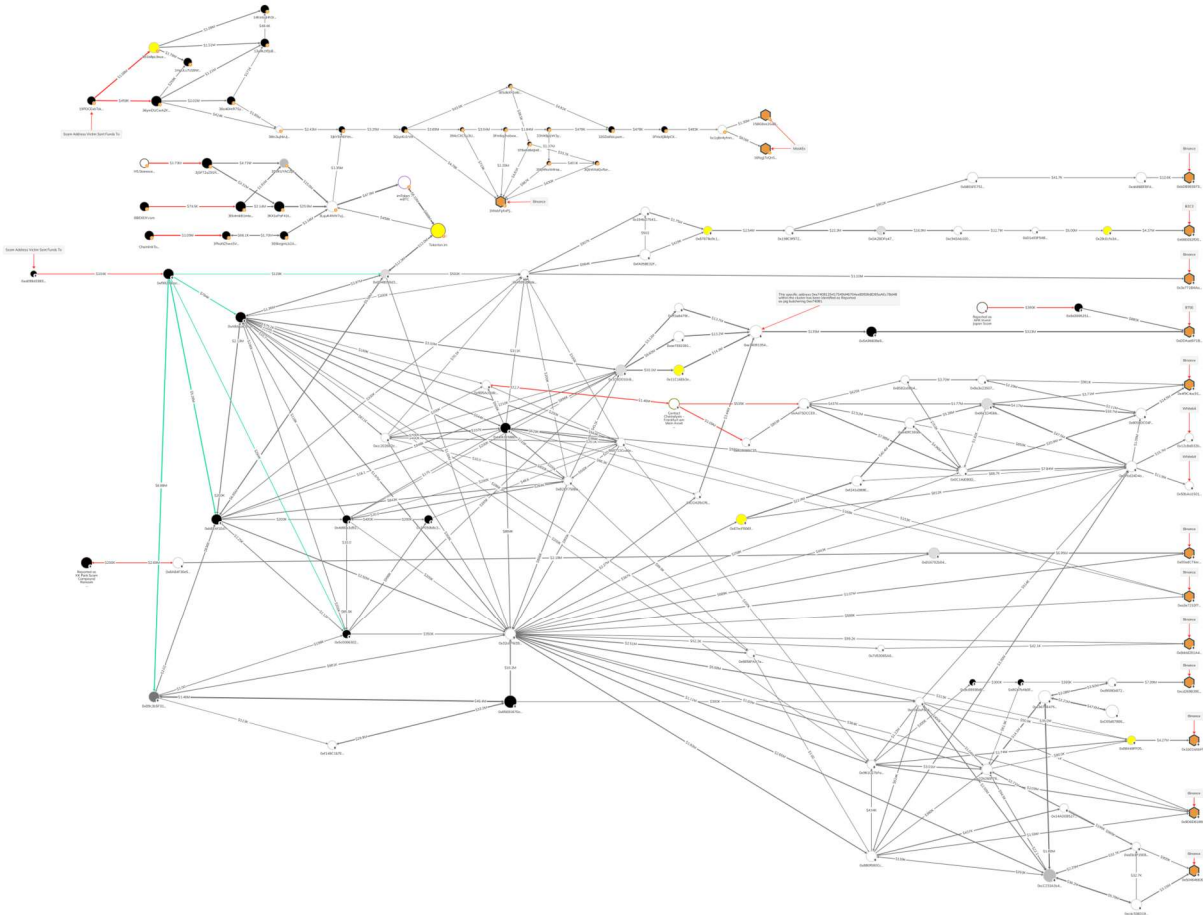
43. First, Plaintiff's BTC was transferred through four levels of transactions, commingled with other Class Member funds along the way, until a portion of Plaintiff's BTC reached BTC address 3QqzKLErVtrdVhXkgJb6hEmb8JdswyJKoA as part of transaction 5d1fbb054c4b3643e16d45e3732150759df2e23839a9e5483b1a6597c55426c9, which amounted to 78.9996 BTC. From this address, Defendants used what is known as a "peel chain" technique² to separate this BTC into smaller amounts at the same exchange address. Approximately 69 BTC of this 78.9996 BTC was deposited to Binance address 1MiobFphxPJu4WiKahfBo2MaZQEvfpnzHp through six transactions. The remaining 9.9 BTC was split and deposited in addresses 15BG9ze2GaB6ZZrHxcsXEWJew9K4bNPE5X and 16fogJ7eQnSkaB7HXshjgWKG5g2XDYuZWk at the exchange MaskEx.

² See <https://www.fraudinvestigation.net/cryptocurrency/tracing/peel-chain>.

44. Portions of Plaintiff's and other Class Member funds were sent to addresses 14KmbiJHh3rS6b1XVrPQFrRCvBZZv9XLSq, 13y9kzXfjsBpo8R81hRTbUCtunra9vDjdk, and 1HqULv7zS9WWmuc3FkPT2pNorjxJL2hCti, from which they were deposited to Binance. A new deposit address was generated for each new deposit to Binance, with amounts typically of a "round" 1 or 2 BTC.

45. According to Inca's investigation, the network of addresses leading to the Binance and MaskEx deposit addresses are associated with entities known among experts in the cryptocurrency community to be "scam entities." This network is set forth in the detailed "tracing graph" below. On the left side of the tracing graph are the wallet addresses that received funds from Plaintiff. Funds then moved from left-to-right, ultimately arriving at the wallet addresses on the right side of the tracing graph. The yellow nodes in the tracing graph represent "scam entities," identified as "WealthFrontExchange.com", "H5.Starexcer.com", "BBEXEIY.com", and "ChainlinkTow.com". These entities have transaction histories that are similar to those in the Coinbit Platform.

