

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

-----X

THE PEOPLE OF THE STATE OF NEW YORK
By LETITIA JAMES, Attorney General
of the State of New York,

Plaintiff,

SUMMONS

-against-

Index No. _____

IAS Part: _____

Plaintiff designate Queens
County as the Place of Trial

Unknown Parties in Ownership and/or Control of
Digital Wallet Addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d,
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and
TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu,
and Unknown Others,

Defendants.

-----X

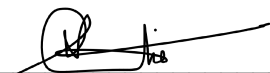
TO THE ABOVE NAMED DEFENDANTS:

YOU ARE HEREBY SUMMONED to answer in this action and to serve a copy of your answer, or if the complaint is not served with this summons, to serve a notice of appearance, on the Plaintiff's attorney within 20 days after service of this summons, exclusive of the day of service. If this summons is not personally served upon you, or if this summons is served upon you outside the State of New York, then your answer must be served within thirty (30) days. In case of your failure to appear or answer, judgment will be taken against you by default for the relief demanded in the complaint.

Pursuant to CPLR § 503, venue is proper in Queens County because multiple Victims are located in Queens County.

Dated: January 9, 2025
New York, New York

LETITIA JAMES
Attorney General of New York

By  _____

Shantelee Christie
Jonathan Bashi
Assistant Attorneys General
Investor Protection Bureau
Office of the New York State
Attorney General
28 Liberty Street
New York, NY 10005

Counsel for the People of the State of New York

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

THE PEOPLE OF THE STATE OF NEW YORK,
by LETITIA JAMES, Attorney General
of the State of New York,

COMPLAINT

Plaintiff,

- against -

Index No. _____
IAS Part _____
Assigned to Justice _____

Unknown Parties in Ownership and/or Control of
Digital Wallet Addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d,
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and
TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu,
and Unknown Others.

Defendants.

Plaintiff, the People of the State of New York, by Letitia James, Attorney General of the State of New York (“OAG” or “Plaintiff”), alleges the following against unknown parties in ownership and/or control of digital wallet addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d (hereinafter “Wallet 1”),
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8 (hereinafter “Wallet 2”), and
TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu (hereinafter “Wallet 3”) (“Unknown Parties”), and other unknown persons (“Unknown Others” and, together with the Unknown Parties, “Defendants”).

NATURE OF THE ACTION

1. From at least January 2024, through at least June 2024, Defendants, a web of unknown individuals, in and from unknown locations, employed a scheme to defraud New Yorkers and individuals across the country—some of whom are recent immigrants to the United

States with very little in assets—by tricking them into believing they would be paid to work remotely for legitimate businesses. Defendants recruited these individuals (each a “Victim”) using text messages and deceived them into purchasing and transferring cryptocurrency into multiple digital wallet addresses, also known as wallets, that Defendants owned and/or controlled, and then secretly moved those assets to other wallets Defendants owned and/or controlled.

2. As part of the scheme, Defendants posed as job recruiters, trainers, managers, and customer service agents of different imposter companies. Through private messages over the WhatsApp messenger application (“WhatsApp”) and other messenger groups, they lured Victims into performing the relatively simple task of reviewing and rating products on now-defunct websites that Defendants created. The task involved clicking on various products shown on the websites to supposedly generate data that helped promote those products to consumers. However, the companies were impersonations of real companies and the websites were merely a façade for a massive fraud.

3. In exchange for their work, Victims were fraudulently promised a convoluted compensation consisting of salary, bonuses, and commissions. Victims were required to create accounts on these websites and make deposits in the form of USD Coin (“USDC”) or USD Tether (“USDT”)—both of which are stablecoins, a type of cryptocurrency theoretically pegged to the U.S. Dollar—to designated wallets Defendants owned and/or controlled. These deposits were ostensibly to cover the price of the products they were reviewing and rating, and to increase their earning potential in performing the work, as Victims were told the more cryptocurrency they deposited the more salary and bonuses they would earn. To make the deposits Victims were instructed to use their own money to purchase cryptocurrency on various platforms.

4. Victims often were unfamiliar with cryptocurrency, and trainers would guide them step by step via text message through the process for opening up accounts on the different platforms and show them how to purchase the cryptocurrency used to make the deposits.

5. Defendants led the Victims to believe they were accumulating compensation in their accounts and that they could ultimately withdraw the amounts they earned during their employment. This was a lie. Once the Victims sent their cryptocurrency to Defendants' wallets, Defendants secretly transferred the cryptocurrency to other wallet addresses that Defendants owned and/or controlled.

6. There was no legitimate operation and Victims earned no actual compensation. Through their deceptive and unlawful practices, Defendants intentionally misled the Victims—including New Yorkers—into believing they had obtained legitimate and income-producing employment when, in reality, Defendants were simply stealing the Victims' cryptocurrency.

7. OAG secured a freeze of the USDC and USDT stolen by Defendants and contained in Wallets 1, 2, and 3. As of April 26, 2024, Wallet 1 contains approximately 219,840 USDC, Wallet 2 contains approximately 862,347 USDT, and Wallet 3 contains approximately 1,097,320 USDT. The cryptocurrency contained in Wallets 1, 2, and 3 are valued at approximately \$2,179,507 and remain available for seizure, disgorgement, and restitution pursuant to an order from the Court.

8. This action seeks an order from the Court (i) permanently enjoining Defendants from engaging in fraudulent, deceptive, and illegal acts in violation of New York's General Business Law ("GBL") Articles 23-A (the "Martin Act") and 22-A, and Executive Law § 63(12); (ii) permanently enjoining Defendants from soliciting New Yorkers for employment, sending any unsolicited text messages or other communications to New Yorkers and engaging in any

practice or course of business related to the issuance, distribution, exchange, promotion, advertisement, negotiation, purchase, investment advice, or sale of any commodities within or from this state; (iii) authorizing OAG to take possession of the frozen USDC and USDT stablecoins in Wallets 1, 2 and 3; (iv) directing Defendants to pay damages, restitution, and disgorgement for their unlawful, fraudulent, and illegal conduct; (v) imposing a civil penalty pursuant to GBL§ 350-d of \$5,000.00 for each deceptive act committed by Defendants; (vi) granting costs to the State of New York of \$2,000.00, pursuant to CPLR § 8303(a)(g), against each Defendant; and (vii) for such other monetary penalties and equitable relief as the Court may deem just and proper.

PARTIES

9. Plaintiff Letitia James is the Attorney General of the State of New York. The State of New York has an interest in upholding the laws of the State, and OAG is charged with enforcing those laws. OAG brings this action pursuant to the Martin Act, GBL §§ 349 and 350, and Executive Law § 63(12).

10. Defendants, Unknown Parties, are persons of unknown location and citizenship in ownership and/or control of Wallets 1, 2 and 3.

11. Defendants, Unknown Others, are persons of unknown location and citizenship who sent unsolicited text messages to individuals located within and from the State of New York and other states, advertising and offering remote employment opportunities that were non-existent. Defendants used spoofed telephone numbers, including New York telephone numbers +1 (917) 553-2445 and +1 (315) 504-5310, to send the messages. Defendants also impersonated websites and real businesses such as Digistore24, FeraAI, Birdeye, Wish, Summit Digital Marketing, Page Zero Media and Sachs Marketing Group, and claimed to be associated

therewith as recruiters, trainers, managers, and customer service representatives in order to fraudulently induce Victims to purchase cryptocurrency and then transfer it to Defendants. These Defendants identified themselves only as “Rachel,” “Emily,” “Maria,” “Alexander,” “Evelyn,” “Olivia,” “Emma,” “Nicholas,” “Chloe,” “Alex(ander),” “Eliana,” “Aria,” “Amy Christian,” and “Anthony.” Defendants, Unknown Others, also used the names “Jemalle Sulay,” “Joymie Lynn Garcia Parinas,” “Princess Rhaiza Maxino Tomawis” and “Annalyn Francisco Castillo” and the email addresses: “sulayjemalle@outlook.com,” “cahneahneol@gmail.com,” “wise071622@gmail.com” and “arrianesey@gmail.com.”

RELEVANT ENTITIES

12. Circle Internet Financial, LLC (“Circle”) is a Delaware limited liability company with its headquarters in Massachusetts and a registered address in New York county. Circle is a financial technology company that controls the software and rules that apply to the USDC stablecoin, which is a commodity¹ under the Martin Act. Circle has the ability to block wallets from sending and receiving (*i.e.* to freeze) USDC and has done so with respect to the USDC contained in Wallet 1.

13. Tether Holdings Limited, the holding company of Tether Limited (“Tether”) is incorporated in the British Virgin Islands. Tether is financial technology company that controls the software and rules that apply to the USDT stablecoin, which is a commodity under the Martin Act. Tether has the same ability to freeze USDT and has done so with respect to the USDT contained in Wallets 2 and 3.

¹ Stablecoins have characteristics of securities and commodities.

JURISDICTION AND VENUE

14. Plaintiff brings this action pursuant to the Martin Act, GBL §§ 349 and 350, and Executive Law § 63(12) to enjoin Defendants' fraudulent, illegal, and deceptive business practices. Plaintiff also seeks restitution on behalf of the Victims, disgorgement, damages, civil penalties, and costs, as authorized by law, to be paid to the State of New York.

15. The Martin Act prohibits fraud and misleading practices and representations by any person or entity where engaged in to induce or promote the issuance, distribution, exchange, sale, negotiation, or purchase within or from this state of any securities and commodities, regardless of whether issuance, distribution, exchange, sale, negotiation, or purchase resulted. The Martin Act empowers OAG to seek legal and equitable relief for the use of fraudulent practices in the issuance, exchange, sale, promotion, negotiation, advertisement, investment advice, distribution or purchase of securities and commodities in or from the State of New York.

16. GBL Article 22-A prohibits deceptive business practices and empowers OAG to seek injunctive relief and restitution. GBL § 349 prohibits "deceptive acts or practices in the conduct of any business, trade or commerce." GBL § 350-d empowers OAG to seek civil penalties of up to \$5,000.00 for each violation of GBL Article 22-A.

17. Executive Law § 63(12) empowers OAG to seek an order enjoining the continuance of repeated fraudulent or illegal acts in the carrying on, conducting, or transacting of business affecting the interests of the public within the State of New York. Executive Law § 63(12) also empowers OAG to seek injunctive relief, restitution, disgorgement, damages, and costs when any person or business entity has engaged in fraudulent or illegal acts or has otherwise demonstrated repeated or persistent fraudulent or illegality in the carrying on, conducting, or transacting of business.

18. Defendants falsely advertised to and solicited New Yorkers and other U.S. citizens for non-existent employment opportunities; used fraud, deceit, false pretense, concealment, and misrepresentations to induce them into purchasing commodities in the form of cryptocurrencies within or from the State of New York; and fraudulently transferred Victims' cryptocurrency to wallets that Defendants owned and/or controlled. This Court has jurisdiction over the subject matter of this action, personal jurisdiction over the Defendants, and authority to grant the relief requested pursuant to the Martin Act, the GBL Article 22-A, and Executive Law § 63(12).

19. Pursuant to CPLR § 503, venue is proper in Queens County because multiple Victims are located in Queens County.

FACTUAL ALLEGATIONS

I. The Structure of the Fraudulent Job Scheme

A. Defendants Solicit Victims for Fake Jobs

20. From at least January 2024 through at least June 2024, Defendants, a network of fraudsters, operated a scheme to defraud Victims in New York and across the country by stealing Victims' cryptocurrencies using a collection of wallets that Defendants owned and/or controlled. In each instance, Defendants initiated the scheme by sending unsolicited SMS text messages to the Victims from various spoofed telephone numbers and posing as recruiters from different staffing agencies claiming to be hiring and offering remote full- and part-time employment opportunities. The messages were sent directly to Victims' personal mobile phones using messaging apps and offered the work opportunities to individuals who possessed a social security number, U.S. bank account, and were of a minimum required age, commonly 23.

21. Recipients who affirmatively expressed interest in the job opportunity were told they would be contacted via WhatsApp by individuals claiming to be “trainers,” and who would share further details about the supposed work opportunity. Persons posing as trainers typically contacted Victims within one to two days.

B. Defendants Use False Statements and Deceptive Images to Perpetuate Victims’ Perception of Legitimate Work

22. Communicating through WhatsApp, the trainers told the Victims they could make money by reviewing products on their new employers’ websites. The “reviews” consisted of clicking on the products on the website, which supposedly generated market data that helped to facilitate sales. The companies the trainers identified to the Victims were real, but the employment opportunities were not and any association between the Defendants and these companies was entirely fake.

23. Defendants sent Victims links to websites that replicated the imagery of the legitimate companies’ websites, but which were really just imitations created to perpetuate the fraud. The links to these imposter websites frequently failed during the time some Victims were ensnared in the scheme, which the trainers attributed to “system updates.” Each time a link failed, Defendants sent Victims new links to the false sites to keep their scheme going.

24. Trainers showed the Victims how to create individual “working accounts” on these websites that would purportedly allow them to conduct the product reviews, receive payment and hold account balances. In reality, the working accounts were illusions—they did not exist, there were no balances accumulating, and working accounts were simply another lie Defendants told to deceive Victims.

