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

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

Class Plaintiff Andrew Chait ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his undersigned counsel, Mandel Bhandari LLP, alleges as follows:

## INTRODUCTION

1. This case involves the systematic theft of millions in cryptocurrency through a fraudulent scheme known as "pig butchering," which targeted the Plaintiff and numerous similarly situated Class Members.

2. Class Plaintiff Andrew Chait ("Plaintiff" or "Andrew") is a resident of New York who, like other similarly situated Class Members, was deceived by six individuals he encountered online, including those identifying themselves as Wendy Lee ("Wendy"), Eileen Burbridge ("Eileen"), Mary Scott ("Mary"), Verna, Ettie Lee ("Ettie"), Keiko Fujiwara ("Keiko"), and other unknown persons, John Doe Nos. 1-25. These individuals were part of a common scheme to manipulate Class Members into transferring funds to cryptocurrency wallets under Defendants' exclusive control, with the intent to steal these funds.

3. This class action is brought to freeze the cryptocurrency wallets currently holding Class Members' funds, which Defendants unlawfully stole and converted, and to secure the return of these funds to the victim Class Members.

4. "Pig butchering" scams represent a new and dangerous evolution in online fraud, where victims are carefully groomed through a process of trust-building before scammers lure them into fake investment schemes. Using social media and messaging platforms, these scammers initiate contact to establish relationships and gradually build trust before introducing, what seem to be, lucrative investment opportunities. Victims are manipulated into transferring funds, predominantly in cryptocurrency, under the false pretense of a legitimate and profitable opportunities. Scammers fabricate convincing evidence of positive returns and create fake websites that closely mimic authentic cryptocurrency trading platforms, job sites, or investment companies. When victims seek to withdraw their supposed earnings, they are met with demands for additional payments or find that the perpetrators have disappeared, leaving them unable to recover their funds.

5. Pig butchering scams have become increasingly prevalent in recent years, leading to billions of dollars in losses across the United States, and prompting numerous state and federal investigations and prosecutions.[1]

6. Defendants in this action employed tactics typical of "pig butchering" scams, deceiving the Plaintiff and other Class Members into transferring funds under the false pretense of legitimate investments. After gaining control of these assets, Defendants diverted them into their own possession, effectively stealing and converting them. To further obscure their theft, Defendants routed the assets through a series of complex transactions online, ultimately depositing them into cryptocurrency wallets under their sole control, where the assets are currently held. The addresses of these wallets are listed in Appendix A.

7. Defendants in this case used fake identities, contacted Class Members through social media and messaging apps, and gradually gained their trust. Once trust was established, they lured victims into fraudulent cryptocurrency schemes by endorsing phony investment

[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

projects, promoting false trading platforms, and fabricating evidence of returns and profits to reinforce their deception.

8. In Plaintiff Andrew Chait's case, from October 2023 to July 2024, each scammer methodically built a relationship with him, presenting themselves as reliable individuals with legitimate investment opportunities. Wendy and Eileen advanced a high-yield investment scheme by directing Andrew to fraudulent websites that posed as the legitimate crypto wallet "SafePal" and the real cryptocurrency exchange "CoinJar"; Mary enticed him to learn cryptocurrency trading through CoinExchange, a fictitious platform; Verna persuaded him to invest in Vbitex, a fabricated gold trading platform; Ettie guided him to Alpha Homora, a real crypto platform, but then directed him to send funds to wallets not associated with the platform; and Keiko Fujiwara convinced him to use ICMarket, another fraudulent platform claiming to offer profitable crypto trading opportunities.

9. The online platforms promoted by Defendants appeared legitimate but were entirely fictitious, with no actual cryptocurrency investments or trades taking place. The funds that Plaintiff and other similarly situated Class Members believed they were investing or trading were, in reality, funneled directly into cryptocurrency wallets controlled by Defendants.

10. After making their initial deposits and seeing apparent profits, some victims were allowed to withdraw small amounts from the fake platforms—a tactic designed to maintain the illusion of legitimacy and encourage further investment. However, when they attempted to withdraw larger sums, they were met with demands for additional deposits, purportedly to cover various fees before the withdrawal could be processed. Regardless of whether these fees were paid, new demands continually arose under the same pretext, ultimately preventing Plaintiff and similarly situated Class Members from withdrawing most, if not all, of their funds.

11. As detailed below, from October 2023 to July 2024, Defendants manipulated Plaintiff Andrew Chait into believing he was making legitimate investments through various fraudulent platforms. Through persistent and calculated communication across multiple messaging platforms, Defendants pressured Andrew into transferring substantial sums into what

he believed were secure investments. Like other victims, Andrew ultimately found himself unable to access the vast majority of his funds. In the aggregate, Andrew transferred a total of approximately $337,000.

12. After deceiving Andrew and other victims into transferring their money, Defendants routed it through a maze of complex online transactions designed to obscure their trail and hinder recovery, effectively stealing and converting the funds. Despite Defendants' efforts to conceal their actions, an investigation by Plaintiff's counsel and experts revealed that these transactions were part of a common scheme to convert Class Member funds.

13. Based on Plaintiff's investigation to date, Defendants' conversion schemes, spanning from January 1, 2023, through at least July 12, 2024, included approximately 2,000 Class Member victims.

14. Following extensive investigation, Plaintiff has identified the cryptocurrency wallets currently holding the stolen assets. This action seeks to recover the misappropriated funds of the Class from these wallets, the addresses of which are listed in Appendix A. Plaintiff requests that the Court issue an order to freeze those wallets.

## PARTIES, JURISDICTION, AND VENUE

15. Plaintiff resides at 420 East 54th Street, Apt. 2407 New York, NY 10022. Plaintiff is the Vice President and CFO of Ralph M. Chait Galleries, the oldest U.S. gallery specializing in fine antique Chinese porcelain and art, based in Manhattan.

16. Defendant Wendy Lee ("Wendy") is an individual who identified herself by that name and claimed to be located in Toronto, Canada. Plaintiff is uncertain of her real name or location, as her true identity and residence remain unknown and are subject to ongoing investigation.

17. Defendant Eileen Burbridge ("Eileen") is an individual who identified herself by that name and claimed to be located in London, England. Plaintiff is uncertain of her real name or location, as her true identity and residence remain unknown and are subject to ongoing investigation.

18. Defendant Mary Scott ("Mary") is an individual who identified herself by that name, claimed to be located in Miami, Florida, and contacted Plaintiff using the phone number 658-441-7432. Plaintiff is uncertain of her real name or location, as her true identity and residence remain unknown and are subject to ongoing investigation.

19. Defendant Verna is an individual who identified herself by that name and claimed to be located in Los Angeles, California. Plaintiff is uncertain of her real name or location, as her true identity and residence remain unknown and are subject to ongoing investigation.

20. Defendant Ettie Lee ("Ettie") is an individual who identified herself by that name, claimed to be located in Jacksonville, Florida, and contacted Plaintiff using the phone number 813-585-9689. Plaintiff is uncertain of her real name or location, as her true identity and residence remain unknown and are subject to ongoing investigation.

21. Defendant Keiko Fujiwara ("Keiko") is an individual who identified herself by that name, claimed to be located in Manhattan, New York, and contacted Plaintiff using the phone number 332-733-6997. Plaintiff is uncertain of her real name or location, as her true identity and residence remain unknown and are subject to ongoing investigation.

22. Defendants John Doe 1-25 are individuals of unknown citizenship who perpetrated the alleged wrongdoing herein. Plaintiff will seek to identify Defendants John Doe 1-25 through discovery.

23. Jurisdiction is proper in New York County because Defendants engaged in activities that directly harmed Plaintiff, a New York resident, and received funds from accounts, including but not limited to, Plaintiff's account at Coinbase, which maintains a presence in New York. Coinbase has employees in New York and maintains a mailing address for its consumer assistance division at 1350 Ave of the Americas, Fl 2 # 1143, New York, NY 10019.[2]

24. This Court also has the right to hear a class action pursuant to CPLR § 901 because (1) the class is so numerous that joinder of all members, whether otherwise required or permitted,

[2] See https://www.coinbase.com/legal/licenses (last accessed Aug. 11, 2024).

is impracticable; (2) there are questions of law or fact common to the class which predominate over any questions affecting only individual members; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; (4) the representative parties will fairly and adequately protect the interests of the class; and (5) a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

25. Venue is proper in New York County under CPLR § 503(a).

## STATEMENT OF FACTS

26. As detailed below, Defendants in this case made false promises about the legitimacy of various investment opportunities and trading platforms. Class Members were enticed to invest through these platforms with the expectation of legitimacy, relying on Defendants' fabricated evidence of returns. However, when Class Members sought to withdraw their funds, Defendants blocked their attempts, ensuring that the funds remained under their control instead.

### PLAINTIFF IS "PIG BUTCHERED" BY DEFENDANTS

#### A. Wendy Lee and Eileen Burbridge

27. In October 2023, Wendy Lee initiated communications with Andrew Chait via Facebook Messenger, and their conversation soon transitioned to WhatsApp and Telegram. Wendy began discussing cryptocurrency investments, claiming that her aunt, Eileen Burbridge, a reputable venture capitalist based in London, had introduced her to a highly profitable opportunity, a "blockchain certified project."