“Tracing Graph”



46. According to Inca’s analysis of the ETH Blockchain, Plaintiff’s ETH was transferred to address 0xf99218cac4d4a1b6bf334d55152937240bafd8a0, and then were split. Portions of Plaintiff’s ETH were traced to the Binance deposit addresses 0xbDB99397306D5Ed439A866a1196C2878fFD30af0 and 0x3e771B4Aae63A8Ff4D6e748b217a478C9e3fD0Fc. Additional portions were traced to address 0xDDAad971BE05321FD541372CD710a7f0555972eD of BTSE

and 0x66E092fD00c4E4eb5BD20F5392C1902d738aE7bC of B2C2. According to Inca, the above addresses represent “omnibus” funds held by BTSE and B2C2 exchange users, meaning that they include not only Class Member funds but other funds. Due to a lack of adequate address attribution data, direct input from the exchanges is necessary to determine at which address Class Member funds entered the respective exchanges.

47. Portions of Class Member funds were sent to five different addresses before arriving at ETH address 0x32c6Ffd39e5FdD2e1c0a56307fD62dB45CddF9f8, which Inca determined to be a “pivot address.” According to Inca, this pivot address used decentralized exchanges such as Tokenlon, BKSwap, 1inch, and Uniswap to swap stolen cryptocurrency for other cryptocurrency, most notably USDT. From this pivot address, funds were routed to various exchange deposit addresses. The tracing graph below annotates Binance deposit addresses of interest that have been active in the past month, as well as an additional two addresses presumed to be deposit addresses at Whitebit, a European based exchange registered in Lithuania and the United Kingdom.

48. The bottom line of Inca’s analysis is that Class Members’ funds converted by Defendants were sent to the cryptocurrency wallets listed in Exhibit A. It is these wallets that Plaintiff seeks to freeze.

CLASS ALLEGATIONS

49. This action may be properly maintained as a class action under federal law.

50. The proposed Class is defined as follows: all persons whose property was converted by Defendants using the Coinbit Platform and associated Coinbit websites, including transactions between July 24, 2023 through March 11, 2024, in which they deposited cryptocurrency into wallets controlled by Defendants, and that cryptocurrency ended up in one or more of the wallets set forth in Exhibit A. Excluded from the Class are individual Defendants and their families; corporate Defendants and their officers, directors and affiliates, if any, at all relevant times; Defendants' legal representatives, heirs, successors or assigns; and any entity in which Defendants have or had a controlling interest. Plaintiff reserves the right to amend or modify the Class in connection with a motion for class certification or as the result of discovery.

51. Based on Inca's investigation, the Class Members are so numerous, in the range of 200-250 victims based on current estimates, and are potentially scattered throughout the world, as to make joinder of all members impracticable, if not impossible. Plaintiff will attempt to ascertain Class Member identities through notice to the original owners of assets contained in the accounts listed in Exhibit A to this

Complaint, as well as through discovery, including into account records at relevant institutions.

52. The same “pig butchering” scheme, involving the same Coinbit Platform, was used to victimize all Class Members, so that commonality of the claims predominates. Nearly all factual and legal issues raised in this Complaint are common to each Class Member and will apply uniformly to every Class Member.

53. Plaintiff’s claims are typical of those of other Class Members, arise from the same practice or course of conduct as the claims of other Class Members, and are based on the same legal theory. Defendants used the same platform to perpetrate their scheme and use the same ecosystem of cryptocurrency wallets to hide their tracks. By pursuing his own interests Plaintiff will advance the interest of the absent class members. Plaintiff, like all other Class Members, sustained damages arising from Defendants’ scheme and subsequent transactions to convert stolen property and hide the locations of victims’ cryptocurrency assets. Plaintiff and Class Members were, and are, similarly or identically harmed by the same unlawful, deceptive, unfair, systematic, and pervasive pattern of misconduct. Plaintiff is entitled to the same declaratory, injunctive, and other relief as other Class Members.

54. Plaintiff will fairly and adequately represent the Class and protect the interests of the class. By proving his claim, Plaintiff will prove the Class’s claims and Plaintiff’s interests are thus fully aligned with those of Class Members. There

are no material conflicts between Plaintiff's claims and those of other Class Members, including absent Class Members, that would make class certification inappropriate. Plaintiff has retained qualified counsel with relevant experience and will actively monitor this litigation. Counsel selected to represent the Class will fairly and adequately protect the interest of the Class, have relevant experience in complex and class action litigation, and are competent counsel for class action litigation. Counsel for the Class will vigorously assert the claims of all Class Members.

55. Class certification is warranted because litigating these claims on a class-wide basis is superior to other ways of adjudicating the claims at issue. For each Class Member to pursue their claim individually would require resource-intensive and time-consuming cryptocurrency tracing, analysis, and investigation through a maze of transactions. This action is properly maintained as a class action in that common questions of law and fact exist as to Class Members and predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy, including consideration of: the interests of Class Members in individually controlling the prosecution or defense of separate actions and/or proceedings; the impracticability or inefficiency of prosecuting or defending separate actions and/or proceedings; the extent and nature of any litigation concerning the controversy

already commenced Class Members; the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and the difficulties likely to be encountered in the management of a class action.

56. Among the numerous questions of law and fact common to the Class are: whether Defendants have acted or refused to act on grounds generally applicable to the Plaintiff and the Class; whether Defendants have a pattern, practice and scheme of “pig butchering” and subsequent digital transactions to convert stolen property and hide the locations of victims’ cryptocurrency assets; to what extent Plaintiff and Class Members are entitled to damages; and to what extent Plaintiff and Class Members are entitled to declaratory and injunctive relief. Defendants have consistently acted and refused to act in ways generally applicable to the Class. Thus, final declaratory and injunctive relief with respect to the entire Class is appropriate.

57. Finally, Plaintiff and Class Members have suffered or are at imminent, severe, and unacceptably high risk of suffering, irreparable harm because of Defendants’ ability to move funds at any time, without notice. If Defendants withdraw funds from the wallets set forth in Exhibit A, Plaintiff and Class Members will not be able to recover their funds, and would lose their property forever.