25. After Victims created their working accounts, they were told to allot between 30 minutes to an hour for “training” in a supposed trainer account on how to click and submit the products in their review sets before they could transition to doing it in their working accounts.

26. During the training sessions, trainers deceived the Victims, telling them that within a product set, each product had a price in USDT assigned to it. In order to review products, Victims were required to maintain a working account balance equal to or greater than the “price” assigned to the product. Victims were assured that they were not buying the products, but that maintaining those account balances helped “legitimize” the data they were generating.

27. To maintain that account balance, Victims were told they needed to purchase and deposit stablecoins into their working accounts, which required them each to create a wallet and connect it to their working account. Defendants also claimed the wallets were necessary for Victims to receive compensation in the form of (i) commissions, as a percentage of the price of the products they reviewed; (ii) salary, upon achieving certain milestones in the number of product sets completed; and (iii) bonuses, upon completing training and hitting other milestones. This compensation, supposedly to be paid in stablecoins, was never real and deposits Victims supposedly made into their “working accounts” in reality simply went into wallets that Defendants owned and/or controlled.

28. Each Victim during, and often after, their training was instructed to communicate with their respective trainer by sending screenshots of what they were seeing and doing while submitting products so that trainers could further guide them. Victims were promised that upon completing their training sessions, they would receive a commission based on the products they reviewed during training, along with a registration bonus for creating their working accounts. That initial compensation would serve as the starting balance for their own working accounts.

29. Most Victims had no prior experience with cryptocurrency and were using it for the very first time. Trainers also showed Victims how to create their wallets and deposit money on various cryptocurrency platforms such as LBank or Crypto.com, and Cash App, a mobile payment service; how to supposedly connect their wallets to their working accounts to collect their promised salaries and commissions; and how to purchase USDC and USDT in their wallets and transfer it to their working accounts. Alternatively, trainers showed Victims how to buy other cryptocurrency, such as Bitcoin or Ether, and convert them into USDC or USDT which Victims then transferred to Defendants. Each unit of cryptocurrency that Victims purchased and transferred constituted the purchase and transfer of a commodity under the Martin Act.

II. Defendants Repeatedly Tricked Victims into Depositing More Cryptocurrency into the Fraud

30. The success of the remote work fraud scheme depended on convincing Victims to keep depositing stablecoins into the scheme while preventing them from getting any of it out. This was typically achieved through three channels: account recharges, “product merges” or “package missions”, and fees, all of which were just ploys to extract deposits from Victims.

31. Once their wallets were connected, Victims were assigned “sets” of products to complete, which would generate fictitious commissions in their working account based on the price of each product. Each product set typically consisted of around 40 products. Inevitably, Victims encountered a product with a review price that exceeded the Victim’s account balance. In those situations, Victims were instructed to “recharge” their working account balances by purchasing and depositing additional stablecoins to cover the shortage, which allowed them to continue the review and achieve their commission.

32. Defendants also enticed Victims into depositing cryptocurrency by promoting participation at higher “tiers” in the product review process. Victims were told that they started

their employment at the Bronze tier (the lowest), but could upgrade to Silver, Gold, Diamond and Premium (the highest). Supposedly, these tier upgrades would bring Victims higher-priced products and higher salaries and commission rates for completed product sets, but also required them to carry significantly higher working account balances. In reality, the tiers were just a means to attract more and larger stablecoin deposits from Victims for the Defendants to steal.

33. Victims viewing their working accounts on Defendants' websites saw illusory balances reflecting USDT deposited and profits supposedly earned, which deceived them into believing that they were earning rather than losing money. Trainers reinforced this belief by showing Victims how to make small withdrawals of their profits from their working accounts into their wallets. But this profit realization was a sleight of hand, as Victims were directed almost immediately to put those amounts back into their working accounts to obtain the next product set.

34. The largest component of the fraud was what trainers referred to as a "product merge" or "package mission," where a Victim received multiple products simultaneously for review whose combined value exceeded the Victim's working account balance. Trainers were quick to characterize these to Victims as a rare but good thing, since Victims' compensation supposedly was heavily tied to the total value of the products they reviewed. Trainers also told Victims that their commission rates for a "merge" or "package" were significantly higher, in some instances claiming it was nine times higher, than when just reviewing a single product.

35. Over a short amount of time, Victims found themselves facing frequent product merges marked by products with high prices. This required Victims to "recharge" their accounts with higher amounts of stablecoin deposits. Conned into believing that the phony profits were real and having already committed substantial sums of their own stablecoins, Victims were

further deceived into believing that if they reached a withdrawal point, they could claim and withdraw their earnings and deposits.

36. The more stablecoins Victims committed to the scheme to cover the deposit demands associated with the product sets, the more desperate they became in trying to realize their purported earnings and extract their balances. Facing working account deficits with increasing frequency and size, Victims went to greater lengths to obtain the funds to clear them, such as borrowing money from friends and family, and undertook extreme efforts to obtain the stablecoins needed to reach a point where they were told they could reclaim the significant assets they had invested in this scam.

III. Defendants Used a Collection of Wallets to Steal Victims' Cryptocurrency

37. Victims were directed at the start of their "employment" to use cryptocurrency platforms to buy and transfer USDC and USDT to their working accounts. When Victims reached one platform's limits for purchasing, exchanging, or transferring USDT and USDC at a given time, or if there was a waiting period, trainers responded by pressuring Victims to open accounts on additional platforms, or to use more expensive options, such as Bitcoin ATMs to keep the cryptocurrency flowing into the Defendants' wallets.

38. Beyond the use of trainers, the Defendants also convinced Victims that their respective fake companies had designated "Customer Service" representatives, which further cemented the fraudulent scheme with the Victims.

39. To transfer stablecoins into their working accounts, Victims were instructed to contact their Customer Service representatives, usually through separate WhatsApp chats. Customer Service provided Victims with intermediary wallets that Defendants owned and/or

controlled (each, an “Intermediary Wallet”) where Victims were instructed to send their stablecoin deposits.

40. The Intermediary Wallets that Customer Service sent the Victims changed daily. The Defendants’ ownership and/or control of these Intermediary Wallets ultimately allowed them to redirect and steal the Victims’ stablecoins. Only an owner or possessor of a wallet’s private key—essentially a long and complex password—can effectuate cryptocurrency transfers out of a wallet.

41. Defendants directed Victims to send their cryptocurrency to nearly 100 Intermediary Wallets during the time Victims were in Defendants’ make-believe employ. At least sixteen of the Intermediary Wallets Defendants provided were used repeatedly to defraud multiple Victims who otherwise had no connection to one another and were theoretically working for different companies performing the same make-believe tasks.

42. Unknown to the Victims, Defendants, as owners and/or controllers of the Intermediary Wallets, transferred the stablecoins from the Intermediary Wallets into two other wallets they owned and/or controlled: (0x6298BfEd428B843d326dDAE1A406441CDB40db80 (“Transition Wallet A”) and 0x7a448169e9d5DB6405087dAB9dfF774Db6589b05 (“Transition Wallet B”, and collectively with Transition Wallet A, the “Transition Wallets”)). Defendants then transferred the stablecoins that went to Transition Wallet A into Transition Wallet B, and then transferred them yet again into Defendants’ Wallet 1.

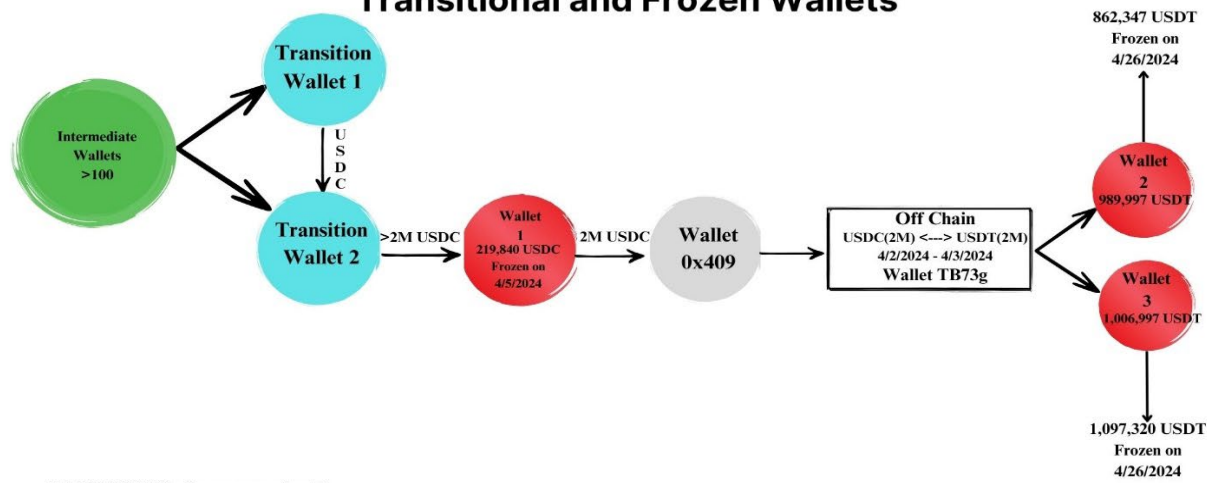
43. By April 1, 2024, over 2 million USDC collectively was transferred from the Intermediary Wallets, Transition Wallets or directly from the Victims’ wallets, into Defendants’ Wallet 1.

44. On and between April 2, 2024, and April 3, 2024, 1,999,999 USDC from Defendants' Wallet 1 was transferred to another wallet 0x409C4A8eC8eEBf4132E33122164D57C5B7039E59 (hereinafter "wallet 0x409"). As of April 5, 2024, Wallet 1 still holds 219,840 USDC, currently frozen and valued approximately \$219,840. Because the remaining USDC in Wallet 1 is frozen, Defendants cannot access, withdraw, or transfer it.

45. After the Defendants successfully transferred the 1,999,999 USDC to wallet 0x409, the Defendants used a foreign cryptocurrency platform, UCC Technologies LLC (doing business as Bitunix) ("Bitunix"), to exchange the USDC for USDT. This exchange was completed by transferring all of the USDC in wallet 0x409 to Bitunix's "mixer" wallet TB73gtW1hsTxxA9XUYKLSJKTSHw6Jk53eH ("wallet TB73g"). Bitunix has no "Know Your Customer" ("KYC") protocol for identifying and verifying its users, which has prevented the identification of the users behind wallet 0x409 and Wallets 1, 2, and 3. Defendants subsequently used three transactions to send approximately 990,000 USDT from wallet TB73g to Wallet 2 and another three transactions to send the remaining approximately 1,007,000 USDT to Wallet 3.

46. Defendants continued executing transactions in USDT in and out of Wallets 2 and 3 until April 26, 2024 when, at OAG's request, Tether froze the remaining USDT balances in those Wallets. As of April 26, 2024, approximately 862,347 USDT remains frozen in Wallet 2, and approximately 1,097,320 remains frozen in Wallet 3, currently valued at approximately \$862,347 and \$1,097,320, respectively. By freezing the USDT, Defendants are unable to access, withdraw, or remove the stablecoins from Wallets 2 and 3. The following chart shows how the Defendants moved the stablecoins through the Wallets up until OAG secured their freeze:

**Movement of USDC/USDT
From Intermediate Wallets to
Transitional and Frozen Wallets**



*All USDC/USDT values are approximated

IV. Defendants Defrauded Victims Using A Common Scheme

A. Victim Theo²

47. On March 1, 2024, Theo, a 39-year old online salesperson and resident of Queens, New York who immigrated from India, received a text message from one of the Defendants, a purported recruiter calling herself “Rachel” from Brilliant Staffing and claiming to have “exciting positions” with “numerous benefits and flexible requirements”. See Fig. 1. After Theo showed interest in the opportunity, Rachel asked permission to contact him via WhatsApp.

[Remainder of Page Intentionally Left Blank.]

² The true names of each Victim are known to OAG but have been replaced here with pseudonyms.