28. On October 26, 2023, Wendy claimed the blockchain certified project generated stable, daily profits. She explained that the project required a minimum investment of $5,200 and suggested that Andrew start with an investment between $5,000 and $10,000. On October 27, 2023, Andrew followed Wendy's instructions and downloaded what he believed to be the SafePal wallet to facilitate his investment. However, Wendy directed him to a fraudulent version of the SafePal platform at https://www.safepaladain.com/, misleading Andrew into believing he was securely transferring his funds to a legitimate crypto platform.

29. On November 16, 2023, following Wendy's instructions, Andrew made his first deposit of $5,225 via a wire transfer from his bank account into what he believed was his SafePal wallet. Thereafter, Wendy directed him to https://www.zerionin.com/, a website controlled by Defendants that purported to show that these funds had arrived in his account by November 19, 2023, and where he was shown fabricated profits. This further convinced Andrew of the legitimacy of the investment.

30. On November 23, 2023, Wendy proposed that Andrew speak directly to her aunt Eileen via the LINE messenger app. Andrew began chatting with Eileen on November 28, 2023. Eileen educated Andrew about "blockchain certification," describing it as a stable, high-return investment. On November 30, 2024, Eileen advised liquidating his traditional investments and moving the capital to SafePal, enticing him with the potential to earn $72,000 per month.

**LINE**
[11/30/2023]
15:08 Eileen Burbidge
Depending on your capital situation, first of all, I'm not sure what kind of income your stocks can bring you. But for blockchain certification, one suggestion I give you is that you can liquidate all the funds in your stock account. Then increase the funds in your blockchain certification account to 200k. When the funds in your blockchain certified account reach 200k, your daily income can increase to 1.2%, and your monthly income can reach 36%. This also means you can earn at least $2,400 per day and $72,000 per month. Depending on your financial situation, I think this plan will be more suitable for you and will also allow you to get a better return on investment.

31. Encouraged by these discussions and his apparent profits, Andrew made additional wire transfers—$25,025 on December 6, 2023, and $25,025 on December 11, 2023— to his Bitstamp account (a legitimate cryptocurrency exchange). From his Bitstamp account, Andrew converted the funds to Etherium and transferred 11 Etherium (approx. $25,715 at the time) and 11.4 Etherium (approx. $24,818 at the time) on December 7 and 11, respectively, to what he believed to be his SafePal account but what was really a crypto wallet controlled by Defendants. Wendy and Eileen continued to reinforce the security and profitability of the project and showed Andrew manufactured but convincing profits.

32. Eileen then recommended setting up a short-term trading account on "CoinJar" as part of the same "blockchain certification" project, claiming it would enhance the returns even further. Eileen provided detailed instructions and directed Andrew to the website

https://www.coinjarin.com/wap/, which, similar to Wendy's SafePal link, led to a fraudulent site. On December 21, 2024, convinced by Eileen, Andrew initiated a wire transfer in the amount of $5,025, to what he thought was his CoinJar account but was really a bank account controlled by Defendants.

33. Eileen then advised Andrew to remit an additional $100,000 to CoinJar to maximize his returns. On January 12, 2024, she provided detailed instructions for completing the wire transfer, directing him to avoid mentioning cryptocurrency to the bank and to state that the funds were for an online purchase of fitness equipment.

LINE
[2024.01.12]
12:59 Eileen Burbidge
Yes, just write down the remittance information and then go to the bank to complete the remittance.
We have done this before, and there are some things you need to know when remitting money.

13:01 Eileen Burbidge
When remitting money, if they ask you about the purpose of the funds. Then you can tell them that you purchased some sports and fitness equipment online, and the funds were used to pay for the equipment. According to this reply, the remittance can be completed smoothly.
Remember, do not mention to them that you are sending money for investment or to invest in cryptocurrencies. These must not be mentioned and must be paid attention to.

13:02 Eileen Burbidge
When you fill out the remittance information form, do not fill in anything in the remarks column. If you must fill in something, you can fill in your name.
Do not fill in investment and do not fill in cryptocurrency. These are also things you need to pay attention to.

13:04 Eileen Burbidge
Do you remember everything I said?

13:09 Eileen Burbidge
Do you keep what I said in mind?

13:10 Eileen Burbidge
What are you doing?

13:18 Eileen Burbidge
When making wire transfers, please pay attention to the precautions I told you.

14:02 Eileen Burbidge
After completing the wire transfer, remember to send me your remittance information sheet and let me check it for you.

34. Following Eileen's instructions, on January 12, 2024, Andrew initiated a wire transfer in the amount of $100,000 to what he believed to be his CoinJar account, but what was really a bank account controlled by Defendants. By January 16, 2024, his CoinJar account

balance on the fraudulent CoinJar user interface appeared to have grown to approximately $540,000. These profits were fabricated by Defendants.

35. In February 2024, when Andrew attempted to withdraw his funds, he was informed that a commission of $71,306.13 was required before he could access his money. Despite his inability to pay this amount, the fee was insisted upon, and he was threatened with a significant penalty for non-compliance.

36. On February 6, 2024, after the payment deadline passed, Andrew was notified that $270,000 had been deducted from his CoinJar account as a penalty for non-payment. Even after this deduction, he was still unable to access any remaining funds.

37. Wendy and Eileen deceived Andrew by sending him links to platforms that appeared to be SafePal and CoinJar but were actually fake platforms under their control. With the ability to manipulate these counterfeit websites, they fabricated false profits, making his investments seem legitimate and encouraging him to make more deposits. In reality, his money was being funneled into cryptocurrency wallets controlled by the Defendants. Ultimately, Andrew lost approximately $160,300 to the scheme.

**B. Mary Scott**

38. On December 9, 2023, Mary Scott first contacted Andrew Chait through Facebook, establishing a friendly rapport. By December 16, 2023, their conversation had moved to WhatsApp, where Mary continued to engage in personal discussions about mutual interests, including cryptocurrency.

39. Andrew confided in Mary about the recent challenges he faced with cryptocurrency investments involving Wendy from Toronto and her aunt. Mary responded by casting doubt on the legitimacy of those investments and sharing an anecdote about a friend's uncle who had been scammed. By subtly acknowledging the reality of such frauds, she positioned herself as trustworthy and genuinely vigilant about avoiding similar scams. This trust later enabled Mary to convince Andrew to invest more on a platform she endorsed, leading him to believe the outcome would be different—only for his funds to be stolen once again.

WhatsApp
[12/16/23, 5:04:01 PM] Mary Scott: So when you just mentioned that your friend in Toronto keeps asking to switch to another social media, it makes me wonder, I know if you have met in person, I think this is suspicious!

[12/16/23, 5:04:30 PM] Mary Scott: Nice, when was this photo taken?

[12/16/23, 5:10:55 PM] Andrew Chait: This picture was taken at the end of August the night before we took my son to college. It was at the White Horse Tavern in Newport, RI. I very much appreciate your concern / suspicion. I have not met Wendy in person yet, only through Facebook. It is a valid concern and I have to admit I had initial concerns and I have been careful but hopefully I have not been taken.

[12/16/23, 5:35:03 PM] Mary Scott: I have to share something that happened around me with you. The uncle of a close friend of mine from Tampa met someone on Facebook who is almost similar to what you just shared—someone who frequently changes social media platforms. This person asked my friend's uncle to switch from Facebook to Telegram, WhatsApp, Line, and, surprisingly, even to Google Chat. In less than two months, almost all of my friend's uncle's information was stolen. Additionally, he lost nearly $1.6 million in USDT from his cryptocurrency exchange account. They seem to exploit various social media platforms to obtain information, and the current technology is indeed frightening.

When my friend asked him, they had never met in person, not even through video calls. So, when I asked you earlier if you've met your friend, and you said you haven't, that's when I decided to share this with you. I hope your friend is not dealing with a fake person from Nigeria <This message was edited>

[12/16/23, 7:45:33 PM] Andrew Chait: Thank you from the bottom of my heart - there are many similarities and to be honest this has caused some alarm bells to go off. Yes there is crypto involved and I have an account on Safepal where the crypto is stored. I have been encouraged to cash out my brokerage accounts and store all the funds in Safepal. I have cashed out some but nowhere near all and am monitoring the Safepal wallet daily.

40. Mary emphasized the importance of using a "regulated platform" to "ensure the safety" of their funds, highlighting the supposed security of the trading platform she recommended, "CoinExchange" (also described as "CoinSafety").

WhatsApp
[12/20/23, 5:30:03 PM]
Mary Scott:
The crypto platform I invested in is regulated so the money I inject is very saf

So the money I inject is very safe. So the crypto platform I invested in is regulated

[12/20/23, 5:33:13 PM]
Mary Scott:
There are so many scams out there nowadays! ! Have to be careful

When investing, you must choose a public trading platform and trade on a regulated trading platform. Only in this way can we ensure the safety of our own funds!