FIRST CAUSE OF ACTION
CONVERSION

58. Plaintiff realleges and incorporates by reference all preceding paragraphs.

59. Defendants intentionally and unlawfully exercised dominion over, and took possession of, the Plaintiff's and other Class Members' property and funds, converting them for their own use.

60. Defendants exercise of dominion over, and possession of, the Plaintiff's and other Class Members' property and funds was inconsistent with Plaintiff's and other Class Members' rights in their property and funds.

61. Plaintiffs property and funds, including the digital assets held in the wallets identified in Exhibit A are unique and identifiable.

62. Defendants' acts of conversion have caused and will continue to cause significant financial harm to the Plaintiff and other Class Members.

SECOND CAUSE OF ACTION
MONEY HAD AND RECEIVED

63. Plaintiff realleges and incorporates by reference all preceding paragraphs.

64. Defendants received Plaintiff's and the Class Members' monies and assets through the scheme alleged above.

65. Defendants have unjustly benefited from the receipt of Plaintiff's and the Class Members' monies stolen through the scheme alleged above.

66. It would be inequitable and unconscionable to permit Defendants to retain Plaintiff's and the Class Members' stolen monies and assets because

Defendants had no right or authority to receive and transfer such monies and assets in furtherance of Defendants' scheme.

67. Defendants' acts have caused and will continue to cause significant financial harm to the Plaintiff and other Class Members.

THIRD CAUSE OF ACTION
FRAUDLUENT MISREPRESENTATION

68. Plaintiff realleges and incorporates by reference all preceding paragraphs.

69. As alleged above, Defendants made material misrepresentations of fact to Plaintiff and the Class Members to solicit phony investments and the transfer of funds and assets from them in furtherance of their "pig butchering" scheme.

70. Defendants' representations concerning the purpose and intended use of Plaintiff's and the Class Members' funds and assets was false, and Defendants knew their representations to Plaintiff and the Class Members were false when they were made.

71. Defendants made these false representations with the intention that Plaintiff and the Class Members would rely upon them and act on them by transferring Plaintiff's and the Class Members' funds and assets.

72. Plaintiff and the Class Members relied and acted upon Defendants false representations by transferring funds and assets to the Defendants.

73. Defendants' false and fraudulent representations have caused and will continue to cause significant financial harm to the Plaintiff and other Class Members.

FOURTH CAUSE OF ACTION
AIDING AND ABETTING/CIVIL CONSPIRACY

74. Plaintiff realleges and incorporates by reference all preceding paragraphs.

75. As alleged above, Defendants combined to act in concert for the unlawful purpose of defrauding Plaintiff and the Class Members and converting their funds and assets in furtherance of their "pig butchering" scheme.

76. Defendants each knowingly acted and participated in furtherance of their unlawful scheme to defraud Plaintiff and the Class Members and to convert their funds and assets.

77. Through affirmative acts alleged above, Defendants aided and abetted one another in participation and furtherance of their "pig butchering" scheme to defraud and convert Plaintiff and the Class Members' funds and assets.

78. Defendants are each jointly and severally liable to Plaintiff and the Class Members for damages suffered as the actual and proximate result of their conspiring and aiding and abetting their fraud and conversion of Plaintiff and the Class Members' funds and assets.

PRAYER FOR RELIEF

Wherefore, Plaintiff, individually and on behalf of all other similarly situated Class Members, respectfully requests that this Court award the following relief and enter judgment, jointly and severally, against Defendants as follows:

- A. Enter a temporary restraining order and freeze the cryptocurrency addresses set forth in Exhibit A;
- B. Preliminarily and permanently enjoin the transfer or dissipation of property and funds held in the cryptocurrency addresses set forth in Exhibit A, along with other digital wallets controlled by Defendants or to which Plaintiff's or Class Members' stolen funds and assets were transferred, until further order of this Court;
- C. Enter an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- D. Enter judgment in favor of Plaintiff and the Class Members on all counts asserted herein;
- E. Award Plaintiff and the Class Members damages in an amount to be determined in excess of Five Million Dollars (\$5,000,000.00);

- F. Impose a constructive trust over, and order the return of, any remaining stolen assets and proceeds derived from the same to Plaintiff and the Class Members;
- G. Award Plaintiff and the Class Members prejudgment interest on all amounts awarded;
- H. Award attorney fees and costs incurred in prosecuting this action; and
- I. Award any other relief this Court finds just and proper.

Respectfully submitted,

ALTIOR LAW, P.C.

s/ Kenneth F. Neuman

Kenneth F. Neuman (P39429)

Matthew D. Smith (P72969)

Attorneys for Plaintiff and Putative Class

401 S. Old Woodward, Suite 460

Birmingham, MI 48009

(248) 594-5252

kneuman@altiorlaw.com

msmith@altiorlaw.com

Dated: March 15, 2024

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

STEPHEN B. SHAYA, on behalf of
Himself and all others similarly situated,

Plaintiff,

v.

KYLIE NOFS, ZHU SHICAI, LUO
YANBING, LIN YIN, YANG ZHENLIN,
and JOHN DOE NOS. 1-25,

Defendants.

Case No.

Hon.