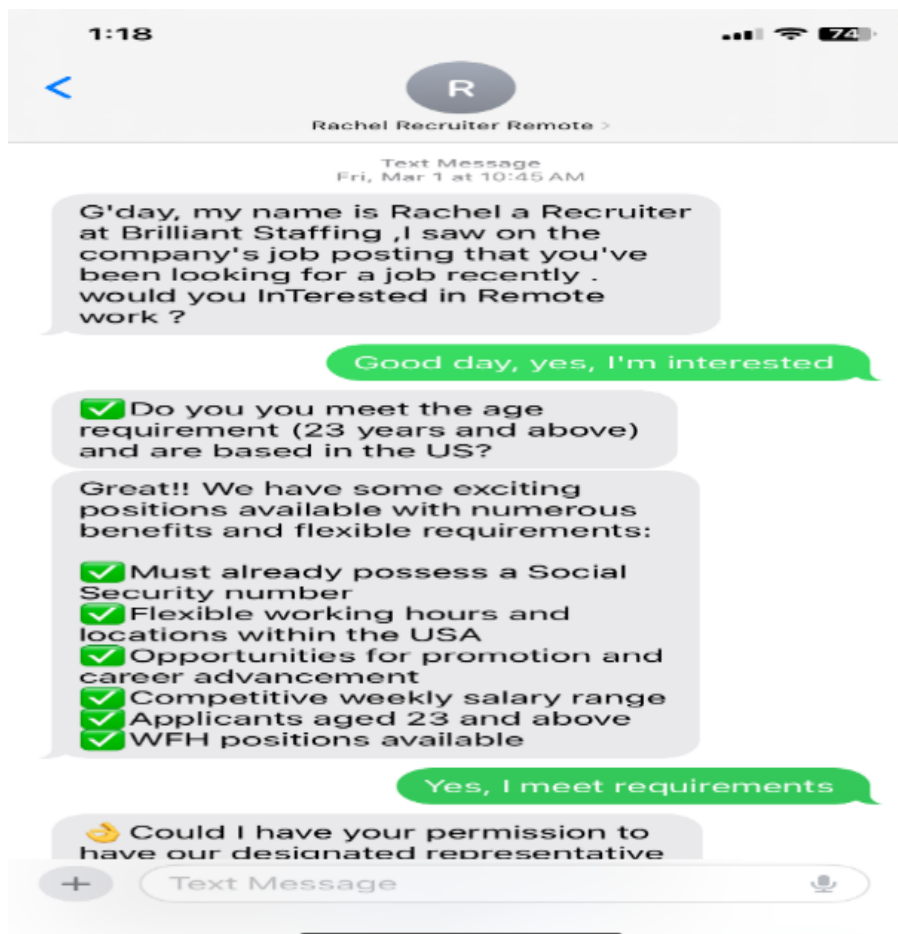


Fig. 1: Screenshot of initial SMS text message sent to Theo.

48. Through WhatsApp another Defendant, “Emily,” who claimed to work as a reviewer for a company called Digistore24 (“Digistore”), with the added role of “instructor/team leader,” offered Theo a remote job. The job purportedly entailed “clicking and collecting data from [Digistore’s] product data optimization platform....”

49. Emily told Theo that he would “get paid for the amount of work [he did]” and that he would earn daily commissions and salary, which would have enabled him to earn, on average, more than \$1,000 per week.

50. Emily provided Theo with access to the purported Digistore portal using a link shared via WhatsApp and she spent about 90 minutes using screenshots to train Theo on how to “master the workflow.”

1. Defendants Repeatedly Tricked Theo into Sending Cryptocurrency to Wallets They Owned and/or Controlled

51. Theo was promised a 15 USDT registration bonus for creating his own working account, as well as 25% of the supposed commissions generated during his training. Emily also instructed Theo on how to open a wallet on LBank and how to connect that wallet to his working account. She also explained that this wallet would be used both to deposit the USDC and USDT into his working account, as well as to withdraw his earnings.

52. In reality, there was no working account, and stablecoins that Theo deposited were actually going into wallets that the Defendants owned and/or controlled.

53. As Theo began working, Emily guided him on how to purchase and deposit more USDT and USDC so that he could continue to “click and submit” products to complete his product sets and earn the promised compensation. At Emily’s instruction, Theo would either buy Bitcoin and convert it in his wallet to USDT to deposit into his working account, or he bought USDC, which he could deposit directly into his working account.

54. Between March 4, 2024 and March 21, 2024, to cover the posted price for each product he was assigned, Theo repeatedly purchased USDC on platforms such as Gemini to deposit into his working account. Alternatively, Theo purchased Bitcoin on Cash App, which he then converted on LBank to USDT, to deposit into his working account.

55. On March 4, 2024, Theo made his first deposit of 34 USDT while reviewing products. Subsequently, each product Theo received increased in price, requiring a larger deposit amount for him to continue in his product set and earn his supposed commission. For example, on March 9, 2024, the price for one product required Theo to deposit 1,220 USDT. By March 12, 2024, another product’s price caused the deposit requirement to jump to 3,889.13 USDC and by March 15, 2024 the deposit requirement increased again to 13,069.51 USDC.

56. Theo grew concerned with these increases in required deposit amounts and noted that, in some instances, he was receiving multiple products simultaneously for review, which Defendants called “product merges.” He voiced these concerns to Emily, who characterized those developments as a “good thing considering the profits from it.”

57. To cover the required deposits, Theo leveraged numerous funding sources, including purchasing cryptocurrency with his credit cards, and borrowing over \$12,000 from friends and family, including people in India. Believing he held more than 50,000 stablecoins in deposits and accumulated earnings in his working account, on March 18, 2024, Theo told Emily that he wanted to withdraw his money.

58. When Theo tried to withdraw 50,000 stablecoins, he was told he needed to upgrade from the Bronze tier membership to the Gold, which required an additional 10,000 USDT deposit. Theo deposited 2,000 USDC toward the upgrade, expecting it would be added to the 7,976.26 USDT earnings balance reflected in his working account. Emily then told Theo that he could not use his account earnings for membership upgrades.

59. Forced to purchase and deposit more stablecoins to resume his withdrawal attempt, on March 21, 2024, Theo, bought an additional approximately \$8,000 worth of USDT, including using money borrowed from a friend, to complete the upgrade to Gold. But that still was not enough. Customer Service then told him his account needed to be verified, which required an additional USDT deposit, before his funds could be released.

60. Unable to purchase any more cryptocurrency, Theo pleaded with Emily to get his money back and even threatened to contact law enforcement. Emily denied any responsibility for returning Theo’s stablecoins and refused to help him. Believing he had been defrauded, Theo reported his losses to law enforcement on March 22, 2024.

2. Defendants Steal Theo's Cryptocurrency

61. From March 1st to March 21st, 2024, Defendants deceived Theo into spending \$58,112 U.S. dollars to purchase 56,046.43 in stablecoins that he was instructed to deposit across thirteen Intermediary Wallets controlled and/or owned by Defendants. Six of those Intermediary Wallets also were used to similarly defraud a Florida resident, Dena, and a seventh was used to defraud a New York resident, June.

62. Defendants used four of the Intermediary Wallets that Theo deposited stablecoins into to transfer a cluster of USDC into the two Transition Wallets. One of the four Intermediary Wallets transferred USDC to Transition Wallet A. The other three Intermediary Wallets transferred USDC to Transition Wallet B.

63. As alleged in Paragraph 42, Transition Wallet A transferred USDC into Transition Wallet B, which then transferred USDC into Wallet 1.

64. As alleged in Paragraph 45, Defendants converted the USDC to USDT and transferred it to Wallets 2 and 3.

B. Victim June

65. On March 8, 2024, Victim June, a 28-year old then-resident of Queens, New York, and a recent immigrant from India, received an unsolicited text message to her mobile phone from a recruiter named "Maria" who claimed to be from the "CultureFit Technology" staffing agency. Maria said she had "many work opportunities with numerous benefits and flexible requirements" for persons who "already possess a Social Security Number and U.S. Bank Account" and who were "aged 23 and above/flexible working hours."

66. June expressed interest in the position and was contacted on or around March 10th over WhatsApp by a person named "Alexander." Alexander offered to train June as a "Product

Traffic Enhancer” with FeraAI (“Fera”) and told her that the position involved reviewing and clicking on products on Fera’s platform to generate data that would boost product visibility and help Fera generate sales.

1. Defendants Repeatedly Tricked June into Sending Cryptocurrency to Wallets They Owned and/or Controlled

67. Alexander promised June that she would earn a salary after she completed her third and fifth days of work, and a commission of 1% of the total value of the products she reviewed, or 9% when she completed a “package mission.” Alexander also represented that all of June’s balances, recharges and commissions would be credited back to her and that she would not lose any money.

68. June had no prior experience using cryptocurrency. After she completed training, Alexander showed her how to establish a digital wallet on LBank and use Cash App to purchase and add cryptocurrency to her Fera working account. He also showed her the phony “income” she supposedly earned in registration bonuses and commissions, as well as how to recharge with more USDT to continue reviewing product sets.

69. Concerned over having to contribute her own money, June told Alexander unequivocally “I don’t want to continue with this anymore.” Having very little in financial assets, June explained that she had not heard of this type of work and that she was looking to earn money, not invest it. Alexander convinced June to continue, asserting falsely that the work entailed generating “genuine data created by real users [to] help promote and enhance [] products,” and giving false assurances about the legitimacy of the company she was working for.

70. Alexander, focused on having June complete her recharges as quickly as possible, directed her through a veritable obstacle course of cryptocurrency platforms during her time as a worker. In the first few days alone, he had her attempt purchases on Cash App and open accounts

on Crypto.com and Trust Wallet, another cryptocurrency platform. Alexander also pressured June, telling her that by not completing the recharge, it would be another day before she finished her product set, which “also means one less day of income,” and that she would not have completed enough working days to collect salary.

71. After June completed her first few training product sets, Alexander showed her how to withdraw her entire earnings balance from her Fera working account to her LBank wallet. But the very next recharge required June to quickly put the full withdrawal, and more, right back into the Defendants’ hands, causing her to buy even more stablecoins to complete the recharge and continue being defrauded.

72. As June reviewed more products as part of her “work,” she told Alexander that she found the process “addicting.” Eventually, June began encountering more and more “package missions,” which Alexander told her she was “lucky” to receive. These package missions required her to commit increasing amounts of her own money to buy cryptocurrency to cover the recharges and fund her working account.

73. These recharge amounts initially were for a few hundred USDT at a time but grew significantly in a matter of days. By March 18th, Defendants sent June package missions and recharge demands of over 1,000 USDT, followed the next day by two more in excess of 2,000 and 5,000 USDT, respectively. Throughout this process, Alexander continued pressing June to use any means available to continue putting up the cryptocurrency she supposedly needed to continue “working.” This included having her use her credit card and money transfers from her personal bank account to buy more USDT through her Trust Wallet account, wiring cash available on her Chase bank credit card to Coinbase, and encouraging her to borrow money from a friend, but without saying what it was for, lest they suspect the fraud.

74. As June scraped together the assets to cover these recharges, her stress and anxiety became palpable. She told Alexander that her bank account was down to virtually nothing, that she “[didn’t] know what else to do,” and “fe[lt] like crying right now” over the money she feared—correctly—that she’d lost. As she prepared to wire the last of the cash balance available on her credit card, June begged Alexander for an assurance that she would not receive another package mission. Alexander assured June that she was “a new user so the chances of getting one are slim” and that package missions were not easy to get.

75. On March 20, June wired approximately \$5,500 from a cash advance on her credit card to cover the pending recharge, hoping to finish her product set and withdraw her balance. Within minutes of completing the recharge and resuming her product set, June encountered another package mission and recharge this time for over 12,000 USDT. June knew she could not satisfy that amount and immediately told Alexander “I’m gonna die,” and begged him to help her get around the product merge. Alexander callously reminded June that product merges were a “good thing for us,” and about all of the money she had already committed.

2. Defendants Steal June’s Cryptocurrency

76. From March 10th to March 20th, 2024, during the time she was “employed” with Defendants, June was deceived into spending approximately \$6,250 purchasing cryptocurrency and transferring all of it in into USDT and USDC to the Defendants. That Defendants stole all of the little money June had is the sole reason she was not defrauded further.

77. Defendants instructed June to deposit her stablecoins into nine Intermediary Wallets. Three of those Intermediary Wallets were also used to defraud Victim Dena, while a fourth was used to also defraud Victim Theo, who is also a New York resident.

78. Defendants used two of the Intermediary Wallets that June deposited stablecoins into to transfer a cluster of USDC into the Transition Wallets. One of the two Intermediary Wallets transferred USDC to Transition Wallet A. The other Intermediary Wallet transferred USDC to Transition Wallet B.

79. As alleged in Paragraph 42, Transition Wallet A transferred USDC into Transition Wallet B, which then transferred USDC into Wallet 1.

80. As alleged in Paragraph 45, Defendants converted the USDC to USDT and transferred it to Wallets 2 and 3.

C. Victim Dena

81. On March 2, 2024, Victim Dena, a 38-year old tech salesperson and resident of Florida, received an unsolicited text message from a recruiter named “Evelyn” who claimed to be from “Sabio Systems Recruitment.” Evelyn offered Dena “exciting positions with numerous benefits and flexible requirements” working for a company, “Birdeye.” As with other purported “recruiters,” Evelyn asked Dena for permission to have someone else contact her via WhatsApp to share the complete details of the job.

82. That same day, Dena received a message via WhatsApp from someone calling herself “Olivia” who told her that the role was for a “Birdeye agent” and the job was “mainly to help merchants promote their low-starred products, increase product exposure, and make them visible to more people” by “click[ing] on the platform provided by the company....” Olivia told Dena that she could earn “\$100-200 a day” in salary and commissions. She also told Dena that compensation was paid in USDT and recorded on a Form-1099.

83. Olivia also conducted Dena’s training by having her work in a “training account,” for which Dena was promised a 25% commission to start her working account balance.