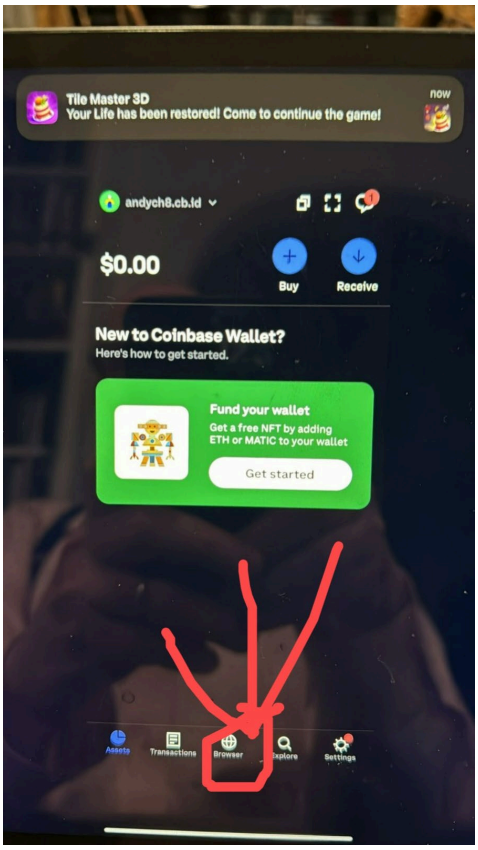
41. On January 3, 2024, Andrew followed Mary's instructions to access CoinExchange. She instructed him to first set up an account using Coinbase Wallet, a well-known application for managing and purchasing cryptocurrency. Once the account was created, Mary directed him to use the browser function within the Coinbase Wallet app— designed to access decentralized applications (dApps) and cryptocurrency-related sites— to visit a specific link for CoinExchange (https://www.coinexchangein.com/wap). Throughout the entire process, Mary

stayed in constant contact, sending him photos she annotated with red circles and arrows to guide Andrew through each step.

**WhatsApp**

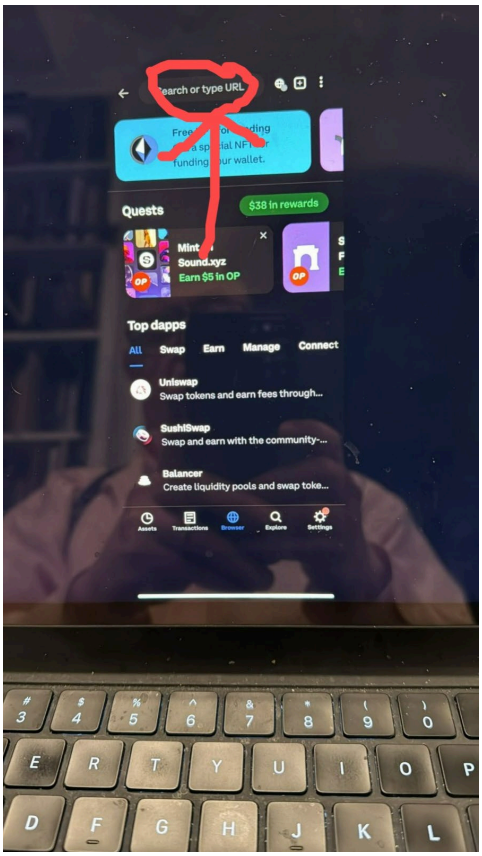
[1/3/24,7:52:50 PM] Mary Scott: You open your app store. Download a Coinbase wallet

[1/3/24, 8:00:54 PM] Mary Scott:




<attached: 00001529-PHOTO-2024-01-03-20-00-55.jpg>

[1/3/24, 8:02:51 PM] Mary Scott:

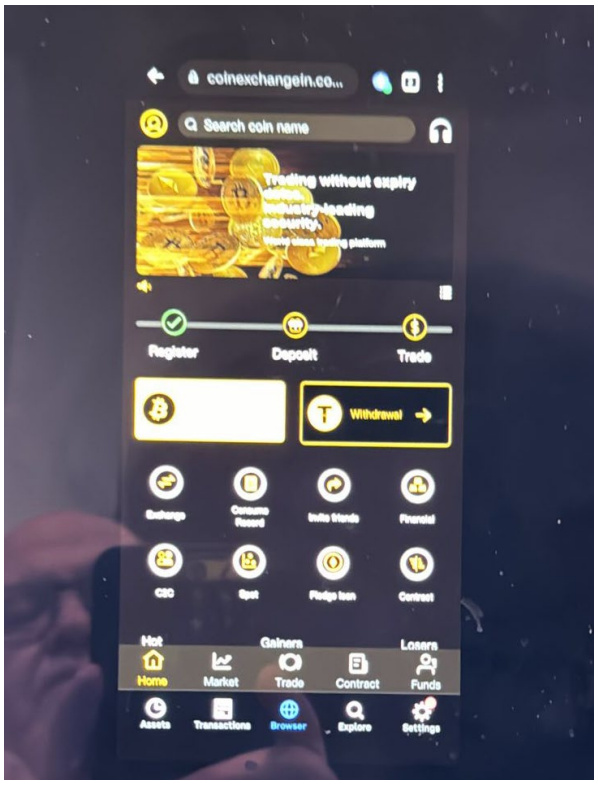



<attached: 00001532-PHOTO-2024-01-03-20-02-52.jpg>

[1/3/24, 8:03:48 PM] Mary Scott: https://www.coinexchangein.com/wap/

[1/3/24, 8:04:14 PM] Mary Scott: Copy the link. Enter linkhttps://www.coinexchangein.com/wap/

[1/3/24, 8:16:31 PM] Andrew Chait:




<attached: 00001555-PHOTO-2024-01-03-20-16-31.jpg>

[1/3/24, 8:17:23 PM] Mary Scott: yes!

[1/3/24, 8:17:25 PM] Mary Scott: bingo！！

42. Andrew entered the link Mary provided into the Coinbase Wallet browser, following her instructions to use the bar at the top. A convincing trading interface then appeared, as shown above. By directing Andrew to access the site through the Coinbase Wallet browser, Mary added an air of legitimacy to the scheme, making the trading platform appear more secure and authentic. This strategy was particularly effective because she had previously emphasized the importance of using regulated platforms.

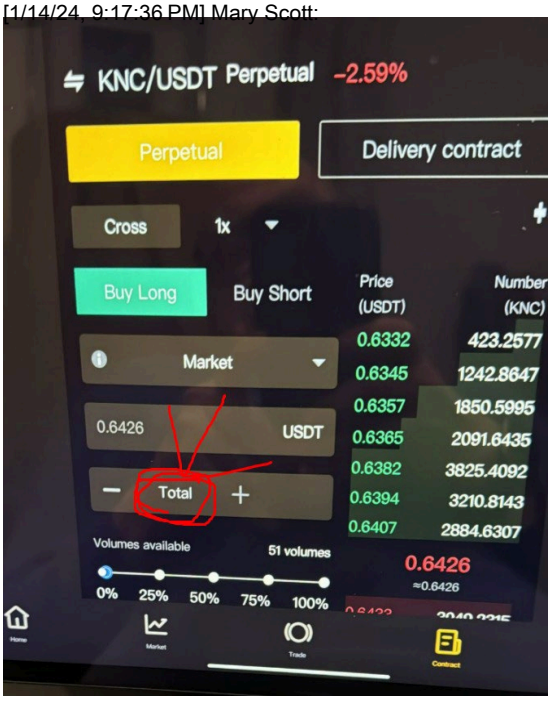
43. On January 11, 2024, Andrew deposited $5,025 and $45,025 into CoinExchange and executed his first trade under Mary's guidance. Between January 11 and February 4, 2024, he completed nine trades, all while following her explicit instructions. As shown in the WhatsApp messages and screenshot photos below, Mary provided real-time guidance, further gaining his trust as he saw what seemed to be impressive results and profits.

**WhatsApp**

[1/14/24, 9:13:07 PM] Mary Scott: Start trading. Let's buy it in advance too! !

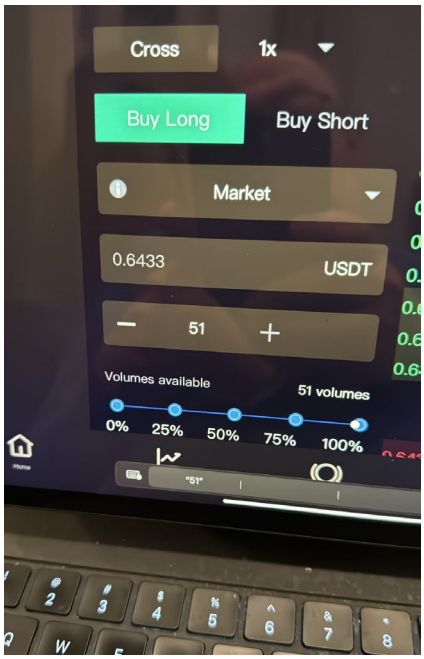
[1/14/24, 9:13:13 PM] Mary Scott: here we go!!!