INDEX OF EXHIBITS

Exhibit A: Cryptocurrency Addresses

EXHIBIT A

E HIBIT A

Cr o rre Addre e e or ed e h e

Binance

- 1MiobFphxPJ4WiKahfBo2MaZQEvfpnzHp
- 0x3e771B4Aae63A8Ff4D6e748b217a478C9e3fD0Fc
- 0xbDB99397306D5Ed439A866a1196C2878fFD30af0
- 0x00adC74eca60bc8570fBfbf2Ae0001bdBA9987d1
- 0xa3e7232f754c25dB48E7B1e45935830c987E81B0
- 0xBddd281A443980a4711442a43c846604F0174e9B
- 0x1b014AbF59be85aa1A9abc16766873239637F4d6
- 0x9D6D61B5b466F870E809659B6c0EFE0cc9B06BA4
- 0xcd269B39EA2855242258F90089cc76e6f10504Ab
- 0x4f9C4ac9107A3Aec6b09Db004810Db0A6c65eD44
- 1MJeD1xARua9y9EzusBXeZwmcZftgZ48kn
- 15coUULzLprp1fQvirgRPxJKF4LaTiVMPW
- 15szMaFnEgsfYAKuVKjafPyeV7kdkKx1LV
- 15UmREUGRssw42ptnC4ie7xK1u5nhXrfi7
- 15yoLFniWtKSt8YTdBCR3YdmnX2DNk3SHM
- 16cX4spbtNpGhqzTpBhedop7EBHPS3tgrk
- 16paf23pp94feCF2YVceDDhTk36FHACihT
- 16vzwevyUmE52U4bsPAHM6cCK9sK31Rjo3
- 1725hUxmFvtaLbdC1SEyHD6ocGTC55eexx
- 1DnVrd1hDjXQz83p3Mh4tf3cFqjsGfvmMv
- 1Ec83cfjkwjSQyafJ9oFXTpgpKmgwjvo2d
- 1EesTgoexyPsPMsRTXtc2R2NVPcYYHbGP8
- 1EJQnosfynok4LZRqcMqTCfDdZMS2Xz9Pb
- 1EWgCTg17DaCHGGQf5ZZ3BV52CFKkF4vE9
- 1EYQ9uvqeGmRg41Yea42yigWoAKqftB9ik
- 1F73oPbsSb2sShxQQbbXY6F1vEQWMfYAwY
- 1FfjgorWHSPc4jgK2HKKHXMNCQHGMRWMYZ
- 1MNMBSVK2oLzQ2TsTwQHm4uHwz6JyxQLx
- 1MUQ7KWARGTTtysgxjxgiL1vk7r3RgYDjY
- 1MVSf7yLxBNJTHqRJxkMj3UscSpVsBW8fJ

- 1N1DEHhgk5nVV2smaeu2RPPKJ671EE7CE7d
- 12397TpnaobznX1Tgmbf7LyWtttUj2ts1g
- 125VuPdt4yxZquEqaDPf4Rb6A7btNmMaCp
- 128wXsuiKxQ9DzQ5xmCXztPvUbdogPUW95
- 18ywsJ3ivFG1QxvRjgyAZ18yzAxLSTbhwb
- 1936HAeaa6mE95dqPKkrbMTzBkAZxepJkE
- 19PZrNm7CucpCZdT39bf9p5ac1Cg1Mh5CS
- 19VVjDPkPnbYUBAep7VCL6MoEKzKPYF4pp
- 1mVKxYij5rozc5a1dtFo2oYpdnHEoDhWc
- 1MXwe75LVDGLWVPQ6PDEkJmCSxEZ6BzU7P
- 1N4mszL8HsBpNwiZzxgdS1eMamtYcdEasp
- 1N9o6a29DNdf6C7VnL5gN2esER79QajSa3
- 1NA9BGRQt7rwYHgfZg4tErBzSeBTgJUALS
- 1NrbPSCbcvKBi8nENgB38vRvnPijewJMwX
- 1NSDjjzCcJGkbBedGioCbFuWqyZvtbxDuZ
- 1NshiPK15HwV2kXB5tMu49URpk8FkdWfo7
- 1NsNQ4QKYCLS1xs5fkzLcVmNyXj69w8jq7
- 1NsPUH3pp6u8W1LHkeDRAW1F9z272g9e9F
- 169w1UwZemYjXWDXkFs1TMxd1828chZpgw
- 16FcFMemjpEzFUrN1D5to8yj6e1mDwkuSE
- 1HA3FT21oJDtmE643hoiKfTN7R6mSZF38p
- 1HDZfKDE2MNdrakAEUtxNFVJSHLDTAYoJG
- 1Hiui2uvD6NtpNoSH2NS9JL526DgXh8BHg
- 1HKi6Z5f6D7dhYomM2JDQXk9kefxr46YP7
- 1MquibWP1iU5ea9g4LQVSwNkLhyF7dCC8q
- 1MSWpiNSHs4rTEBoKXZBEc9LvWmDRKZphA
- 14Jc8uZYw4xcgUBpWtZUT2YqaFuc5ZQ79k
- 14nx4kPz3jrru15NwA6bxyjoCfN39B6Hxd
- 19KjbadinBFiFqqfRWJqpGU9cMG2pbYkbz
- 19UZo6BKzWXMj1mufPaCYqMRpBFvEnSGcM
- 1AmK9LabYF6xdUPmawJ4w7kiydUc6xUh1p
- 1ASuucPKYgCs3zVStcCqhWbC9Ngh4tCAsn
- 1FVk38iEdd5KZGYR8DS6cXCdRiLNRmD4U7
- 1G5iM759XrbpGdSugAE64T3NgQ1LFKTqat
- 1GTVTLWNfYGrS5TMMg6jg9bTVV3JsyEjbS