**1. Defendants Repeatedly Tricked Dena into Sending
Cryptocurrency to Wallets They Owned and/or Controlled**

84. Once registered and working in her own account, Defendants directed Dena to use Crypto.com, Cash App, Coinbase and Trust Wallet to purchase and send USDT in order to review products on the Birdeye platform.

85. Dena made her first deposit of 240 USDT to the platform on March 7, 2024. As with the other Victims, Dena quickly encountered “package missions” that significantly increased her recharge requirements. For example, on March 12th, Dena was required to deposit over \$20,000 worth of stablecoins, and the very next day, was instructed to deposit over \$40,000 more. On March 18th, Dena added over \$90,000 more worth of stablecoins spread out over 10 different deposits to cover her recharges. Dena used funds from her personal bank accounts to purchase a large portion of the stablecoins she deposited with the Defendants.

86. By March 21, 2024, Dena had deposited over 300,000 USDT to clear products on the platform and was led to believe she had earned substantial commissions and salary that brought her Birdeye working account balance to 400,000 USDT. That same day, when she attempted to withdraw from her working account, Olivia told Dena for the first time that she was a Diamond-tier member and had a withdrawal limit of 150,000 USDT. Olivia also told her that a full withdrawal of her working account balance required Dena to deposit 10,000 more USDT to upgrade to Premium tier, which would allow for unlimited withdrawals once Dena completed an additional set of 65 product reviews.

87. Dena demanded her money back and an end to her “never ending nightmare,” after which Birdeye’s Customer Service offered to waive the cost of the upgrade to Premium. Nevertheless, despite the “free upgrade,” Dena was never able to withdraw her money. Instead,

she received a new product set to complete, which required her to deposit 448,700.97 USDT. See Fig. 2.

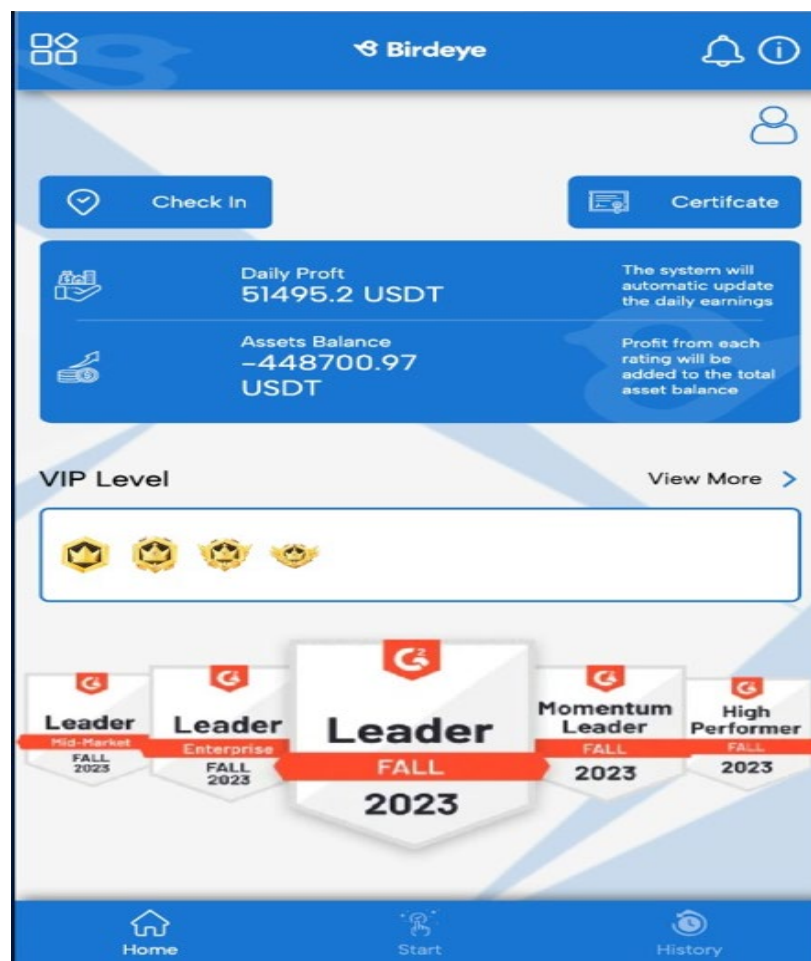


Fig. 2: Screenshot of Dena's supposed Birdeye working account showing her wallet balance and purported profits.

88. On March 21, 2024, Dena realized she had been victimized by Defendants and that her money was stolen. She stopped communicating with both Olivia and Birdeye Customer Service and reported her losses to law enforcement on March 22, 2024.

2. Defendants Steal Dena's Cryptocurrency

89. From March 2nd to March 21st, 2024, during the time she was “employed” with Defendants, Dena was deceived into purchasing \$305,954 worth of cryptocurrency and transferring all of it in the form of USDT and USDC to the Defendants.

90. Defendants instructed Dena to deposit her stablecoins into 12 Intermediary Wallets. Six of those Intermediary Wallets were also used to defraud Victim Theo, while another three were used to defraud Victim June, who are New York residents.

91. Defendants used eight of the Intermediary Wallets that Dena deposited stablecoins into to transfer a cluster of USDC to the two Transition Wallets. Two of the Intermediary Wallets transferred USDC to Transition Wallet A. Four of the Intermediary Wallets transferred USDC to Transition Wallet B. Two other Intermediary Wallets transferred USDC indirectly to Wallet B through a separate Intermediary Wallet.

92. As alleged in Paragraph 42, Transition Wallet A transferred USDC into Transition Wallet B, which then transferred USDC into Wallet 1.

93. As alleged in Paragraph 45, Defendants converted the USDC to USDT and transferred it to Wallets 2 and 3.

D. Victim Mark

94. On January 16, 2024, Victim Mark, a 30-year old engineer and resident of Virginia, received an unsolicited text message from a person named “Emma” who claimed to be a recruiter with “Insight Global.” Emma contacted Mark using a spoofed telephone number with New York state area code “585” and offered a “variety of full-time, part-time and freelance jobs.”

95. After Mark expressed interest, Emma told him that another person, “Nicholas,” would contact him within a day via WhatsApp with more details about the job.

96. Nicholas contacted Mark initially over WhatsApp, but eventually moved to another app called “Telegram.” He claimed to be an agent from “Wish” and explained that the

job was to help Wish merchants enhance their products. Nicholas told Mark he would earn a salary of \$800 every five days.

97. As with other Victims, Nicholas had Mark begin working in a training account before moving to his own working account. On January 18th, Nicholas provided Mark links to Wish's imitation site and spent much of that day training Mark on how to use the supposed work platform. Nicholas showed Mark how to review product sets, and how to make deposits to clear "negative balances to positive balances."

98. Nicholas instructed Mark to create an LBank wallet to connect to the platform and told to him to contact customer service to obtain the latest wallet address for his deposits.

1. Defendants Repeatedly Tricked Mark into Sending Cryptocurrency to Wallets They Owned and/or Controlled

99. On January 19, 2024, Nicholas told Mark to begin working in his own account and Mark used the LBank platform to purchase and send USDT to fund his account balance. Mark was able that same day to withdraw some of his supposed earnings but, by the next day, January 20th, he received a package product that required him to put the entire withdrawal back into his working account, and to purchase and deposit 200 USDT more to cover the balance of the deposit and continue working.

100. On January 23, 2024, Mark's deposit requirement increased, requiring him to spend another \$1,500. Two days later he was forced to spend another \$6,000 in order to send 5,947 USDT to complete the supposed work package in his Wish working account.

101. By January 26, 2024, after having deposited approximately \$8,150 worth of USDT, Mark received a package product that required another deposit of over 18,000 USDT. Mark told Nicholas he had "drained his savings," was unable to meet the demand, and that he wanted to withdraw his account balance. Mark also contacted Customer Service and explained

his limited financial circumstances, his need to have the money to support his family, and even his willingness to accept some loss. But Customer Service told him only that he could keep his balance in his working account until he was able to complete his product set. See Fig. 3 and 4, below.

[Remainder of Page Intentionally Left Blank.]

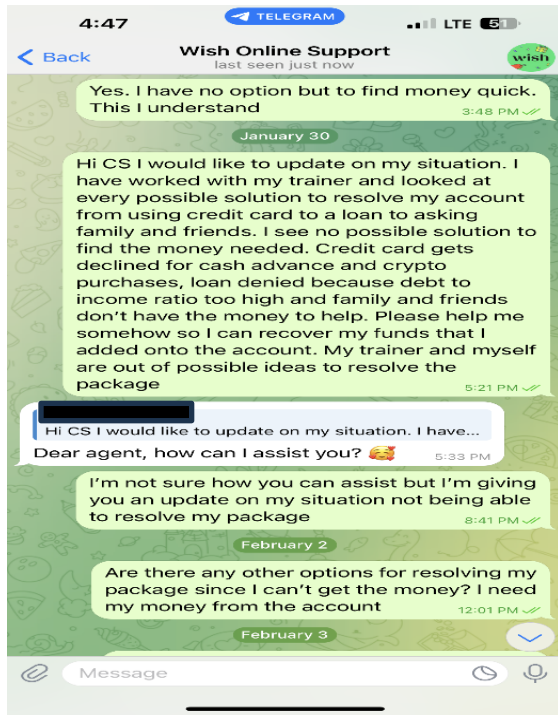


Fig. 3: Screenshot of Mark's conversation with the supposed Wish Customer Service from January 30, 2024 through February 2, 2024

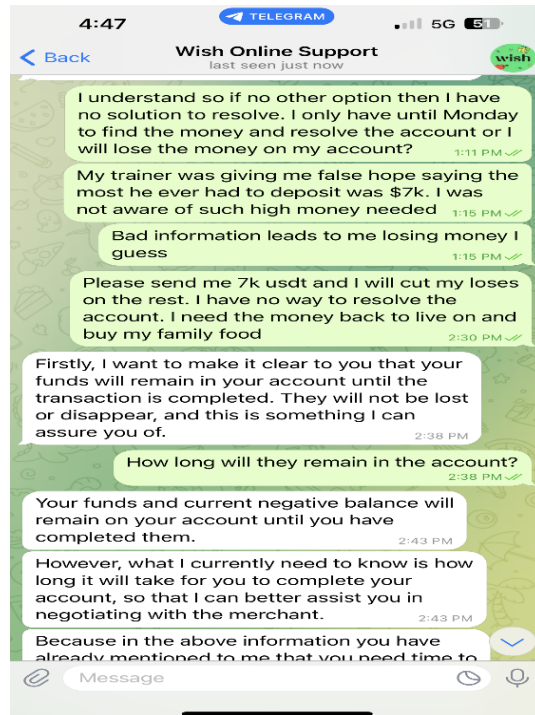


Fig. 4: Screenshot of Mark's conversation with the supposed Wish Customer Service on February 3, 2024.

102. In an effort to squeeze more stablecoins from Mark, Defendants offered to provide “extensions” throughout February to give him time to source funding. However, each extension, besides having no basis in reality, was also accompanied by fees that would only increase the amount of USDT Mark would need to deposit.

103. By March 8th, Mark was able to obtain funds to purchase and deposit USDT to cover the outstanding recharge and fees. However, on March 15th, he received another package

mission that required a new recharge of over 80,000 USDT. That day, Mark purchased and deposited another \$50,000 worth of stablecoins towards that amount, and on March 22nd, deposited more stablecoins to cover the balance and reach a point where he was led to believe he could withdraw.

104. When Mark attempted to withdraw his balance on March 22nd, Customer Service told him that he was subject to a withdrawal limit based on his membership tier, and that he had a low-credit score of 17%, which needed to be increased to 50% to obtain his funds. To boost his credit score, Defendants required Mark to deposit 1,000 USDT for every 2% he needed to raise. Between the recharge amount, membership upgrade, and credit score improvement fees, Mark deposited over \$80,000 more worth of stablecoins into the fraud.

105. To cover the costs of all of these “charges,” which exceeded \$140,000 in March alone, Mark was forced to use his tax refund, borrow money from family, and withdraw from his retirement plan.

2. Defendants Steal Mark’s Cryptocurrency

106. Between January 16, 2024 and March 22, 2024, the Defendants defrauded Victim Mark out of approximately \$157,130 worth of stablecoins. Defendants instructed Mark to deposit his stablecoins into 11 Intermediary Wallets owned and/or controlled by Defendants.

107. One of the Intermediary Wallets to which Mark deposited his stablecoins also received stablecoins from a separate Intermediary Wallet used to defraud Victims Theo, a New York resident, and Dena.

108. Defendants used two of the Intermediary Wallets that Mark deposited stablecoins into, including the Intermediary Wallet in Paragraph 107, above, to transfer a cluster of USDC into the two Transition Wallets.

109. As alleged in Paragraph 42, Transition Wallet A transferred USDC into Transition Wallet B, which then transferred USDC into Wallet 1.