[1/14/24, 9:17:36 PM] Mary Scott:




<attached: 00003380-PHOTO-2024-01-14-21-17-37.jpg>

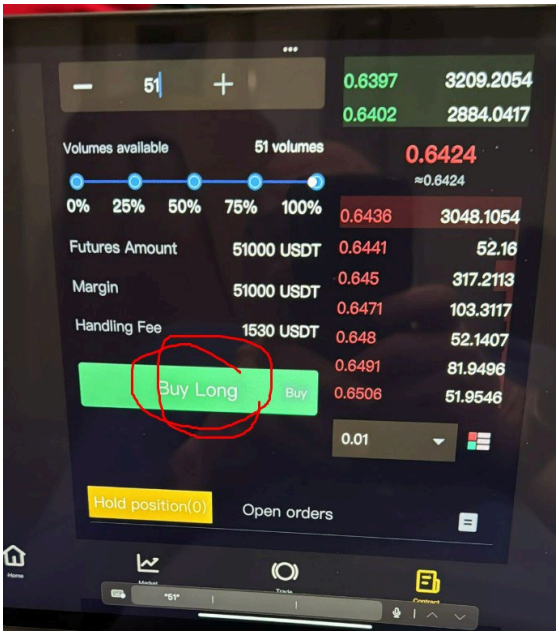
1/14/24, 9:17:46 PM]




Mary Scott: Enter quantity 51

<attached: 00003382-PHOTO-2024-01-14-21-18-09.jpg>

[1/14/24, 9:19:12 PM] Andrew Chait: Am I buying long yet




[1/14/24, 9:19:13 PM] Mary Scott:

<attached: 00003386-PHOTO-2024-01-14-21-19-14.jpg>

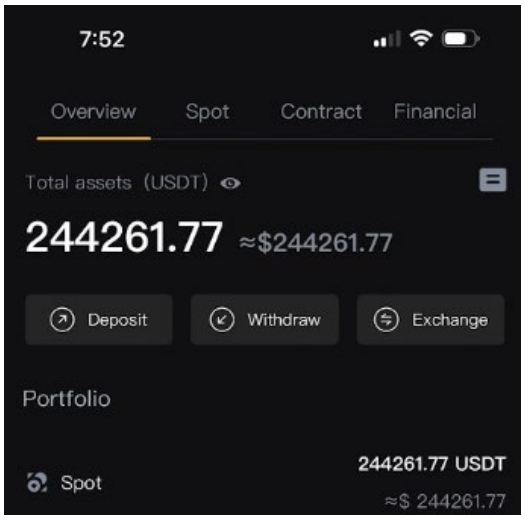
[1/14/24, 9:19:14 PM] Mary Scott: buy long

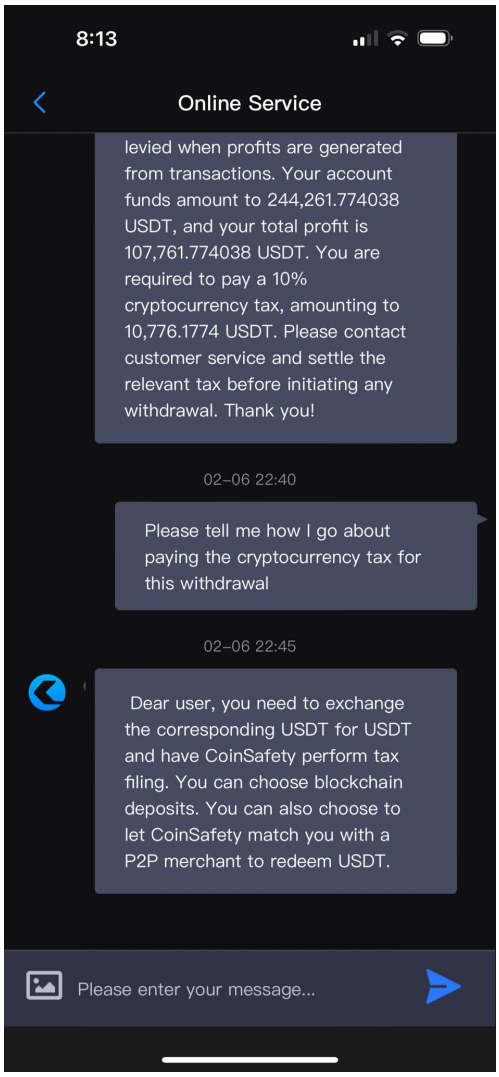
[1/14/24, 9:19:49 PM] Mary Scott: ok ! !

[1/14/24, 9:20:08 PM] Mary Scott: Tonight our ROE is 16%

44. Encouraged by initial "profits" and his ability to withdraw small amounts, Andrew deposited larger sums. Mary persuaded him to deposit an additional $50,025 on January 25, 2024, and another $50,015 on January 26, 2024. These funds were transferred from TD Bank to Chong Hing Bank Ltd. in Hong Kong to an account named Jinpeng Trading Co. Ltd. By the end of January 2024, Andrew had deposited a total of $150,090.

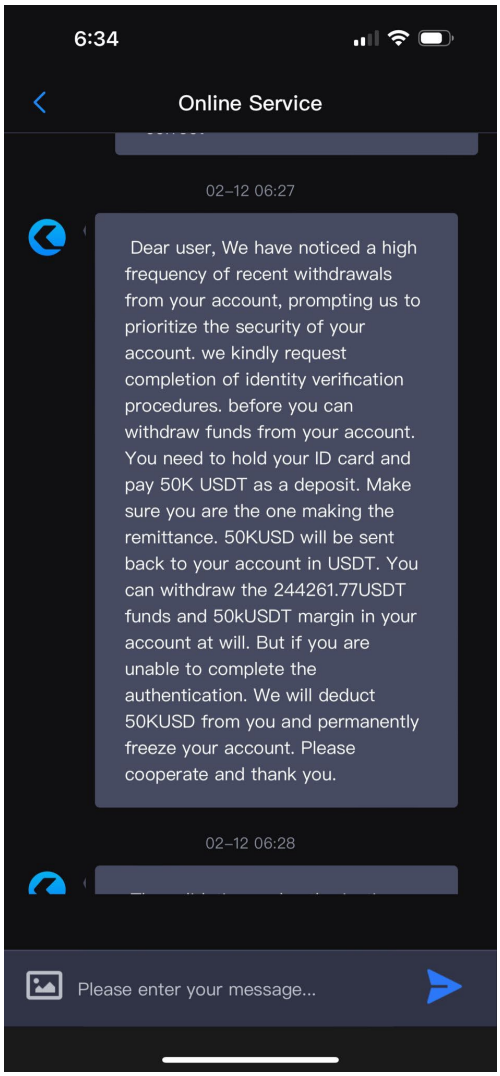
45. On February 6, 2024, Andrew's CoinExchange account showed a balance of $244,261.77 USDT, which he believed was the result of his profitable trades. However, when he attempted to withdraw funds on this date, CoinExchange Customer Support confirmed the balance but demanded a 10% "cryptocurrency tax" of $10,776.18 USDT before releasing the



funds. As a result, on February 8, 2024, Andrew made a final deposit of $10,801.18 to cover the supposed tax.

46. On February 12, 2024, Andrew again attempted to withdraw his funds and close his account, but he faced another unexpected fee demand. CoinExchange Customer Support




informed him that he could not access funds until he completed an identity verification procedure and paid an additional $50,000.

47. When Andrew informed Mary of the situation, she claimed that such demands were standard for large withdrawals and urged him to pay an additional $50,000, further revealing her intent to extract more funds.

**WhatsApp**
[2/15/24, 9:00:21 AM] Andrew Chait: They are asking for a $50,000 verification deposit to withdraw my funds.

[2/15/24, 9:01:14 AM] Mary Scott: This is standard for large withdrawals. It ensures security and compliance.

[2/28/24, 8:00:21 AM] Andrew Chait: They froze my account. I can't access my funds.

48. Unable to make this large payment, Andrew's account was purportedly frozen, leaving him unable to access any funds. Despite appearing to be legitimate, the CoinExchange platform was a complete fabrication, and no real cryptocurrency trades occurred. Unbeknownst to Andrew, his funds were being transferred to Defendants.

49. Defendants continued to contact Andrew to convince him to provide additional funds. On May 7, 2024, following instructions of Defendant Mary Scott, Andrew transferred 5 USDC (approximately $5 at the time) from his Coinbase account to what Defendant claimed was Andrew's CoinExchange account but was really a crypto wallet controlled by Defendants. Andrew similarly transferred an additional 0.00334134 ETH (approximately $10 at the time) to the same crypto wallet on May 9.