- 1H3VMz3TSTjAWAriL1ne2fnhbmSYvZrdM7
- 14qCkB9mJhw11y9cz5j5Xr9bZwi2bm1sm5
- 14TZhP7mz81ZUQzrs1972j634EDh1GXLWT
- 15MeVNmbBKVGMXNtkfynxSGzn6nRCLtD8p
- 15yBbpfvZXsJ41CooazuFhxJy1C5a43Bp
- 1AHS2No53TWCu3MbWMX8ohBwADu8fa2qGS
- 1Ak7DpAZ3eFhwUQn9HL1PbvdxVDLspqRg
- 1BDfdgoRNxWdpTvzfSePieAwPPofcoPpGT
- 1BLzTUMCZu2tNrttm8sHgXwUXxwCxLLagL
- 1GCneffC1U7UYYckshcLyf4cfhh3tNYS71
- 1GH4CRqr5VQ3fnbAH6QpNT57nmuqqxHXX6
- 1H1nJZzuM5xg48SLddYPMRym6hgRpf3NAU
- 1HHkrX1DRDvbnfYJmmKdD2B2zKQNXwD5GM
- 1LCVhF5anPJS2FASQRUEsVdxq2afPyDTGY
- 1LgbogW6HUP9fJocrAHzZAwME7y4cgY9jo
- 1LtdJGoS5L6ZGzLMcncrLj9g8bqhJFRYZRK
- 1LyhJLGEU7eFpnmki2rfWNWL7xT5V7kPA
- 1Nyyd79kFwpQPoYE5R4dyXzwDS1V4UZMhq
- 1NZ9yWWHXcjAfKoFwKipdB9kJXTris5ZnD
- 1PFXMFbxGq79hR1v7BZa5UrfHAqEKXKon3
- 1PGDztMH8VhdCnw4A2U5oVzjKWWqn3p7PK
- 1D87Vs9PUHR2ijJtVYqmanaiaEj4hWfkjS
- 1DDhqCLVhaoFpGzqWv5RgSvDtKdTiJ4LiU
- 1DdEktRXYmccUbcgsU3eisKYPEsTmhd1gQ
- 1DF8jgMcBmrV8FQG5N7rVZRvgXt48hP2VD
- 15SdZTiwcRc51kiTexNUJv2NXvw4q3QUuU
- 16pRfRQ5xCfbd9YtnwD79dDRLFgJHZhtUC
- 17WJuMFLEKnaJrVBe4fRP1sw8byoUT4X98
- 1Azx8GBjDcQwjQXi6Xc5FH4sPPcudZaqGZ
- 1BRQ6LgAdpajteWJKbHJAmGG3j5t4tULVH
- 1FXXGzqEkJ6NzWQMtaAPw2qhctFoVnVR8Y
- 1JwGFMTraBSEAvXiHo72DaMHsbEs4Mtv9W
- 1JXisr7TWLtcM5Usd3b9DJgksfW1p8RPAD
- 14FekUrC7731cZJT7esWU3k2pdTNRPWFiB
- 14kfqCgPycuaUirxExdJB7HQz2sEaphzVb

- 156Q1uyp9PDA8Mr3y3WjzXydi9EriJUUpwZ
- 15CuHWUhTzXaaUGUQCQsZya3xPKYne3GB4
- 16WkEnmZnymXeCLQx4qsaoGT8YJk2F54tr
- 174PwTD1XrhTHu4fwPHaco1136E92sFoMH
- 1D3FupnMmDkQVeFLYoFkBy4mhB8bpK5jW9
- 1DbpS8YzMFmKHP1q2kkLJjWJbtBVNp6vby
- 1FkTLS92MNLNXjCDECtLWiWC7JvpY9RDBM
- 1FMrc2A5o6jWZTAqzA3bpDMzX8PX2rpUdD
- 1HRczVBeYGxUWUqFoUTrGmbJPe84S5aNWe
- 143tHbjpcX86LrL1RGj2ZBUxocpspgwwmv
- 14hc6zc1ccc9gBUQ5DkucefBTpUiAezhxm
- 19nKmdnCfoce4feqNovS58BQgJJ6WY2ipx
- 19Vh8o2Au5jnSv7a7eccs2s2tep3Noragj
- 1AEQoCh8MpwnawnQ9KJEbmuypcTZKo6WGM
- 1Am9jAyKHEhA5DzXBUsNEvEkbk4peaVU3
- 1FW4P7BQyAr4NBpKo6em4xPHMSxufLryoW
- 1G5DAgZL3TZtkbHsMKHXEHeE6Yv7VCmMcK
- 1GVAdXwrcTQyrYHQVtpjPxcQBQqecyHU3Y
- 1H5zSDEmuVXBReJkZ7HAbKSd2BnzphUaqL
- 14RFvtJvh5W8erSrWeyrQKzC2qkWRQURda
- 14vocoFAARZnsVT2q4sYxnZ3NoQTrr5UZD
- 15mZWe6535nCj5yFg1PaTMmM5HKwTUSeqL
- 15xwAKxfe7chKomG7BLXarU1L3XDRYoMvC
- 1aGeJGokd128aWy8QKaNYKqKMP4yhf7pb
- 1AMHyhnEZyrGCafFuGrMyz3HWC1vuDQfQs
- 1BCfNqLspBXLzoVQoVbCjGk1u39JQmCtTj
- 1BiFQbqF9hpYsoPPQkofB7GVX7pkmGT1w2
- 1GbgkLfJB7fhwM4KhPsNYjv5MuBDyeG6SL
- 1GHG8Ayj88DXjZw782vrsjDbE6aszEkzhF
- 1H2x67nzqLYzNtSKq5ZLMAmn66sGF75uFy
- 1HhqJoMjS99byZ6LsSXXGyftcpfHz7sqWw
- 1LaudpkfDuwRghXNC1ku32rMhbWkrNCqaN
- 1LG9yHdB7xWDTv5gRd5paxz6YDqGkzo98T
- 1LsGct4neXRPnAigRUvXEAhQ7eXhrq6Hkh
- 1LzKstp1uQsxX58ZBFCgFZcdqWDrELCobZ