110. As alleged in Paragraph 45, Defendants converted the USDC to USDT and transferred it to Wallets 2 and 3.

E. Victim Ally

111. On January 5, 2024, Ally, a naturalized U.S. citizen from Croatia, who works as a hotel receptionist and lives in Nassau County, New York, was contacted by “Chloe” who claimed to work at USA Staffing Solution. Chloe told Ally about work opportunities for people who had a social security number, bank account and who were at least 23 years old. Ally expressed interest in the opportunity and was contacted the next day on WhatsApp by a trainer named “Alexander”³ who told her she would be working as a “Task Manager for Product Ranking” for the company “Summit Digital Marketing” (“Summit”). Alex told Ally that the work involved helping “retailers and merchants give their products better rankings.”

112. On or around January 7, 2024, Alex began training Ally in Summit’s training account. Alex taught Ally the phony process for reviewing and submitting products. He also fed her the lie that she would earn commissions for submitting product data based on the posted price of the product, and that product merges—which were supposedly rare—would pay her three times as much in commissions compared to those for a single product.

1. Defendants Repeatedly Tricked Ally into Sending Cryptocurrency to Wallets They Owned and/or Controlled

113. To sell the fraud, Alex explained that Ally would be using her money to make more money and promised she would make at least 8% on a daily basis off of the amounts she

³ To avoid confusion with June’s trainer named Alexander, Ally’s trainer is hereinafter referred to as “Alex.”

deposited. Alex also promised higher earnings through bonuses and increased commission rates if Ally upgraded her status using Summit's membership tier system.

114. Alex showed Ally how to download a secure wallet through LBank and how to convert cryptocurrency she held in a Coinbase account she already possessed into USDC for use on the Summit platform. He then showed her how to "recharge" 100 USDC to her working account from the balance in Coinbase. That same day, after Ally completed a product set, Alex showed her how to withdraw her entire earnings balance of 165.76 USDT in her Summit account to her Coinbase wallet.

115. The next day, January 8th, after Ally converted other cryptocurrency in her Coinbase wallet to USDC, Alex convinced her to fund her Summit working account with 500 USDC, ostensibly to receive a 5% deposit bonus and start earning higher commissions. He promised her during the process, that "there's no loosing [sic] money... everything that we can put in we can take out once done so don't even bother yourself about that."

116. Near the end of her first week, Ally was able to withdraw approximately 1,000 in USDC to her Coinbase wallet and 3,700 USDT to her LBank wallet from her Summit working account. These were the last withdrawals Ally would ever be allowed to make. Over the next few weeks, Ally was pulled further into the fraud and ended up putting all of these amounts and much, much more right back into Summit.

117. First, Alex told Ally that she could earn a 7% bonus if she upgraded to Silver and started with 1,500 USDT in her working account. Convinced by the promises of profitability, Ally spent \$1,050 to upgrade to the Silver tier. Afterward, while working on her product sets, she received one product merge after another, leading to an onslaught of large recharge amounts she could barely satisfy. The largest recharges required her to deposit over 13,000 USDT on or

around January 12, followed by nearly 30,000 USDT on or around January 15, and finally more than 50,000 USDT on or around January 29.

118. Ally went to painful lengths to cover the recharges so she could reach a withdrawal point and extract her balance. These included depleting her available savings and borrowing more than \$30,000 from friends, family members and a co-worker that she could hardly afford to repay. Meanwhile, Defendants made Ally migrate between Coinbase, Gemini, Cash App, LBank and a Liberty X bitcoin ATM, all to ensure that she would complete her cryptocurrency purchases and transfer it to Summit.

119. During all of this, Ally was unequivocal about the negative toll Defendants' fraud was taking on her. She told Alex on January 12 that the latest recharge was "too much money to put down" and on January 13 that she "couldn't sleep...thinking about [the] current situation." On January 15, after receiving the next recharge, Ally lamented that she would need to fall behind on her mortgage and owed money to her sister to repay an earlier loan to cover the previous recharge. On January 30, after she learned of the largest recharge, Ally told Alex that people she had asked to borrow money from had refused and they warned her she was being defrauded, which she said, "broke my spirit."

120. While Ally tried to figure out how she would cover the last and largest of these recharges, Alex offered to "loan" her approximately 14,000 USDT towards it so that she could complete her product set. Once Ally began accumulating and transferring the required USDT, Alex supposedly furnished the amount he'd promised by transferring it directly to the same Intermediary Wallet Ally had used. This was followed by a corresponding, illusory "reduction" in Ally's Summit working account balance. In reality, the true purpose and net result of Alex's "generosity" was that Ally was defrauded out of another 37,000 USDT by the Defendants.

121. Finally, once Ally reached a point where she theoretically was permitted to withdraw her earnings, Defendants moved the finish line by adding new fees and creating new requirements to prevent Ally’s cryptocurrency from ever being returned to her. On February 14, 2024, Ally sought to withdraw over 100,000 USDT in “earnings” she was told she had accumulated. But Summit’s Customer Service responded that Silver tier members were subject to a 20,000 USDT withdrawal limit and recommended she upgrade to Diamond—at a cost of 10,000 more USDT— at which level her full withdrawal would be processed. When Ally tried to lower her withdrawal request to the Silver limit, Defendants told her that “once a withdrawal request has been submitted, it cannot be canceled... to ensure the security and integrity of [Summit’s] withdrawal transactions.” See Fig. 5 and 6, below.

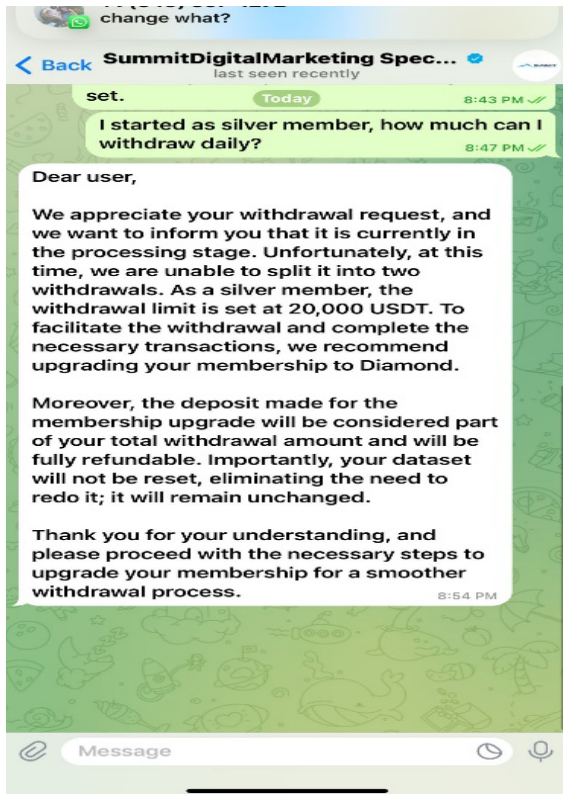


Fig. 3 Summit's messages to Ally imposing withdrawal limits.

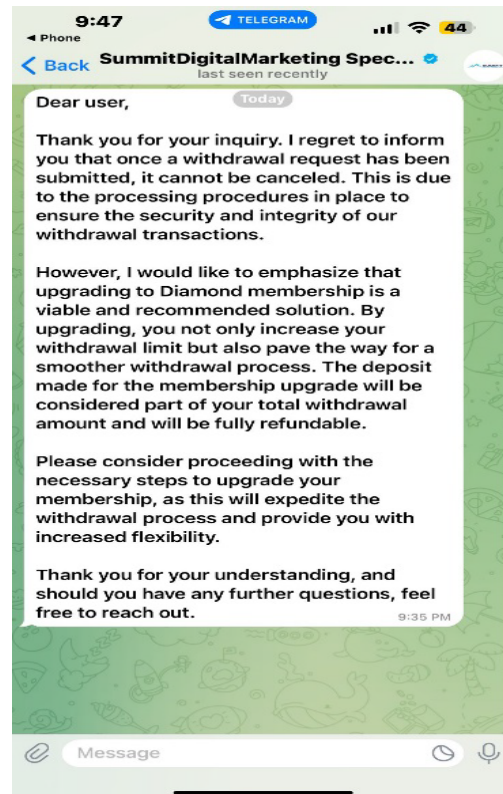


Fig. 4: Summit's messages recommending Ally "upgrade" to Diamond tier

122. Ally satisfied the amount needed to upgrade to Diamond nine days later, on February 23, 2024. Defendants responded the same day that Customer Service would process her withdrawal immediately; however, over the next few days Defendants sent additional messages incorrectly stating that Ally had upgraded only to Gold tier and telling her the withdrawal request “lacks the necessary confirmations on the blockchain.” Ally was told she could resolve this by depositing another 15,000 USDT to cover a “blockchain verification fee.” See Fig. 7-9, below.

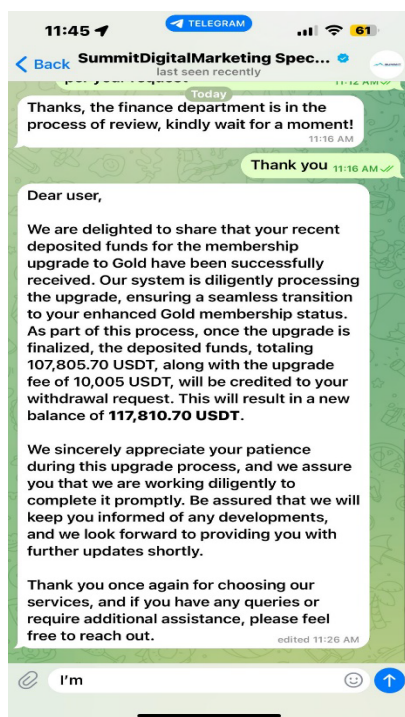


Figure 5: Summit's message confirming Ally's membership upgrade and assuring her they would process her withdrawal request.

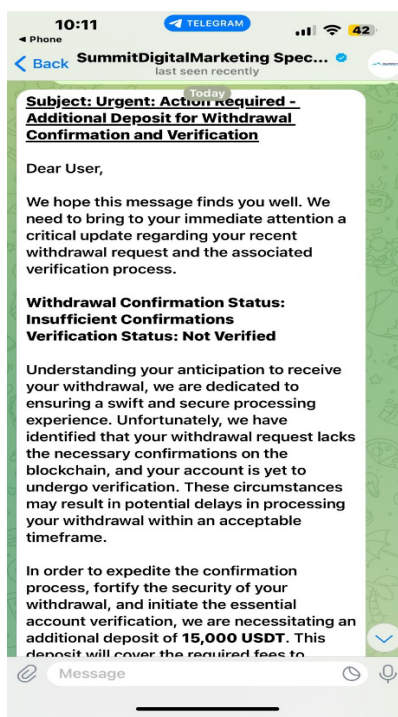


Figure 6: Summit's message telling Ally her account must undergo verification.

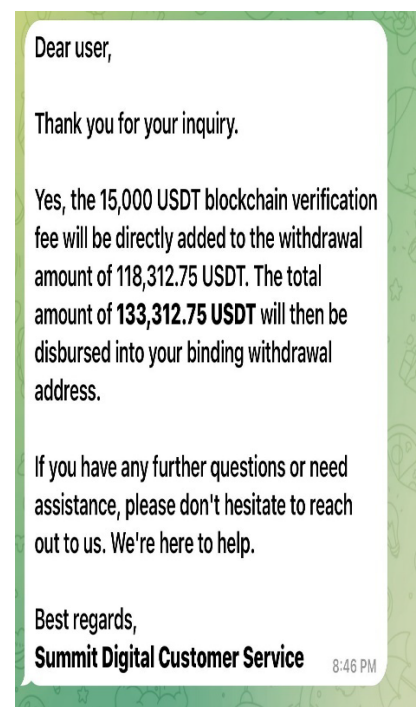


Figure 7: Summit informing Ally of the 15,000 USDT verification fee.

123. After Ally underwent additional hardship to obtain and transfer the USDT to cover the supposed “verification fee,” Defendants suddenly informed her that she needed to pay another 9,332 USDT to cover an “escrow fee.” Ally paid this as well and Defendants initially

indicated that it would process her withdrawal, but then both Customer Service and her trainer Alex simply stopped responding to Ally's WhatsApp messages.

2. Defendants Steal Ally's Cryptocurrency

124. From January 5, 2024, when she was first contacted, through May 9, 2024, when she made her last deposit into Summit, Ally purchased and transferred over \$100,000 worth of cryptocurrency to Defendants.

125. Ally deposited this amount across at least 11 different Intermediary Wallets that Defendants owned and/or controlled. Defendants used one of those Intermediary to defraud Victim Luca and two other of those Intermediary Wallets to defraud Victim Mell, both of whom are from New York.

126. Defendants used five of the Intermediary Wallets that Ally deposited stablecoins into to transfer a cluster of USDC into the two Transition Wallets.

127. In addition, Defendants transferred stablecoins from one of the five Intermediary Wallets that Ally deposited stablecoins into to another wallet, and Defendants transferred stablecoins from that wallet to Transition Wallet B.

128. As alleged in Paragraph 42, Transition Wallet A transferred USDC into Transition Wallet B, which then transferred USDC into Wallet 1.