50. In total, Defendant Mary Scott stole approximately $160,906.18 from Andrew using the fraudulent CoinExchange scheme.

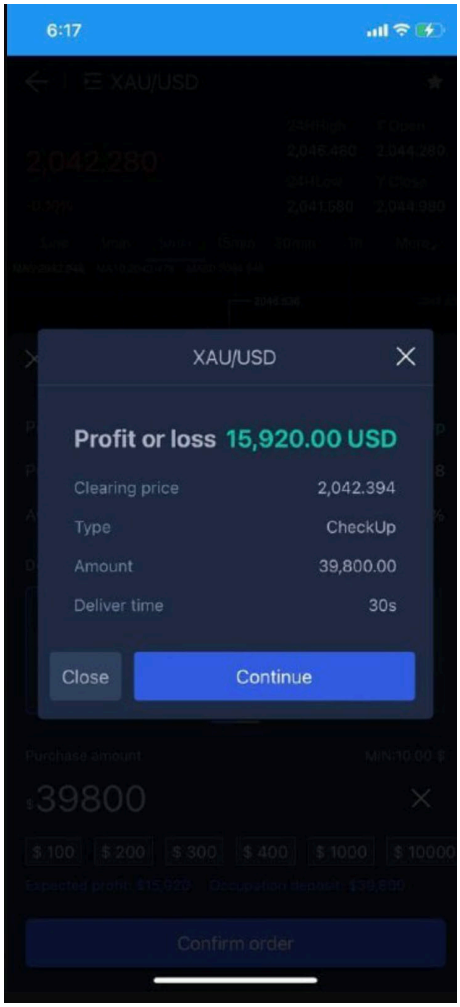
**C. Verna**

51. On December 27, 2023, an individual who identified herself as "Verna" contacted Andrew through an "accidental" text message from the phone number 270-392-1684, which quickly led to communication via Telegram. Verna introduced herself as a jewelry designer and gold options trader based in Los Angeles.

52. Over the following weeks, Verna gradually built a rapport with Andrew and shared her success in gold trading. On January 7, 2024, she sent him a screenshot, claiming to have made a $15,920 profit in just 30 seconds on a $39,800 investment, boasting a 40% return.

**Telegram**
**[January 7, 2024]**
13:51
Verna
I'm relaxing at home today, watching some financial news, reading books, watching my gold options trading market, and doing some trading in the afternoon.
21:31
Verna

21: 32
I just finished my gold options trade and I made myself a profit of $15,920 in 30 seconds using $39,800. My return is 40% and I'm happy to share my profits and happiness with you.




21:34
Andrew Chait
Congratulations that is very impressive

53. On January 21, 2024, Verna, encouraging Andrew to make his first investment, claimed she had grown an initial $200,000 investment to $1.7 million.

**Telegram**
**[January 21, 2024]**
14:42
Verna
I first entered the gold options market, and my first investment was US$200,000. When I entered the market, it happened to be a bull market. After making money, I continued to add funds, so the income in the first year was very considerable. At its peak, I held $1.7 million.

14:44
The investment principal depends on your own financial situation. For your first investment, I recommend you try from US$1,000-10,000. When you see stable profits, you can choose to increase your principal, depending on your own ideas. Of course, the more money you invest, the more you will gain.

54. On January 25, 2024, Verna introduced Andrew to the platform where she claimed to have made sizeable profits, "Vbitex." She provided him with a link to the site. When Andrew experienced difficulties accessing the platform, Verna sent him an alternative mobile web link on January 26, 2024, to ensure he could gain access.

**Telegram**
**[25 January 2024]**
11:58
Verna
Ok dear, I don't know if it supports your region, let's try downloading it first.
11:58
https://www.vbitcoinex.com/p/app
11:58
Dear, you need to copy the link and open it in your browser
11:59
After opening it, send me a screenshot and I will teach you how to download the Gold Options Exchange.
---
**Telegram**
**[26 January 2024]**
15:39
Verna
Dear, that may be a region restriction.
15:39
Then you should use the mobile web version first.
15:40
https://www.vbitcoinex.com/p/m

55. Through persistent communication and reassurances about the legitimacy of the site, Verna convinced Andrew to begin investing. On March 4, 2024, Andrew made his first deposit of $491.64, transferring funds from his MetaMask wallet to Vbitex with Verna's step-by-step assistance.

56. On March 5, 2024, Verna coached Andrew through his first trade, which appeared to yield profits. Andrew continued to trade under Verna's guidance, seeing perceived profits including $82 on March 5th, $240 on March 7th, and $338 on March 12th.

57. Encouraged by these early successes, and with Verna consistently urging him to invest more, Andrew made two additional deposits to Vbitex. He transferred $500 on March 28, 2024, and another $500 on April 4, 2024, each time with Verna's direct assistance.

58. Under Verna's guidance, Andrew's perceived profits steadily increased, with his account balance reaching $4,372 by April 17, 2024, and $5,446 by April 18, 2024. The real-time direction Verna provided for executing trades—including one on May 1, 2024, where profits seemed to be $1,080—is illustrated in their Telegram conversation below.

**Telegram**
**[1 May 2024]**
22:36
Verna
Click[buy up]
Select[30S]
Enter[3200 USD]
Confirm Order
22:38
? ?
22:38
Finished?

22:38
Andrew Chait
Profit 1280 I mistresses key and had to recenter
22:39
The tv is off now and I'm totally focused

22:39
Verna
Click[buy up]
Select[30S]
Enter[1000 USD]
Confirm Order

22:40
Andrew Chait
Done
22:40
Profit 400

22:40
Verna
Click[buy up]
Select[30S]
Enter[1500 USD]

Confirm Order

22:41
Andrew Chait
Profit 600

22:41
Verna
Today's node is over

22:43
Andrew Chait
Thank you honey today profit 1480 - paid my car repair bill 😊

59. Despite the apparent success reflected by his growing account balance, Andrew's attempts to withdraw funds from Vbitex on June 9, 2024, were unsuccessful. He lost access to the platform and was unable to recover his funds, resulting in a total loss of $1,458.98.

60. Unbeknownst to Andrew, Vbitex was a completely fabricated platform, and no real trades occurred. The funds Andrew believed he was using to execute real profit-generating trades were, in fact, being transferred directly to cryptocurrency wallets controlled by the Defendants.

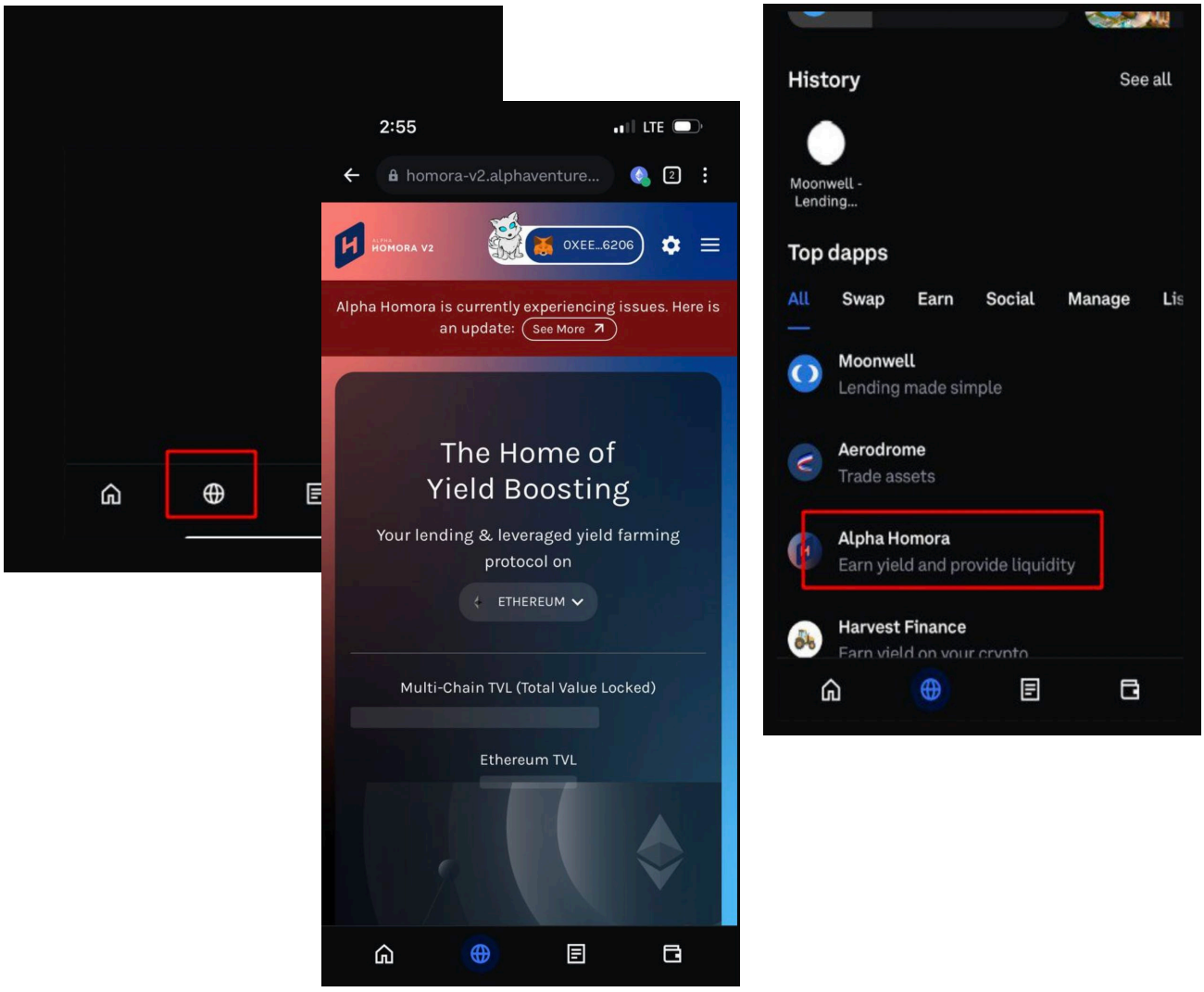
**D. Ettie Lee**

61. On April 25, 2024, Ettie Lee initiated contact with Andrew through Facebook Messenger. She revealed personal details about her life, sharing that she had two sons and a daughter, and expressed genuine concern for Andrew's well-being. She established a connection and built a sense of friendship with Andrew. They transitioned their conversations to Telegram.