- 1NYsJU4ZPPmGxDUz5vmSxfMUYfN4cofupP
- 1NZ8baQep6p18hC44bbVn7zfRCLAwCjwYh
- 1PG4NXEbjc99t99UQHjXkpfL18TEj7gmPp
- 1PgDwv7ctR13kHMD6zjgb7mT8f6goD8pXS
- 13nf6Ywr3WP3xa7LXJQzAaxi7c8bbFMovk
- 13yDqzriRosjp7dSYqewhVT666M2sn7P1R
- 143zMHHAzHQSLJvcR3HcSt3QUPCXi6rVpM
- 1D8PfpDcQdULAerV9H4scG9G56yYkA8HaH
- 1D7BJaU7JV4HsrBDvAdBLmUod2oFrYJKtY
- 1Dd7smpd9fL6uQQDf1roDr9LFihVKnxx1V
- 1DEiAn9Xhx9fr9hmY5DGpwK8FGx5tqRZe4
- 15Tk5DQMD73X16k9JGCaLofuftphJUepCg
- 15UH6YS1MfXmZ8y5jY4iMAEF1wbPbgZQWp
- 166yJrfoqFcs5HzD631Mx7vTJMxYJ8kqZg
- 17vYgtbzkSm3NY4EakEoCWsqu9gVXDCi5s
- 1B1KhZMsmVhkl46Vxa9k1QeV8rRQQR58eG
- 1BPiftyW56wnjzv97c5QMAFwEryNGqLHjm
- 1BUVZSUhCVWf2mPRoPw7P2f5xrWbFErEak
- 1JwMx3PUT4j2vuNFBbyTLC41pEE5JeWiKg
- 14hFMNwknSJfi358kejXTGHyZiWu4Ke1Tq
- 14KRgxcivg391N68nqNK9iW4y7iqkpw8X
- 15aKQnkKzfokJy9fnvUxkwyZdXbALisWWv
- 164ABGGG7SpGjbyHuvAZD395DW71W1d9re
- 16WAA7Rno1AynKNo3vKPMW8CHhbsPAHsR
- 1718GhR1vpxHrzoBWTgvcb1zPzMn4Z7D3R
- 1CzzTTVmxJG1UioHL6EnmqeQN6oLiALKi3
- 1DbD8WvUTDZxWCR1PkKvW2sfj92kh2vU7R
- 1Fjr6FMR8hfDn1fLqd8f3vFayFBdVtcgxx
- 1FnyMqtXKUPFLb8ydibvLvq6TYUomawHgd
- 1HkbMbM2K8V6nv929xDib2cLaurRzwmHMK
- 1HSJEevcdx71ZGTrWdnSbq1cww6YWD34BY
- 12EdTtq8ZZeWs2Wdr6bztN7pGDbHJP1ry5
- 12KwfqAr4wCTfPwUCNLbPhLJ69JesJohE
- 12qGNXVXSvsjZtieDupYqvq2thazyJFr5F
- 12wa8tT8mCqebmkkJvmEfeFr1jd46EDtue

- 12zkVgriHrpTdqM7MMR9Fe6qoUSxS7xW6z
- 137fsnp643eUf2XWv4vC82WE2ELDaUPuB7
- 13gAkrPnPMZMDtyTLvZkpkcr9UoJT6WRum
- 13k77pp1z9QhiP7j7bYKwN3fTT6vAPrpCD
- 13RfJ63gLLxAj2YDcknUhu6ucDYTAhdzi1
- 13xWEjxgDjX9k82uJyvZHUFRC7b4opkaQa
- 17Q4Rayqv65sRSkhLRAHMiWxiDK6YzrTS3
- 18asd18XCewna9zBF12GMXVc2Lc4PrzWc
- 19ERtZgKiNMw9noS8qUYaP8AVBJ9fntYM4
- 1CzWyndREVGFgGcHHQUfARbhrtJEBYUkZCB
- 1D9CeuK4mQqfYmZQgMGqnck1br38JMCKcT
- 1DETqftov8aca9a5x3JKRcVXmfxcUAHRzH
- 1DL17qD7JrsgjnZa5FoFSuh7mqMJwwsPHs
- 1DTXKuJFAXWi9Z73fCKprR8FAfpkC6dwqz
- 1E1dFDRw6Kq56EwLvGPQdTe7MQqN1WWE8f
- 1E3wVz4eCBFWU2CHycVZznDGLrSkgcHfwz
- 1E9oWH8pJ8YmtNJvEV1hxBdEk2DFKJ5hfc
- 1EcpeKZquA6Cnt89aAxKqn9bYUMq3RrNoq
- 1EeF81e5Bzo3K6eiKGhXZsHtpMWTnyqhsV
- 1BxoxcVYWcYcHwVTSLBE6Z6FQ6puJNECZu
- 1FLLCsStZFL6eXqUx5PTXfi6tzAqWS6J8o
- 1FKtoEsRhNAaGMZAehsqS5x4SxebNUGEVN
- 1FyLKjSrNHsnHEX9KLFpBKilUsixm2LMon
- 1FYzy9HoqPhHi9VtF9XGNXh9LYU6i9RpH5
- 1GbmVc1dErt7WCruXAQ5uk9E4bKVHYdBQQ
- 1JiDvvnZTfqpw9zJEugPFu39SoqqubGBqj
- 1KbMXBddvgsVo7nuiyfnkUk3zrq6FdWKEd
- 1KcUjPbCEX8L5Mf2LwnBLA3Pg7gZMXBh3V
- 1KgNNfbdSGrEoB7d1UJNULQ3jVcNnA1cYc
- 1Kkd5nbh2g5tff5gsgEYQRVUfuNJxmvcVK
- 1KMUeSMo9ep4FeSZzqJp2PsUSvEAgPLTjv
- 1KNwR5yrxF2qJHDatsDKdxsYKyLvcwoMp3
- 14X6V5WFGsRA5pEgpeb5e8H3bmdBs5vZpm
- 159uD1UYN45HKMp2nt4KTKTKVjQbMoVUbS
- 15hKD15DbCGiHmodgvsYFbLsjRTrdWzZez