129. As alleged in Paragraph 45, Defendants converted the USDC to USDT and transferred it to Wallets 2 and 3.

F. Victim Luca

130. On January 17, 2024, Luca, a 24-year old I.T. technician and resident of Nassau County, New York, received an unsolicited text message from a person named "Eliana" claiming to work for "Diverse Staffing" and offering remote work positions. Luca expressed interest and

allowed Eliana to share his WhatsApp contact to receive the job details. Luca was then contacted via WhatsApp by “Aria,” who claimed to be his trainer and provided him with details to work with “Page Zero Media” (“Page Zero”).

131. Luca was told the work involved helping Page Zero’s clients by driving product data and generating more exposure to “attract consumers and investors to expand their market.” Aria told Luca that he had to complete sets of product data, which “[would be dispatched] and all [he] had to do [was] submit [the] data in just one click.”

132. Aria provided Luca with a link to the supposed Page Zero website and showed him how the platform worked and how to register his working account. Aria also trained Luca to “slide and submit” data once the “system” dispatched a product with its price and explained that he would be compensated through commissions and salary, with product merges supposedly generating triple the commission.

133. Luca was told that all of his deposits to the platform would be included in his account balance along with commissions earned, and that he would be able to withdraw his deposits and his earnings after completing a product set.

1. Defendants Repeatedly Tricked Victim Luca into Sending Cryptocurrency to Wallets Defendants Owned and/or Controlled

134. Luca began working in his individual working account on January 17, 2024, using 40 USDT Aria told him he earned during his training. Aria also told Luca about Page Zero’s perks and different membership tiers, noting that Luca was starting at the Bronze level.

135. As with other Victims, Luca very soon began encountering product merges that required larger and larger deposits of stablecoins. A product merge on January 30, 2024, required Luca to deposit 1,882.03 USDT, which he was unable to complete until February 7, 2024. Immediately after making that deposit, Luca the same day received another product merge, this

time requiring an even larger deposit of 3,463.18 USDT, which Luca satisfied by withdrawing money from his brokerage account. Afterward, on February 16, 2024, Luca received yet another product merge requiring an even larger deposit of 9,072.83 USDT, which he was unable to complete until February 23, again using funds from his brokerage account.

136. Immediately after clearing the February 23 product merge, Luca immediately received another one, requiring a 32,358.03 USDT deposit. Luca immediately began trying to assemble the funds to purchase the stablecoins needed to satisfy the deposit requirement and contacted Page Zero's Customer Service about obtaining more time.

137. On or around February 26, 2024, the Federal Bureau of Investigation ("F.B.I.") called Luca and alerted him that his "employment" with Page Zero was a suspected fraudulent scheme. Luca followed up with the F.B.I. on February 28th to report his losses from the fraud.

2. Defendants Steal Luca's Cryptocurrency

138. From January 17, 2024 to February 23, 2024, Defendants deceived Luca into purchasing and depositing \$15,428.24 worth of stablecoins into their fraudulent scheme.

139. Luca deposited this amount across nine different Intermediary Wallets owned and controlled by Defendants, one of which Defendants also used to defraud Victim Mell, another New York resident. Defendants also had Luca deposit stablecoins into a separate wallet also used to defraud Mell.

140. In addition, Defendants transferred stablecoins from four of the Intermediary Wallets used to defraud Luca to the Transitions Wallets.

141. As alleged in Paragraph 42, Transition Wallet A transferred USDC into Transition Wallet B, which then transferred USDC into Wallet 1.

142. As alleged in Paragraph 45, Defendants converted the USDC to USDT and transferred it to Wallets 2 and 3.

G. Victim Mell

143. On January 11, 2024, Mell, a 31-year old teacher and resident of Queens, New York, received an unsolicited text message from a person named “Amy Christian” who claimed to be a recruiter from “Work Source Inc” and was looking to hire people for open positions at “Sachs Marketing Group” (“Sachs”). After Mell expressed interest in the opportunity, he was contacted the same day via WhatsApp by a trainer named “Anthony” who claimed to work at Sachs and supposedly was assigned to train Mell for a role as a “Platform Rating Agent.”

144. Anthony told Mell his role was to “create review[s] by giving 5-star rating[s] to low-ranked products,” and that he would earn a commission and salary of approximately \$500 to \$1,600 per week. He also told Mell that Sachs conducted all transactions in USDT, requiring Mell to create a wallet to receive his compensation. Anthony gave Mell a link to the fake Sachs website to register and create his own profile to use at the end of the mandatory training.

1. Defendants Repeatedly Tricked Victim Mell into Sending Cryptocurrency to Wallets They Owned and/or Controlled

145. Mell already had a Coinbase account when Defendants first contacted him on January 11, 2024 but Anthony instructed Mell to create another wallet on LBank to withdraw his working account balance from Sachs. After completing his supposed training, Mell began that same day to use his own working account to complete his product sets. Anthony showed Mell how to withdraw some USDT from his working account that supposedly represented his purported earnings. But, as with the other Victims, the Sachs platform quickly required him to put the withdrawn amounts right back onto the platform.

146. Anthony sent Mell links to the cryptocurrency platform paybis.com to purchase USDT to fund his account. Each time Mell had to deposit stablecoins, he contacted Sachs' Customer Service to obtain the wallet to which he would send his deposit.

147. Between January 16 and January 22, 2024, Mell was instructed to make multiple recharges to his Sachs working account totaling 26,202 USDT. Consistent with the fraudulent scheme, each recharge was bigger than the last. To fund the recharges, Mell mostly used money from his personal Chase bank account and bought USDT on LBank.

148. Anthony also had Mell create an account on Wise.com ("Wise"), a Money Service Business, which allowed Mell to send U.S. dollars directly to Sachs to cover the recharges. When Mell used Wise, Sachs' Customer Service provided him the names and email addresses of the individuals to whom he had to send the dollar amounts to cover his deposit demands. *See* Fig. 10-12 below.

[Remainder of Page Intentionally Left Blank.]

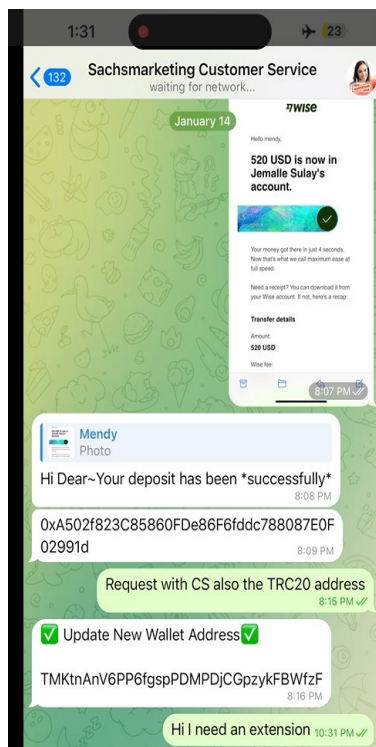


Fig. 10: Customer service telling Mell the U.S. dollars sent through Wise for Sulay was deposited to a wallet address.



Fig. 11: Customer service advising Mell before his second Wise U.S. dollar transfer.

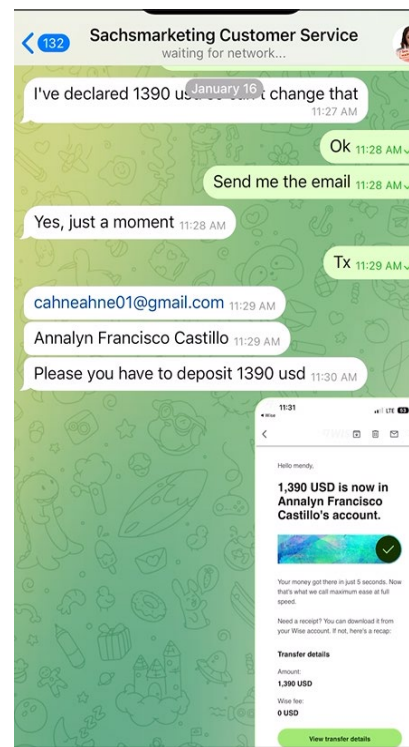


Fig. 12: Customer service providing Mell with the name and email address of the Wise recipient ahead of his second U.S. dollar deposit.

149. On January 14, 2024, Mell sent \$520 to a person using the name “Jemalle Sulay” at “sulayjemalle@outlook.com,” and \$1,390 on January 16, 2024 to a person using the name “Annalyn Francisco Castillo” at “cahneahne01@gmail.com.” See Fig. 10-12 above. On January 16, 2024, Mell received yet another recharge for \$4,300 that he covered using a third Wise transfer to someone using the name “Princess Rhaiza Maxino Tomawis” at “wise071622@gmail.com.” Each time Mell sent U.S. dollars to the names Defendants provided, Sachs’ Customer Service claimed it converted it to USDT on his behalf to cover his deposit requirements.

150. Fearing yet another recharge, Mell requested to Customer Service to withdraw his funds from the platform. Customer Service responded that Mell needed to complete two more product reviews before he could withdraw. The first of these reviews was for two products

simultaneously, referred to as a “bonus mission,” which required another recharge of 8,832 USDT, leaving Mell confused and near tears.

151. When Mell responded that he could not put any more money into the platform, Defendants offered only to extend his time to make his deposits without losing any money and also promised to “help [him] reduce the probability of getting a bonus mission.” Defendants also told Mell he would receive “bonuses” in his working account to incentivize him into making his outstanding deposits. It worked. On January 17, 2024, Mell sent another \$8,832 via Wise to a person using the name “Joymie Lynn Garcia Parinas” at “arrianesey@gmail.com” to cover the recharge for the bonus mission.

152. At Defendants’ request, Mell attempted another Wise transfer in U.S. dollars to cover another deposit but was unsuccessful. Defendants then pushed Mell to make the transfers in British pounds. When Mell proposed calling Wise to remedy his failed requests, Defendants advised him to “stop transferring money for now and let your account cool down for a while” and that he needn’t contact Wise, as Defendants would “find a way for [him].”

153. When Mell eventually insisted on contacting Wise, Customer Service told him to “always say the amount [is] to transfer to a family member and don’t let customer service ask you too many questions because there will be a lot of questions.”

154. On January 18, 2024, Wise terminated Mell’s account with a frozen balance of \$9,010.96 for exceeding the platform’s risk tolerance, with a two-to-five day waiting period before he could withdraw his funds. Defendants then urged Mell to make his deposits using wire transfers on Coinbase.

155. On January 22, 2024, Mell purchased approximately 18,835 USDC on Coinbase, which he sent to Defendants using a wallet address he received from Sachs’ Customer Service.

Despite the transfer, the USDT balance in his working account did not increase to reflect that deposit. Mell told Defendants he was “scared” and wanted to withdraw his funds.

156. In response, Customer Service told Mell he was a Diamond-level participant and needed to complete 10 more missions before he could withdraw. In addition, Mell’s working account required another deposit of 116,082 in USDT. Overcome with shock, Mell responded that he was “shaking” and needed to “go to the E.R.” because he was “about to die.”

157. To preserve Mell’s willingness to keep depositing, Defendants claimed to have “negotiated” with the product merchants to lower the amount owed by 35,000 USDT, and that Mell would only need to deposit 81,082.78 USDT. Mell countered that it was “impossible” and that he “could not even pay rent.” Customer Service then offered to lower the amount further by applying “bonuses” that Mell had earned, leaving him still responsible for a balance of over 61,000 USDT. Mell remained adamant that he was still unable to pay this amount and even sent Customer Service a screenshot of his bank account showing a negative balance of \$84.00.

158. The next day, January 23rd, Customer Service continued to negotiate with Mell, telling him that if he deposited 40,000 stablecoins, he would receive another 16,000 in bonuses that he could apply to his negative balance, and that “[f]or \$44k, [Mell] can settle the entire negative amount of the account.” Mell borrowed money to cover the reduced amount, including \$5,000 from a friend, which he used to purchase the stablecoins and transferred to Defendants on January 24th and 25th.

159. In reality, none of these bonuses or advances were real. All of these “gestures” were Defendants simply reducing the amount Mell believed he owed, leaving him to cover the difference, which meant that he kept sending stablecoins to Defendants. The net result is that Defendants defrauded Mell out of an additional over \$44,000 worth of stablecoins.

160. On January 25, 2024, believing he held 194,838.42 USDT in his Sachs working account which included approximately \$80,235.40 of his own deposits, Mell tried to withdraw his entire balance. Instead, Mell was told his withdrawal password was incorrect and that resetting his password required a 24-hour waiting period as a “platform protection mechanism.”

161. After the 24-hour waiting period, Defendants again denied Mell’s withdrawal, this time because his “account credit score” supposedly was insufficient due to the multiple deposit extensions he had been granted. To improve the score, Customer Service told Mell he needed to deposit 40% of his requested withdrawal amount—77,935.38 USDT—which would be added to his balance, resulting in a total withdrawal of 272,773.80 USDT.

162. When Mell balked at this additional deposit, Customer Service again lowered the amount through “loans” and “gifts,” bringing Mell’s deposit requirement down to 57,735.86 in stablecoins. Not wanting to lose his \$80,235.40 and still believing Customer Service’s lies, which included a promise to lend him another 28,000, Mell took out a bank loan on February 12, 2024 for \$30,000 to send to the Defendants. Shortly after, Customer Service increased the portion Mell was responsible for by another \$8,000 worth of stablecoins.