62. In May 2024, Ettie claimed success in crypto trading on a platform called Alpha Homora. Andrew, cautious due to previous difficulties withdrawing cryptocurrency, emphasized his preference for trusted platforms like Robinhood or Coinbase. Aware of his concerns, Ettie reassured him that they would not go through other platforms and that he only needed to "transfer the funds to the Coinbase Wallet." However, this was a misrepresentation, as she later directed him to use the Coinbase Wallet's browser to access the Alpha Homora website—a platform entirely unrelated to Coinbase.

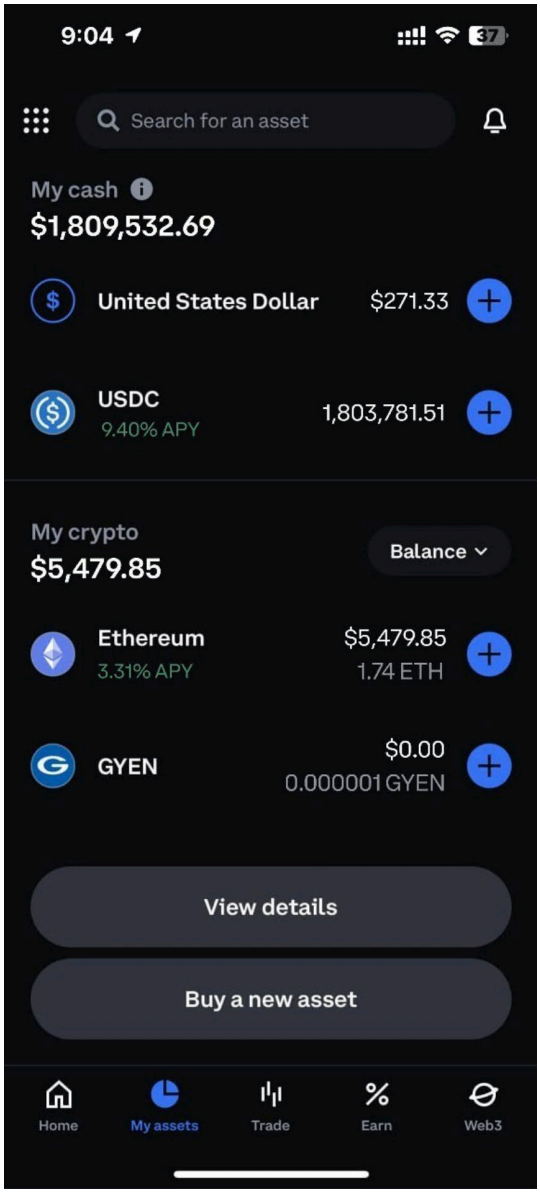
**Telegram**
**[1 May 2024]**
22:41
Ettie Lee
Coinbase is of course regulated. We don't need to go through other platforms. Just transfer the funds to the Coinbase wallet.
---
**Telegram**
**[2 May 2024]**
14:47
Ettie Lee
I can feel it: you still want to encounter good investments to help you realize the funds you once lost, am I right?
14:48
You should enjoy your lunch. We should forget the bad past and remember more of the good times: like your dad and good friends like you.
14:50
If you trust me, I can teach you to buy some mainstream coins, but the income may not be as high as you think
14:51
Andrew Chait
That is correct which is why if I do anything I am only doing it on Robinhood or Coinbase platform. Need to fid a better platform for the gold options than the one I am o as I a suspicious with every successful trade showing 40% profit. Because I am suspicious I have very little there. My criteria is I want platforms where I can get my funds out with no surprises.

63. As shown in the screenshot photos below, Andrew accessed the legitimate Alpha Homora platform through the Coinbase Wallet application with Ettie's directions.

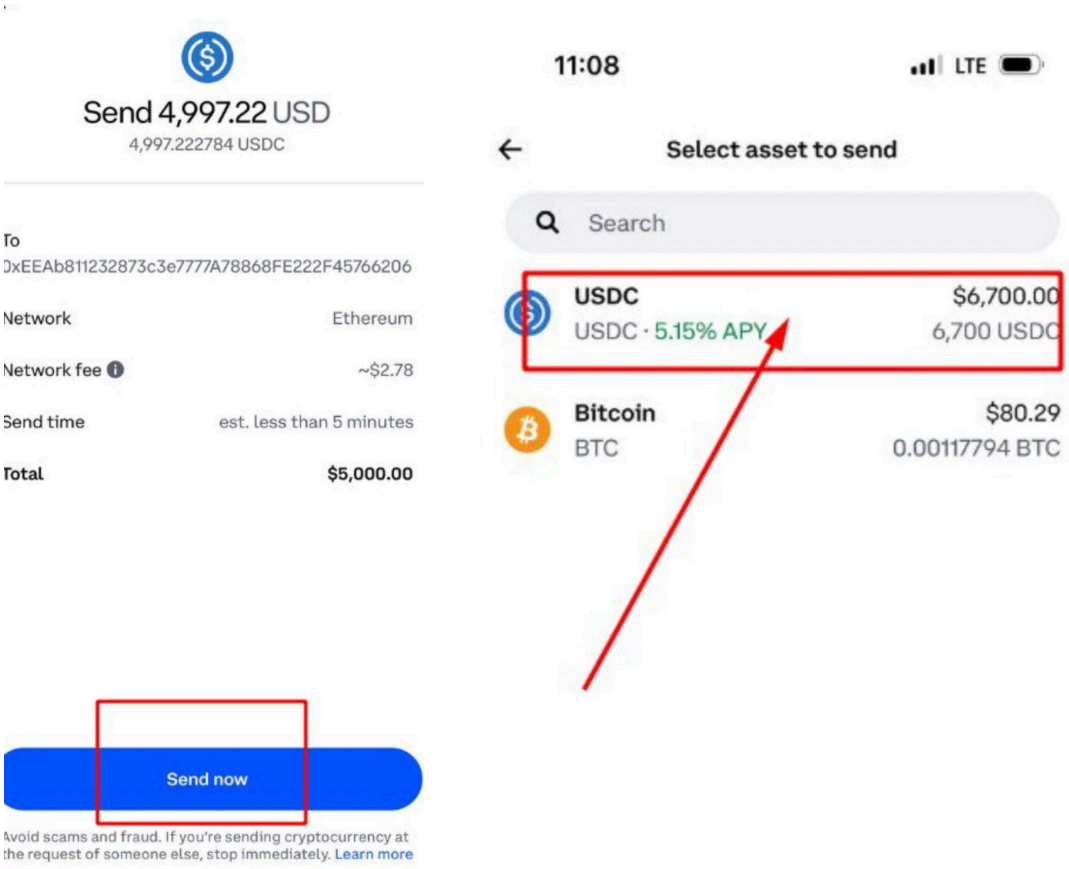


64. On May 5, 2024, Ettie shared a screenshot of her supposed $1.8 million account balance, claiming that simply keeping funds in Coinbase Wallet would generate earnings.

**Telegram**
**[5 May 2024]**
21:05
Ettie Lee
This is my most recent deposit, and some earnings. If you deposit one day earlier, you can get one more day of earnings. As long as I keep it in the coinbase wallet, it can generate earnings.



65. Between May 23, 2024, and May 29, 2024, Andrew transferred over $12,500 in USDC and Ethereum to under Ettie's guidance to what he beelived to be Alpha Homora, but which was really a crypto wallet controlled by Defendants. Throughout the process, Andrew sent Ettie photos and screenshots at various stages. As exemplified below, she annotated these images with red squares and arrows, indicating precisely where to click and what steps to take next, before




sending them back to Andrew to ensure the transfers were completed correctly.

66. On July 8, 2024, when Andrew attempted to withdraw his funds, Ettie informed him that an additional $12,000 was required to cover margin requirements and fees before his funds could be released. Despite Andrew communicating his inability to deposit more funds, Ettie persisted, emphasizing that the payment was necessary to unlock his investments. She warned that his funds could be forfeited or used by others if he did not comply.

67. By August 2024, Ettie ceased responding to his requests for assistance. Ultimately, Andrew was left unable to withdraw any of his funds, with losses exceeding $12,500.

**E. Keiko Fujiwara**

68. On April 30, 2024, Keiko Fujiwara initiated contact with Andrew Chait through Facebook Messenger, establishing a connection by discussing their shared interest in art. The conversation quickly transitioned to WhatsApp, where Keiko continued to build rapport with Andrew by complimenting his personality and sharing personal anecdotes.