- 15kBWZiYC1CD61obR7wyp6od8rWSR6P7nV
- 15n7EfMfwTJu2ANLSbdvtsGTiqGGTz8E2
- 15P7s3YJAhMjGh3u1aZdqk5QNU93wbKWM7
- 1GLnvGR2QcnjSHkNGVJ2Eev85L4mU7jhSA
- 1GMZ5TmNhFbwmXowdJwRH27seuWfa86QJc
- 1GMNLYaHvTrBzWjS5X87bKLBM11ovSvbo9
- 1HcB9Ld2dfpuQfGqpCTxaCRLfeKp31MTto8
- 158ZDCPXopsAo6Ybhawduuq1XPDKR75SqY
- 1DgsexDXnhriRbSZXVHxy1WRDFmBQbDmu2
- 1LBRgXyUKnY5wsj9LMXADTSu87cBD5J2Wk
- 1Ciiza4dVvBEwbdkEQB2MsBxBKBEmsohRo
- 1HgRxi6ZwxNLVjYRUm4aUnPHEygFKN4cQu
- 1Dot7dXt8ynUa16J4Ep5wfae9Pr241TtVk
- 1DrY7D1tjoE4qTqhyb4rqozqeCbx1TyYPz
- 1DuQv2pWkXvpJjUTi492BweiwKYdsjgJji
- 1DTVWgAr5uusEPMgYW6A6vosZ5DK7BrXWe
- 1DW9FNy1RsR2SDgMHAf7yccnYqJVT3iwJX
- 1DZKPqk6awD1ZWmw1aZUXiB1SNpnK46fmU
- 1EehA1pVFkQk3gBTUh5h1a956iGt4NhXnT
- 1ELcug4RecqUsw6DH7tH7pqVbvRDarGwtM
- 1KLvo7yx4LN5gR7oW8eY1EytT5ZWMTQpXR
- 1KwLSR6atAfYsAYBFbBtKeKSN7ZJ6uvQLn
- 12FFq4VURcZjQfvMP2va2t1grjpoQU54kw
- 1MWAeR6FgaacmY4aPqyQkVJZs1WRQxCdgG
- 1MXdDyrt8oTFai7odqQ9m7tyykhNzZjYaq
- 1N2szUzBsgWij2ueReFnJVAzwf9ddFxagA
- 1N6k3bryq35e8sAJdxtpaq5AZ67dsXWHQ9
- 1N6oHECud3uYhXwk3gJE5sqlsAq7Cf5m2P
- 1KeKu2XJEgkn1luraCieVCw5dp3xgf8Y7Si
- 1KfRBQS4h2nkVvofkSsG2qoTVYcpfX6UsH
- 1KeUyFmb7h5AuUXuRuA7Tb2EdGVGtYG47y
- 1KTHBVQyvsu1uaJQFnmTVEUTwfb4GZjLfr
- 1KWZDHBZFUdOk5PkDGFyPR31nPeEvHmwdw
- 16NXY7qC2Xnz9kJLjdfUKD8G3RybzRtJYU
- 175RZA88buvQPjqJo9QhN3KmQQGYAprCkW

- 1H2XQSgYBvpUfPsCuwrR2Fykh6WxLoQkDM
- 1HdmbYAQDnN7pK49cgoqrrsNLWwDZmJoYJ
- 1HhD13ffoMVt5ioeEY2oD2HeDp41Tt1FEf
- 1HrV7njhev1UQTTRTXzqLxDG5MKYbwMYf8
- 1MrTUKT5JdGjmA2gg77X2y6F5KQXhysy6y
- 1MseQjHk8efgKtrHgXPfphLBCkeri7J1aZ
- 14iNmRSpXeBgCdMMxeU1yfScDtk3ci63ip
- 14ogaEECDuuXN2rfNdsUsn1oEd6zHMfjrq
- 19N2tN5mo4hRAs9RAsUDLwsfk7pBxSQJsX
- 19rkHRcQzcMJ7V61Tct8B8uH7FeC9BuaC1
- 1AM52X6yKqgQWGppB6RwMq8o14F3bioUYq
- 1Ask5fc3RPKKtxd8uLofzDwsdVqfBpAq3y
- 1FTkTxCJa9coo46bS6hH5TbjQJ37bY7146
- 1G4pCRUiQsxSv5Xd7P3TbGqCH4JbazDfC9
- 1GVJEJHdpSVWxiR26mCtWafUpEsoJPTYQ9
- 1H4cav6ZGbq2xvJHPB4QdwEG6CvkAekoDc
- 14QAHPAX67KrxLqRJDfvVopCbs55nGdXse
- 14VPsVjVqouBTMQenTfuiT9V9ckMGZRfi1
- 15nEeJfBhrq2WSR2kjBCdVGV3sYPYZ2MmX
- 15vpAKUjjRQ9XVijf2AnMhHDCDtH1AxhP4
- 1AgUTiJpnNEM8VHqjrgAJZ3f85SSU24zU6
- 1ACPACfzbWFrN4fMrZjceoyVxH6xEn2udi
- 1BaeLbXaBJFGSgzBc6xvbCvXkP8aio6epS
- 1BL5QE1zKr22Tq9qEnkgU3tMhR9zCwEB9G
- 1Gdv8LwDfLAXG8xVoTG1i4dfgd1wJnFzNy
- 1GG8KacmHAZuqNDPtA7cxr74g7CpR7Gtjw
- 1H5i1iKfpYhK5x51m4jHhV8nJL3a38t9kk
- 1HDEaXVy2DPByVZ4pcmGeEH9gkQLgcLH7n
- 1LcQ1tutGsbLvBMfgpLuAEa3chPpC5axoH
- 1LFRvHnx48vS5jyM5cBD6HCDtgQRbTvxbj
- 1LTQDFfNJwLcCyahMpFWS3pv1fQmKcbEUo
- 1LyuBQ8s8Zz59vbdCSqDHHkjCjKBePbxBv
- 1NywPrkvfRV7wwDcEXCfNcmmLuNGWFt8tG
- 1NZdKKbPBdokgXVfNB5wAXCXrfo2VNbnsR
- 1PFz8rkprQpnRFs9vboR3cvrZnsLDSYwpx