163. To keep Mell believing he would be able to withdraw his balance, Defendants sent \$30 to his LBank wallet as a “test” of the withdrawal process. However, Defendants then demanded Mell pay back 70,000 USDT in supposed loans they had sourced for him before the final withdrawal. They also told Mell they could not deduct the 70,000 USDT from his balance and that he had to send it separately. Mell was unable to deposit this latest amount and was never able to withdraw his deposits from the Sachs platform which, in total, exceeded \$100,000 worth of stablecoins.

2. Defendants Steal Mell's Cryptocurrency

164. From January 11, 2024 to March 1, 2024, Defendants defrauded Mell into purchasing and depositing \$118,535.40 worth of stablecoins into their fraudulent scheme.

165. Mell deposited this amount across nine different Intermediary wallets that Defendants owned and/or controlled. Defendants used the Intermediary Wallets and a separate wallet they instructed Mell to deposit stablecoins into to defraud fellow New York resident Luca. Mell was further instructed to send stablecoins to two other wallets that Defendants used to defraud Ally, another New York resident.

166. In addition, Defendants transferred stablecoins from seven of the Intermediary Wallets used to defraud Mell to Transition Wallet B.

167. As alleged in Paragraph 42, Transition Wallet B transferred USDC into Wallet 1.

168. As alleged in Paragraph 45, Defendants converted the USDC to USDT and transferred it to Wallets 2 and 3.

CAUSES OF ACTION FIRST CAUSE OF ACTION

Martin Act Commodities Fraud- Article 23-A of the General Business Law § 352 et seq

169. The Attorney General repeats and re-alleges the paragraphs above as if fully stated herein.

170. The stablecoins referred to herein are cryptocurrencies that constitute commodities under the Martin Act.

171. The acts and practices alleged herein violated Article 23-A of the GBL in that Defendants employed, or employs, or is about to employ any device, scheme, or artifice to defraud or for obtaining money or property by means of any false pretense, representation or promise in the issuance, exchange, purchase, sale, promotion, negotiation, advertisement,

investment advice or distribution within or from this state of commodities, and constituted fraudulent practices as defined in GBL § 352 *et seq.*

172. The acts and practices alleged herein violated Article 23-A of the GBL in that Defendants employed, or employ, or are about to employ deception, misrepresentation, concealment, suppression, fraud, false pretense or false promise in the issuance, exchange, purchase, sale, promotion, negotiation, advertisement, investment advice or distribution within or from this state of commodities, and constituted fraudulent practices as defined in GBL § 352 *et seq.*

SECOND CAUSE OF ACTION

Martin Act Commodities Fraud- Article 23-A of the General Business Law § 352-c

173. The Attorney General repeats and re-alleges the paragraphs above as if fully stated herein.

174. The acts and practices alleged herein violated GBL§ 352-c(1)(a) in that Defendants used or employed fraud, deception, concealment, suppression, or false pretense, where engaged in to induce or promote the issuance, distribution, exchange, sale, negotiation, or purchase within or from this state of commodities, as defined in GBL § 352, regardless of whether issuance, distribution, exchange, sale, negotiation or purchase resulted, and constituted fraudulent practices as defined in GBL § 352 *et seq.*

175. The acts and practices alleged herein violated GBL§ 352-c(1)(b) in that Defendants made promises or representations as to the future which were beyond reasonable expectation or unwarranted by existing circumstances where engaged in to induce or promote the issuance, distribution, exchange, sale, negotiation, or purchase within or from this state of commodities, as defined in GBL § 352, regardless of whether issuance, distribution, exchange,

sale, negotiation or purchase resulted, and constituted fraudulent practices as defined in GBL § 352 *et seq.*

176. The acts and practices of the Defendants alleged herein violated GBL§ 352-c(1)(c) in that Defendants made, or caused to be made, representations or statements which were false, where (i) they knew the truth, or (ii) with reasonable efforts could have known the truth, or (iii) made no reasonable effort to ascertain the truth, or (iv) did not have knowledge concerning the representations or statements made where engaged in to induce or promote the issuance, distribution, exchange, sale, negotiation, or purchase within or from this state of commodities, as defined in GBL § 352, regardless of whether issuance, distribution, exchange, sale, negotiation or purchase resulted, and constituted fraudulent practices as defined in GBL § 352 *et seq.*

177. The acts and practices alleged herein violated GBL§ 352-c(6) in that Defendants intentionally engaged in fraud, deception, concealment, suppression, false pretense or fictitious or pretended purchases or sales, or made material false representations or statements with intent to deceive or defraud, while engaged in inducing or promoting the issuance, distribution, exchange, sale, negotiation or purchase within or from this state of commodities, as defined in GBL § 352, and thereby wrongfully obtained property of a value in excess of two hundred fifty dollars, and constituted fraudulent practices as defined in GBL § 352 *et seq.*

THIRD CAUSE OF ACTION

Repeated and Persistent Fraud-Violation of Executive Law § 63(12)

178. The Attorney General repeats and re-alleges the paragraphs above as if fully stated herein.

179. The acts and practices of the Defendants alleged herein constitute conduct proscribed by Executive Law § 63(12), in that Defendants engaged in repeated fraudulent acts or

otherwise demonstrated persistent fraud in the carrying on, conducting, or transaction of business.

FOURTH CAUSE OF ACTION
Repeated and Persistent Illegality- Violation of Executive Law § 63(12)
(Illegality) Violations of the Martin Act

180. The Attorney General repeats and re-alleges the paragraphs above as if fully stated herein.

181. The acts and practices of the Defendants alleged herein constitute conduct proscribed by Executive Law § 63(12), in that Defendants engaged in repeated fraudulent or illegal acts in violation of GBL § 352 *et seq.*

182. Defendants' conduct constitutes repeated fraudulent or illegal acts or otherwise demonstrated persistent fraud or illegality in the carrying on, conducting or transaction of business.

FIFTH CAUSE OF ACTION
Repeated and Persistent Illegality- Violation of Executive Law § 63(12)
(Illegality) Violations of GBL § 349

183. The Attorney General repeats and re-alleges the paragraphs above as if fully stated herein.

184. GBL § 349 prohibits “[d]eceptive acts or practices in the conduct of any business, trade, or commerce or in the furnishing of any service in [New York].”

185. By virtue of their actions alleged above, Defendants have engaged in repeated and persistent violations of GBL § 349.

186. By repeatedly and persistently violating GBL § 349, Defendants have engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SIXTH CAUSE OF ACTION
Repeated and Persistent Illegality- Violation of Executive Law § 63(12)
(Illegality) Violations of GBL § 350

187. The Attorney General repeats and re-alleges the paragraphs above as if fully stated herein.

188. GBL § 350 prohibits “[f]alse advertising in the conduct of any business, trade or commerce or in the furnishing of any service in [New York].”

189. GBL § 350-a further provides that “false advertising” is advertising that is “misleading in a material aspect.”

190. By virtue of their actions alleged above, Defendants have engaged in repeated and persistent false advertising in violation of GBL § 350.

191. By repeatedly and persistently violating GBL § 350, Defendants have engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands order and judgment as follows:

1. 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, the approximately 219,840 USDC in Wallet 1 and the approximately 862,347 and 1,097,320 USDT in Wallets 2 and 3, respectively, until such time as OAG is able to take custody thereof, or arrange for Circle and Tether to transfer custody thereof, to an OAG-designated third-party;
2. Permanently enjoining Defendants from engaging in the fraudulent, deceptive, and illegal acts alleged herein and from violating the Martin Act, Article 23-A of the General

Business Law, Article 22-A of the General Business Law §§ 349 and 350 and Executive Law § 63(12);

3. Permanently enjoining Defendants from engaging in any business related to the issuance, offer, distribution, exchange, promotion, advertisement, negotiation, purchase, investment advice, or sale of commodities within or from this state;

4. Permanently enjoining Defendants from advertising to, or soliciting persons for, employment opportunities, within and from this state;

5. Permanently enjoining Defendants from sending any unsolicited text messages or other communications to New Yorkers, within and from this state;

6. Directing Defendants to make restitution of all funds they obtained from all persons harmed by fraudulent and deceptive acts fraudulent and deceptive acts and repeated fraudulent acts and persistent illegality complained of herein;

7. Directing Defendants to pay damages as well as any applicable pre-judgment interest to all persons who were directly or indirectly defrauded by Defendants' violations of the Martin Act, Article 23-A of the General Business Law, Article 22-A of the General Business Law §§ 349 and 350 and Executive Law § 63(12);

8. Directing Defendant to disgorge all amounts obtained in connection with or as a result of Defendants' violations of the Martin Act, Article 23-A of the General Business Law, Article 22-A of the General Business Law §§ 349 and 350 and Executive Law § 63(12);

9. Directing Defendants to pay a civil penalty of \$5,000 to the State of New York for each violation of Article 22-A pursuant to GBL §350-d;

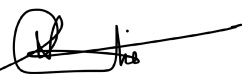
10. Directing that Defendants pay Plaintiff's costs and fees;

11. Directing such other equitable relief as may be necessary to redress Defendant's violations of New York law; and

12. Granting such other and further relief as may be just and proper.

Dated: January 9, 2025
New York, New York

LETITIA JAMES
Attorney General of the State of New York

By: 

Shantelee Christie
Jonathan Bashi
Assistant Attorneys General

Kenneth Haim
Deputy Chief, Investor Protection Bureau

Shamiso Maswoswe
Chief, Investor Protection Bureau
28 Liberty Street
New York, New York 10005
Tel.: (212) 416-8769

Counsel for the People of the State of New York

At IAS Part [] of the Supreme Court of the State of New York, held in and for the County of Queens, at the Courthouse thereof, 88-11 Sutphin Blvd, Jamaica, New York, on the ___ day of _____, 2025

PRESENT:

Honorable _____, JSC
Justice Presiding

-----X

THE PEOPLE OF THE STATE OF NEW YORK
By LETITIA JAMES,
Attorney General of the State of New York,

Plaintiff,

[PROPOSED] ORDER TO
SHOW CAUSE

-against-

Index No. _____
IAS Part _____
Hon. _____
Motion Sequence No. _____

Unknown Parties in Ownership and/or Control of
Digital Wallet Addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d,
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and
TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu,
and Unknown others,

Defendants.

-----X

Upon reading the affirmation of Assistant Attorney General Shantelee Christie together with the exhibit(s) annexed thereto (the “Affirmation”) and the accompanying memorandum of law; and upon the application of the Office of the New York State Attorney General (“OAG”) for an order permitting alternative service of process of the Summons, Complaint, this [Proposed] Order to Show Cause, the Affirmation, memorandum of law in support thereof and all documents submitted contemporaneously therewith (collectively, the “OAG Pleadings”) upon Defendants by airdropping—i.e., depositing to each of the digital wallets listed in the caption—one of three separate non-fungible tokens (“NFTs”) with each NFT to be hyperlinked to the same website containing the OAG Pleadings;

Let Defendants, or their attorneys show cause at I.A.S. Part [], Room [], of this Court, at the Courthouse, 88-11 Sutphin Blvd, Queens, New York, on the ___ day of _____, 2025, at ___:___ .M., or as soon as the parties to this proceeding may be heard why an order should not be entered herein, pursuant to CPLR § 308(5), permitting service of the OAG Pleadings upon the Defendants by airdropping one of three separate NFTs to each of the digital wallets listed in the caption, and with each NFT hyperlinked to the same website containing the OAG Pleadings; and it is further

ORDERED that service of a copy of this order together with the Summons and Complaint, Attorney Affirmation, and Exhibits annexed thereto, Memorandum of Law in support of this order, and all documents submitted contemporaneously therewith, upon the Defendants by airdropped NFTs into each of the wallets identified in the caption, with each NFT hyperlinked to the same website directing persons to the webpage wherein OAG will publish the order to show cause and the papers upon which it is based, on or before the ___ day of _____, 2025, is deemed good and sufficient service thereof. An affidavit or other proof of service shall be presented to this Court on the return date fixed above; and it is further

ORDERED that the application brought on by this order to show cause shall not be orally argued unless counsels are notified to the contrary by the Clerk of the Court.

Dated: _____, 2025
 _____, New York

ENTER

J.S.C.

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

THE PEOPLE OF THE STATE OF NEW YORK,
by LETITIA JAMES, Attorney General
of the State of New York,

Plaintiff,

- against -

ATTORNEY AFFIRMATION

Index No. _____
IAS Part _____
Assigned to Justice _____

Unknown Parties in Ownership and/or Control of
Digital Wallet Addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d,
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and
TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu,
and Unknown Others,

Defendants.