69. Keiko introduced Andrew to ICMarket, portraying it as a profitable trading platform she had been using successfully. Keiko described how she had seen substantial returns, encouraging Andrew to explore the platform as a means of growing his investments.

70. On June 3, 2024, Keiko guided Andrew through the process of setting up an ICMarket account and transferring $1,074.69 via Coinbase. She continued to emphasize the potential profits, leading Andrew to make an additional transfer of $1,220.56 on June 20, 2024.

71. On July 5, 2024, Keiko emphasized the importance of capitalizing on trading opportunities, suggesting that Andrew sell his stocks to increase his available funds for trading in options on ICMarket. Keiko presented herself as a knowledgeable and trustworthy mentor and continued to guide him through seemingly profitable trades. She urged Andrew to increase his account balance to reach “VIP1” status, promising greater trading benefits.

72. On July 9, 2024, Keiko guided Andrew through a series of trades on ICMarket, resulting in a reported $632 profit. Afterward, a screenshot photo showed that his account balance was $4,107.86.

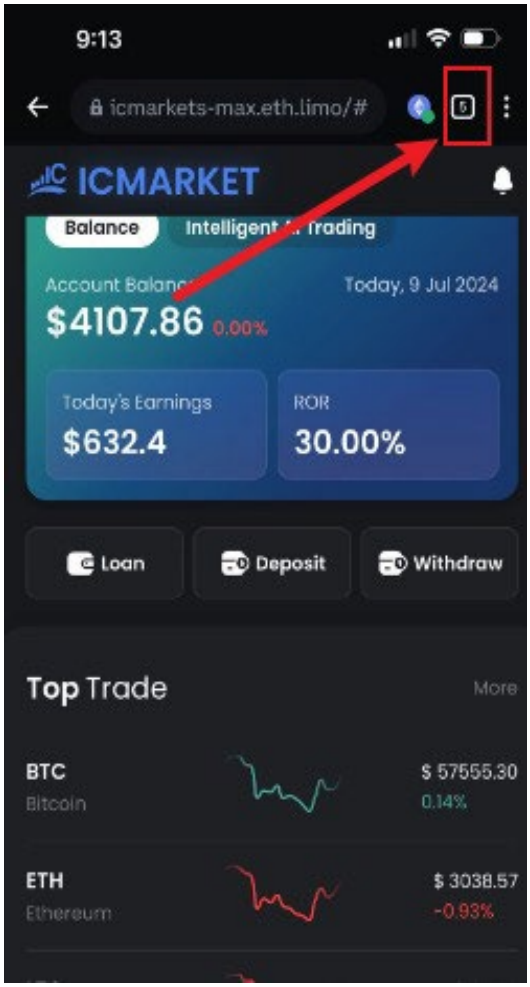
**WhatsApp**
[7/9/24, 9:14:23 PM] Andrew Chait: Another successful night

[7/9/24, 9:14:32 PM] princess 🏓 keiko Fujiwara: Tonight's profit is $632! Very well done!

[7/9/24, 9:14:54 PM] Andrew Chait: You made it possible

[7/9/24, 9:15:59 PM] princess 🏓 keiko Fujiwara: Yes, so I hope you can cherish every tradable node that appears in the market. The profits it brings us are very attractive.

[7/9/24, 9:16:14 PM] princess 🏓 keiko Fujiwara:




<attached: 00002519-PHOTO-2024-07-09-21-16-14.jpg>

73. Keiko continued to pressure Andrew to invest more, promising that achieving VIP1 status would unlock additional benefits and ensure smooth withdrawals.

74. On July 17, 2024, following Keiko's instructions, Andrew transferred 3,597 USDC from his Coinbase account to ICMarket. The next day Andrew transferred another 4,415 USDC, again following Keiko's instructions.

75. On August 15, 2024, Andrew tried to withdraw $1,000 from his ICMarkets account. ICMarkets Customer Service informed him that to access his funds, he needed to pay a total of $4,741.43 in various fees. When Andrew questioned these fees, he was told they covered transaction costs from June to July and that payment was required by August 19, 2024, to avoid an additional $100 per day fee.

76. Andrew could not meet demands for additional funds and was unable to withdraw anything. He lost $10,307.25.

**INCA DIGITAL TRACES STOLEN ASSETS**

77. After Plaintiff was unable to recover his funds, he contacted Inca Digital ("Inca"), a digital market investigation firm. Inca's investigation revealed that Defendants orchestrated a common scheme to steal money from Plaintiff and similarly situated Class Members. The investigation further determined that these stolen funds were transferred to cryptocurrency wallets under Defendants' control, which are listed in Appendix A.

78. Based on its analysis, Inca concluded that the Class Members include approximately 2,000 victims.

79. Inca's investigation revealed that Defendants utilized fake platforms to move and convert Class Members' assets, transferring the funds through a series of transactions designed to obscure their origins. Inca's investigation was conducted in two precise, reliable, and replicable phases. In Phase One, Inca's "forward tracing" began tracking the flow of funds by examining transfers from Plaintiff to the addresses he was given by Defendants, and then tracking subsequent transfers. This process involved three steps: (1) identifying the addresses of wallets that initially received Plaintiff's assets; (2) tracking the subsequent transfer of those assets to intermediary addresses; and (3) determining that Plaintiff's assets were ultimately deposited into the wallets

listed in Appendix A, which include wallets on the cryptocurrency exchanges Binance, OKX, and KuCoin.

80. 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.

81. 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.

82. 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.

83. 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. Overall, these interactions between the different wallets in the network provides a high degree of certainty that the entire network exists as part of the scam and is controlled by Defendants.

84. **Wendy Lee & Eileen Burbridge.** Plaintiff 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 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.

85. These funds were then transferred by Defendants through their fraudulent network of crypto wallets, including Pivot Address 0x63390bF7BD8c81809D69963D9d4b1E5F22844909 (Pivot Address 1) and Pivot Address 0x9f30654d708a2FD0C28855f8a5ee34a0Ce0b587c (Pivot Address 2).

86. 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

information and belief, Defendants used these funds to purchase cryptocurrency which was transferred through the network controlled by Defendants.

87. **Mary Scott**. On May 7, 2024, Plaintiff transferred 5 USDC (approximately $5 at the time) to the address 0x70B63e1F650CE252304c9E7f825fc4d68177706D. On May 9, Plaintiff transferred 0.00334134 ETH Ethereum (approximately $10 at the time) to the address 0xe978a33aA86529dA089F5C1EEfDDcC17939Ebc88. Defendants told Plaintiff that these transfers were to his CoinExchange account, but they were really to a crypto wallet controlled by Defendants. Once transferred, these funds were no longer within Plaintiff's control.

88. These funds were then transferred by Defendants through their fraudulent network of crypto wallets, including Pivot Address 0x9a3642A0C6D95485d3a5dF9cA25Ddc8971Be122b (Pivot Address 3) and Pivot Address 0x1Ee69c435fd024DD639110C00059e0904bc2905E (Pivot Address 4), ultimately ending up in Crypto wallets controlled by Defendants, including the wallets listed in Appendix A.

89. 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 information and belief, Defendants used these funds to purchase cryptocurrency which was transferred through the network controlled by Defendants.

90. **Verna**. On March 5, 2024, Plaintiff transferred 0.133 ETH (approximately $470 at that time) to address 0x19cBE2012d79f28065cD3005Ab8Cbc12A301c82B. On March 29 and April 5, Plaintiff transferred 0.138 ETH (approximately $480 at that time) and 0.151 ETH (approximately $490 at that time) to address 0xe77025E924346A3F140a24d2B92c5b8449605235. Plaintiff believed these transfers to be to his Vbtex account, but they were really to wallets controlled by Defendants. Once transferred, these funds were no longer within Plaintiff's control.

91. These funds were then transferred by Defendants through their fraudulent network of crypto wallets, including Pivot Address 0xd2b57f175E2CBb1B561d6109CbAAF17B09AcEcE2 (Pivot Address 5), ultimately ending up in Crypto wallets controlled by Defendants, including the wallets listed in Appendix A.

92. **Ettie Lee**. On May 24, 2024, Plaintiff transferred 0.01084736 ETH (approximately $30 at that time) to the address 0xEEAb811232873c3e7777A78868FE222F45766206. Once transferred, these funds were no longer within Plaintiff's control. That same day Plaintiff made two additional transfers of 798 USDC and 6,696 USDC to the address 0xEEAb811232873c3e7777A78868FE222F45766206. On May 29, Plaintiff made an additional transfer of 4,997 USDC to the same wallet. Plaintiff believed these transfers to be to be the platform Alpha Homora, but was really a wallet controlled by Defendants. Once transferred, these funds were no longer within Plaintiff's control.

93. These funds were then transferred by Defendants through their fraudulent network of crypto wallets, including Pivot Address 0x1Ee69c435fd024DD639110C00059e0904bc2905E (Pivot Address 4), ultimately ending up in Crypto wallets controlled by Defendants, including the wallets listed in Appendix A.