- 1PgeJviuXMChGPsbB1GzqUo3BYA1R2wHcp
- 1D45EvvmMEYFUEt4K27Z4gBvcj4kLBDstD
- 1DaJCDCWMPxMuNADciKHnrmUE8fZkAwE43
- 1DBnQCCNfeeHkyiXdL253yZB3zWPysohWY
- 1DEq9xyaobP5A7RkihSVR1fJftAyMDG89Q
- 15S577eRkxhuLtPBGgy5DWDFoCba9nyXmH
- 16puhJn5DyFU31ZoykhG4JyVADue7WPzyH
- 17vbwJdLMBTiieyqoo7iENkZmoCwHpvQvd
- 1AzzxvmtCaTewtty1VejmMsJabdj4ruLXM
- 1BrnjhdJNHuZAwKvR5ouL4JgT2qKAfvwSf
- 1FvRHcz5udj8hMiNcq4TPus8MPn3v7s3Yv
- 1JWirwX2uvD5w2VxVk2uP5Nsrz7EPSVpHm
- 1JZ5nd4i6AMR4oNDxJrNiwptwRSXXrmCde
- 14frtNUnULbiqZqtpnapUBVkgjATVqtgeg
- 14Hnf5HwW8RTpxkfaLyH3XqpCYKhDXLP9c
- 157diGyebe2NiQB577xcfT9tvj26WcuLCY
- 15EFyTcNxyFquTtng3Hd558yZs9HtiwyT
- 16WmYHZfhB3zwSpqfpSX1TaDqYUfa6zbcu
- 174GdhvgviWBV8fnw69smJrkbYDkmDsXoy
- 1D14zBoQ6N9RUTecA6UsKfpQNe8xXnAE8c
- 1FL2inyBSyQxZv2nhKBsg3pbXEXn4JqDq9
- 1FrDNEu54dwhyBtwoahxJLcvigT5CbbYzm
- 1FVPV1LYkZt3zuRUTtc7GHB3zRMnLSVyUS
- 1HPZd5ARUsmZXLqzooSAbiT69oka4HVxxh

Whitebit

- 0x12c8aB32bfC3b5da73d987073EB854d212909c85
- 0x50bAa1501fa610d79269c50fBcd52eFE46C80d80

MaskEx

- 15BG9ze2GaB6ZZrHxcsXEWJew9K4bNPE5X
- 16fogJ7eQnSkaB7HXshjgWKG5g2XDYuZWk

BTSE

- 0xDDAad971BE05321FD541372CD710a7f0555972eD (Omnibus Account)

The above BTSE account is an “omnibus account,” meaning that, on information and belief, it contains funds in addition to Defendants’ funds.

B2C2

- 0x66E092fD00c4E4eb5BD20F5392C1902d738aE7bC (Omnibus Account)

The above B2C2 account is an “omnibus account,” meaning that, on information and belief, it contains funds in addition to Defendants’ funds. On information and belief, the following transactions hashtags (“TX Hash”) involved Defendants’ funds.

- 0x2d316ca9d2b52989107a020f14af82408f17c1e5c83cbd9450f5893be8b42c3a (TX Hash)
- 0xc11f4ad41b733373d0d673f6be4c4654b6beaa7529770c4b8d04ec7f62ebb948 (TX Hash)
- 0x5ff986baa5bdb8405dc04d2ccee1ca1ed52bf5ff277115ce79b6d44932555712 (TX Hash)
- 0x2ac884b86d774e2be6fa501452d413124bec1e45b6c872b11ba0fd397c3c1815 (TX Hash)
- 0xbe9b2f25b1b2da44f2c139a62e0aa97d87601187ca1a582ea74f1f0d5f84ee5d (TX Hash)
- 0x990da9517570415f126672ea5c85127ef9ecd6c3ed8f47f569dceaa5004ffbe9 (TX Hash)
- 0xe6a52077edb1dccfa984cdb66bdf3ead032cc7ceed998fbef0c95f99d6ffc03 (TX Hash)
- 0x6f4903a36c9f71f2cbcc30dc9ec9f53dea241507fb2e7e5c9191df0d67feec5a (TX Hash)
- 0x3306915a99fcc9cdc09f2ee067564af35f13474cff2f5a090295fc6bb08b2543 (TX Hash)
- 0x25f14dfd96ca516c02ef69e5594670e27c1df0425fbfe36acd77250870ce651c (TX Hash)

- 0xfa804d4bac7d30c55eafc5fd4a4c4fd344c38079b4682647550d087365140e24 (TX Hash)
- 0xa1ed9a9db5bd3394cd1417d0286f35e65a732c0e43240a8425a2734f9b376cf0 (TX Hash)
- 0xb2d775989fe37bf33c35becfa54d6fc9cebd330eccd376db3af7c25f31744ded (TX Hash)
- 0xb332d28abca541199f60dc330419d42f0bbf60458e7a2b82d74a716dc45dcf45 (TX Hash)
- 0x020b7e77931290d162d00cfe8e80c29ca9492c4d3ae41f61872fa10810f3c0e6 (TX Hash)
- 0x4cfe9b82fc5886718804bf525f429476357156e3540cc9e2c3ad92823a069d69 (TX Hash)
- 0xa91d23889f9d5b86f2b955a83de12516052a0aff004971963de3305bd8d03741 (TX Hash)
- 0xa775eb324e6fdef4b5414523b9a36609a98b75f285d6b7d119b8e18b825ae7d4 (TX Hash)