94. **Keiko Fujiwara**. On June 4 and 21, 2024, Plaintiff transferred 1,074 USDC and 1,219 USDC to the address 0xdCEc886f0D82074F4D5d03657d95D3aCbE05c8b1. Plaintiff transferred an additional 3,597 USDC to the same address on July 17 and an additional 4,415 USDC on July 18. Plaintiff believed these transfers to be to his ICMarket account, but they were really to a wallet controlled by Defendants. Once transferred, these funds were no longer within Plaintiff's control.

95. These funds were then transferred by Defendants through their fraudulent network of crypto wallets, including Pivot Address 0xb28B13e4a88316bDa38675C0BFC23c974a7fb5e4 (Pivot Address 6), ultimately ending up in Crypto wallets controlled by Defendants, including the wallets listed in Appendix A.

96. On information and belief, Defendants' scheme involved facts common to Class Members, including:

(i) persuasive conversations with Class Members to lure them into investing through the common fraudulent platforms, facilitated by communications via social media and messaging apps, the use of fake identities, and false claims related to cryptocurrency investing and trading;

(ii) the common use of counterfeit websites and applications by Class Members;

(iii) the intentional and unlawful conversion of Class Members' cryptocurrency for Defendants' own use;

(iv) the common use of cryptocurrency wallets under Defendants' exclusive control; and

(v) significant financial harm to Class Members resulting from the conversion of their assets.

97. The consistent patterns uncovered by Inca's investigation provide compelling evidence of a systematic fraud network designed to funnel stolen funds and launder money. Inca's meticulous tracing established a direct link between Defendants' actions and the financial losses suffered by Plaintiff and other Class Members, underscoring the organized and deliberate nature of the fraud. Given Defendants' ability to move funds at any moment, this evidence supports the urgent need for immediate injunctive relief, without notice, to freeze the wallets listed in Appendix A.

## CLASS ALLEGATIONS

98. This action may be properly maintained as a class action under Article 9 of the CPLR.

99. The proposed Class is initially defined as follows: all persons and entities whose funds were unlawfully taken by Defendants beginning on January 1, 2023, and whose stolen cryptocurrency is contained in the wallets listed in Appendix A.

100. 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.

101. Plaintiff reserves the right to amend or modify the Class in connection with a motion for class certification or as the result of discovery.

102. Plaintiff does not currently know the precise size of the proposed Class, but Plaintiff is aware that the Class is so numerous that joinder of all members is impracticable, if not impossible, because of the number of Class Members and the fact that Class Members are potentially in geographically disparate locations. Upon information and belief, the Class includes at least one hundred members.

103. Although the number and identities of Class Members are currently unknown to Plaintiff, it is possible to attempt to ascertain Class Member identities through notice to the original owners of assets contained in the accounts listed in Appendix A of this Complaint, as well as through discovery, including into account records at relevant institutions.

104. Nearly all factual and legal issues raised in this Complaint are common to each of the members of the Class and will apply uniformly to every member of the Class.

105. The claims of the representative Plaintiff are typical of the claims of each member of the Class, and by pursuing his own interests Plaintiff will advance the interest of the absent class members.

106. Plaintiff, like all other members of the Class, sustained damages arising from Defendants' schemes and subsequent digital transactions to convert stolen property and hide the locations of victims' cryptocurrency assets.

107. The representative Plaintiff and the members of the Class were, and are, similarly or identically harmed by the same unlawful, deceptive, unfair, systematic, and pervasive pattern of misconduct.

108. Plaintiff, like all other members of the Class, is entitled to the same declaratory, injunctive and other relief as the members of the Class.

109. Plaintiff will fairly and adequately represent and protect the interests of the Class. There are no material conflicts between the claims of the representative Plaintiff and the other members of the Class, including absent members of the Class, that would make class certification inappropriate.

110. Counsel selected to represent the Class will fairly and adequately protect the interest of the Class and have experience in complex and class litigation and are competent counsel for class action litigation.

111. Counsel for the Class will vigorously assert the claims of all members of the Class.

112. This action is properly maintained as a class action in that common questions of law and fact exist as to the members of the Class 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:

a. the interests of the members of the Class in individually controlling the prosecution or defense of separate actions and/or proceedings;

b. the impracticability or inefficiency of prosecuting or defending separate actions and/or proceedings;

c. the extent and nature of any litigation concerning the controversy already commenced by members of the Class;

d. the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and

e. the difficulties likely to be encountered in the management of a class action.

113. Among the numerous questions of law and fact common to the Class are:

f. whether Defendants have acted or refused to act on grounds generally applicable to the Plaintiff and the Class;

g. 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;

h. to what extent Plaintiff and members of the Class are entitled to damages; and

i. to what extent Plaintiff and members of the Class are entitled to declaratory and injunctive relief.

114. Defendants have consistently acted and refused to act in ways generally applicable to the Class. Thus, final injunctive relief with respect to the entire Class is appropriate.

115. Plaintiff and the members of the Class 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 detailed in Appendix A, Plaintiff and the members of the Class will not be able to recover their funds and would lose their property forever.

## FIRST CAUSE OF ACTION
## CONVERSION

116. Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

117. Plaintiff's and members of the Class's stolen funds are identifiable intangible articles of property, traceable using identified techniques and associated with specific virtual asset addresses.

118. Plaintiff and other Class members had an immediate possessory right to the stolen funds.

119. Defendants intended to and did exercise absolute dominion over Plaintiff's and members of the Class's stolen funds when Defendants transferred the stolen funds to addresses over which Plaintiff and the Class have no control and moved those assets through multiple digital transactions in an attempt to hide the illicit transactions and current location of the stolen assets.

120. Defendants' dominion over Plaintiff's and the Class's stolen assets was in derogation of their rights to the assets, completely depriving Plaintiff and the Class of the use of the stolen assets.

121. Defendants' dominion over Plaintiff's and the Class's stolen assets damaged Plaintiff and the Class.

**SECOND CAUSE OF ACTION**
**MONEY HAD AND RECEIVED**

122. Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

123. Defendants received Plaintiff's and the Class's stolen assets from them by way of the "pig butchering" scheme described above.

124. Defendants benefited from receiving Plaintiff's and the Class's stolen assets by transferring them to digital wallets under Defendants' sole control.

125. In principles of equity and good conscience, Defendants should not be allowed to retain Plaintiff's and the Class's stolen assets because Defendants had no authority to receive and transact Plaintiff's and the Class's stolen assets.

**THIRD CAUSE OF ACTION**
**UNJUST ENRICHMENT**

126. Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

127. Plaintiff and members of the Class each conferred a benefit on the Defendants when, as part of the "pig butchering" scheme described above, they sent assets to Defendants under the false pretense of participating in legitimate investments.

128. Defendants did not use Plaintiffs' assets for legitimate investments, and instead, after gaining control of these assets under false pretenses, Defendants diverted Plaintiffs' assets into their own possession.

129. Defendants' retention of Plaintiffs' assets is inequitable.

130. It is against equity and good conscience to allow Defendants to retain these assets at the expense and detriment of Plaintiff and Class members.

**DEMAND FOR RELIEF**

131. Wherefore, Plaintiff respectfully requests that this Court:

132. Enter a temporary restraining order and preliminary and permanent injunctive relief prohibiting Defendants from disposing of, processing, routing, facilitating, selling, transferring, encumbering, removing, paying over, conveying or otherwise interfering with debts, accounts, receivables, rights of payment, or tangible or intangible assets of any kind, whether such property is located inside or outside of the United States, including, but not limited to, cryptocurrency or other digital assets held in cryptocurrency wallets detailed in Appendix A, including Plaintiff's and the Class's property;

133. Award Plaintiff damages in the amount of at least $337,000, that being the value of Plaintiff's stolen assets at the time of the theft from Plaintiff;

134. Declare this action to be a class action properly maintained pursuant to CPLR § 901, appoint Plaintiff as representative of the Class, and designate Plaintiff's counsel as Class Counsel;

135. Award compensatory damages, restitution, disgorgement, and any other relief permitted by law or equity;

136. Award Plaintiff reasonable attorneys' fees and costs pursuant to CPLR § 909, and any other applicable provision of law; and

137. Award Plaintiff and the Class such other relief as the Court may deem just and proper under the circumstances.

Dated: October 23, 2024

/s/ Rishi Bhandari

Rishi Bhandari, Esq.
Mandel Bhandari LLP
80 Pine Street, 33rd Floor
New York, NY 10005
Phone: (212) 269-5600 ext. 100

*Attorneys for Plaintiff*

**APPENDIX A**

Binance
0x8E670D1d6993413Ce7B23FCEB4e26101D2b816e0
0xE025Fcc2D58CA09852DEd8d0FCdb9db4355f4a8F
0xa3364D012dA0E925b908cfE98008418D4d145573
0xb4B44239Bc9B5c4c810A181Cb5aFE2b15F1C7087

OKX
0x5d8814d1268d70d89c2EE8cdF9e14fF64902fcE6
0x0eC4E0303897a8E8b477Fdce43e577B3981b5617
0xdA22870E0Bd87133250fbC319476E278D7af93c2
0x03A080f0763E53A2304e98A4f9bC663f66ad1B26
0x5594c5ECA2B8CF2CD3A2c0FbA172F1dF2C15645F

KuCoin
0x21317D512417c31a5CEA75Fb6A57f6206F02c0e6