SHANTELEE CHRISTIE hereby affirms under penalties of perjury that:

1. I am an attorney admitted to practice law before the courts of New York State and an Assistant Attorney General in the Office of Letitia James, Attorney General of the State of New York (“OAG”). I am familiar with the facts and circumstances of OAG’s investigation of Defendants’ deceptive and illegal acts in violation of New York law, in perpetrating a fraudulent remote work cryptocurrency scheme. I submit this affirmation and exhibits annexed hereto (the “Affirmation”) in support of OAG’s Proposed Order to Show Cause for permission to serve i) the summons, complaint, and fee-exemption letter in this action, and ii) the Proposed Order to Show Cause with the Affirmation and memorandum of law in support thereof (collectively, the “OAG Pleadings”) upon Defendants for whom the only available and useful contact information are the cryptocurrency wallets identified in the caption. OAG specifically seeks an order permitting service of the OAG Pleadings upon Defendants by airdropping—*i.e.*, depositing to specific wallet addresses— one of three separate non-fungible tokens (“NFTs”) to the wallets.

NFTs are unique and immutable cryptographic tokens that exist on the blockchain and cannot be replicated. The NFTs will each be hyperlinked to the same website containing the OAG Pleadings.

2. In the course of my duties, I conducted an investigation into Defendants' conduct as described in the Complaint. OAG seeks to recover the following stablecoins, a type of cryptocurrency, currently frozen in wallets Defendants used to steal stablecoins from New Yorkers and individuals across the country ("Victims") via fraudulent transfers:

- Approximately 219,840 USDC stablecoins located in wallet 0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d (hereinafter "Wallet 1") and valued at \$219,840 as of January 9, 2025;
- Approximately 862,347 USDT stablecoins located in wallet TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8 (hereinafter "Wallet 2") and valued at \$862,347 as of January 9, 2025; and
- Approximately 1,098,320 USDT stablecoins located in wallet TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu (hereinafter "Wallet 3") and valued at \$1,097,320 as of January 9, 2025. (Collectively Wallet 1, Wallet 2, and Wallet 3 will be referred to as the "Wallets").

3. Unless otherwise indicated, I make this Affirmation based upon my investigation and review of documents and other evidence on file with OAG.

4. OAG cannot effect service of process upon Defendants by the means specifically enumerated in the CPLR, as it is impracticable given the facts of this case. Despite its diligent efforts, OAG has been unable to identify or locate Defendants. Instead, OAG has only been able to identify the following: i) telephone numbers Defendants used to communicate with Victims to perpetrate their scheme; ii) email addresses used to deceive one Victim into sending money to Defendants by way of a money services business; and iii) Wallets Defendants used to steal the

Victims' cryptocurrency. As detailed below, neither the telephone numbers nor the e-mail addresses have yielded any verifiable physical addresses for service.

5. Defendants stole and transferred Victims' cryptocurrency across the Wallets and used a collection of telephone numbers (the "Telephone Numbers") to send text messages and engage Victims in conversations in WhatsApp messenger chats. Cmpl. ¶¶ 20.¹ Defendants also provided one Victim with four names and associated email addresses (the "Email Addresses") to whom the Victim was instructed to send U.S. dollars. Cmpl. ¶¶ 149 and 151.

I. Defendants Continued to use the Wallets After Stealing Victims' Stablecoins

6. As part of its investigation, OAG traced stolen stablecoins to Wallets 1, 2, and 3. Defendants deceived Victims into purchasing and transferring USDC stablecoins into dozens of Intermediary Wallets,² from which more than 2 million were transferred to Transition Wallets A and B. Cmpl. ¶ 41-43. The stablecoins were then consolidated in Transition Wallet B and transferred to Wallet 1. *Id.* at 42. By April 1, 2024, over 2 million USDC was sent to Wallet 1. *Id.* at 43.

7. On and between April 2, 2024, and April 3, 2024, approximately 1,999,999 USDC was transferred from Wallet 1 to another wallet ("wallet 0x409"). After that transfer, approximately 219,840 USDC, currently valued at approximately \$219,840, remained in Wallet 1, which OAG caused to be frozen on April 5, 2024. Cmpl. ¶ 44. Defendants then used a "mixer" wallet ("wallet TB73g") on a foreign cryptocurrency platform, Bitunix, to exchange the 1,999,999 USDC for USDT. *Id.* at 45. Bitunix has no "Know Your Customer" protocol for identifying and verifying its users. *Id.*

¹ References herein to "Cmpl. ¶" refer to paragraphs within the Complaint filed against the captioned defendants: Index No. not yet assigned.

² Capitalized terms not defined herein have the meanings attributed to them in the Complaint.

8. After the exchange to USDT, Defendants transferred approximately 990,000 and 1,007,000 USDT into Wallets 2 and 3, respectively. *Id.* Defendants continued to effect USDT transactions in Wallets 2 and 3 until April 26, 2024, when OAG secured a freeze of the USDT in both Wallets. Cmpl. ¶ 46. As of April 26, 2024, approximately 862,347 USDT remains frozen in Wallet 2, and approximately 1,097,320 USDT remains frozen in Wallet 3, currently valued at approximately \$862,347 and \$1,097,320, respectively. *Id.*

9. As a part of OAG's investigation I caused a review of all activity in the Wallets since the USDC and USDT were frozen. On April 12, 2024, Defendants transferred other cryptocurrency out of Wallet 1 to a different wallet. Wallet 1 also received three NFTs via airdrop between May 3, 2024 and August 30, 2024, and received additional cryptocurrency on September 7, 2024. Defendants also transferred cryptocurrency from Wallet 2 to other wallets on April 30, 2024 and May 2, 2024 and continued to receive cryptocurrency via 62 transfers into Wallet 2 between April 30, 2024 and December 4, 2024, and 12 transfers into Wallet 3 between April 30, 2024 and September 18, 2024.

II. Defendants Used Spoofed Telephone Numbers and Sham Email Addresses to Remain Anonymous

10. In furtherance of OAG's investigation into Defendants' identity and location, I caused messages to be sent to the Telephone Numbers via SMS text message informing the message recipients that OAG intends to file an action against them and requesting a mailing address from each recipient. I additionally caused phone calls to be made to each of the Telephone Numbers. On and between December 6 and December 9-11, 2024, phone calls were made and text messages sent to 14 Telephone Numbers.

11. The majority of the Telephone Numbers either provided no response to OAG's text messages or appeared to be spoofed in that some Telephone Numbers mimicked and used

telephone numbers that were assigned to landlines, which do not natively support text messages. *See* fig. 1 below. Each Telephone Number that imitated a landline generated an automated return message to OAG’s text messages identifying those numbers as landlines. Text messages could not be delivered to those Telephone Numbers without converting them to voice messages. *See* Exhibit 1. Telephone Numbers that provided no responses to OAG’s text messages also, when called, gave varying but similar notices that said Telephone Numbers were either “disconnected” or “cannot accept calls.” *See* fig. 1. Only two of the Telephone Numbers responded to OAG’s communications and neither provided a verifiable mailing address, as requested.

Telephone Number Contacted	Result
705-535-****	Landline; only voice message feature available
343-212-****	Landline; only voice message feature available
778-924-****	Landline; only voice message feature available
579-204-****	Landline; only voice message feature available
401-364-****	Landline; only voice message feature available
415-235-****	No text reply received; not in service
249-516-****	No text reply received; call cannot be completed
203-990-****	No text reply received; “user busy” msg when called
917-640-****	No text reply received; cannot accept calls
617-304-****	No text reply received; cannot accept calls
917-553-****	No text reply received; answered call but hung up
310-593-****	No text reply received; answered call but hung up
626-492-****	“Womp Womp” text reply; not receiving calls
585-420-****	Txt reply “no longer in service”; disconnected

Figure 1: Results of OAG's text and call efforts to the Telephone Numbers.

12. OAG sent emails to the four Email Addresses on December 6, 2024 with both read receipt and delivery receipt requested. Only one Email Address, sulayjemalle@outlook.com, returned a “delivered” responses message. OAG did not receive any response from the user providing the mailing address requested. Messages OAG sent to two other Email Addresses were relayed with no delivery notification provided by the destination server. OAG’s email to the fourth Email Address, “cahneahneol@gmail.com,” was not delivered as the destination server

labeled the email address as “not found at gmail.com.” See Exhibit 2. No read receipts were received.

Email Contacted	Results
sulayjemalle@outlook.com	Received a delivery confirmation, but no reply
wise071622@gmail.com	Message relayed, but no delivery confirmation received
arrianesey@gmail.com	Message relayed, but no delivery confirmation received
cahneahneol@gmail.com	Message not delivered; address not found at gmail.com

Figure 2: Results of OAG's communication with the Email Addresses.

13. Although the Wallets, Telephone Numbers and Email Addresses used to facilitate Defendants' fraud highlight the advancement of technology as a means of modern communication, none have provided OAG with verifiable information regarding Defendants' identities and location, so it is *per se* impossible for OAG to serve Defendants using the conventional methods set forth in CPLR § 308(1) – (2), and (4), rendering personal service of process impracticable and service pursuant to CPLR § 308(5) warranted.

III. OAG's Proposed Alternative Service is Reasonably Calculated to Apprise Defendants of OAG's Action

14. Alternative service is necessary to allow OAG to pursue its claims against Defendants and recover Victims' stolen cryptocurrency. OAG seeks to airdrop—*i.e.*, deposit—one of three separate NFTs into each Wallet. Each Wallet is a pseudonymous identifier of their respective wallet-holder(s) and only those in possession of a wallet's private key—essentially a long and complex password—can access that wallet. Each NFT will contain a link to the same OAG-created website, containing copies of the OAG Pleadings. Each NFT will also have its own metadata that will include a hyperlink in the NFT name that, when clicked, will bring users to the website containing the OAG Pleadings.

15. OAG will then airdrop the NFTs to their respective wallets, ensuring that one NFT is sent directly to each of the Wallets. The airdrop process is automatic and does not require

Defendants to take action to receive the NFTs. The website, once created, will not appear on search engines because it will include a “noindex directive,” and will adhere to cybersecurity standards that will prevent visitors from altering or deleting the site.

16. The Wallets are certain to receive airdropped NFTs, which are reasonably calculated to apprise Defendants of OAG’s action. Wallet 1 is already known to have repeatedly received airdropped NFTs. *Supra* ¶ 9. OAG also plans to monitor the Wallets to ensure that each receives one of the three NFTs, log the exact date and time each NFT is clicked, and observe the website’s traffic.

17. OAG requests that the Court enter an order in the form of the Proposed Order to Show Cause permitting OAG to serve Defendants via delivery of separate NFTs to each of the Wallets, hyperlinked to the same website containing the OAG Pleadings.

18. A prior application has not been made for the relief now requested.

WHEREFORE, OAG requests that this motion be granted and any such other and further relief this Court may deem just and proper.

Dated: January 9, 2025
New York, New York

By: 

Shantelee Christie
Assistant Attorney General
Tel: 212-416-8355
shantelee.christie@ag.ny.gov

EXHIBIT 1

5:41



+90 (008) 000 42 22 >

Text Message • SMS
Today 5:29 PM

[+1579-204-0513](tel:+15792040513) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1401-364-2565](tel:+14013642565) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1401-364-2565](tel:+14013642565) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1705-535-3810](tel:+17055353810) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1343-212-2551](tel:+13432122551) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline



Text Message • SMS



5:41



+90 (008) 000 42 22 >

Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

[+1705-535-3810](tel:+17055353810) is a landline #.
Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

[+1343-212-2551](tel:+13432122551) is a landline #.
Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

[+1778-924-7495](tel:+17789247495) is a landline #.
Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

[+1778-924-7495](tel:+17789247495) is a landline #.
Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

The sender is not in your contact list.

[Report Junk](#)



Text Message • SMS



5:42



+1 (626) 492-2024 >

iMessage
Today 5:35 PM

The Office of the Attorney General of the State of New York intends to file a lawsuit against you. Please provide your mailing address and confirm whether you are willing to accept service of process through this correspondence. Please let me know if you have any questions about this message. Thank you.

Delivered

Womp womp



iMessage



5:39



+1 (585) 420-6410 >

Text Message • SMS
Today 5:32 PM

The Office of the Attorney General of the State of New York intends to file a lawsuit against you. Please provide your mailing address and confirm whether you are willing to accept service of process through this correspondence. Please let me know if you have any questions about this message. Thank you.

This phone number is no longer in service.



Text Message • SMS



EXHIBIT 2

Christie, Shantelee

From: Microsoft Outlook
To: arrianesey@gmail.com
Sent: Friday, December 6, 2024 6:21 PM
Subject: Relayed: Hello from the NY Office of the Attorney General

Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:

arrianesey@gmail.com (arrianesey@gmail.com)

Subject: Hello from the NY Office of the Attorney General



Hello from the NY
Office of th...

Christie, Shantelee

From: postmaster@outlook.com
To: sulayjemalle@outlook.com
Sent: Friday, December 6, 2024 6:13 PM
Subject: Delivered: Hello from the NY Office of the Attorney General

Your message has been delivered to the following recipients:

[sulayjemalle@outlook.com \(sulayjemalle@outlook.com\)](mailto:sulayjemalle@outlook.com)

Subject: Hello from the NY Office of the Attorney General



Hello from the NY
Office of th...

Christie, Shantelee

From: Microsoft Outlook
To: wise071622@gmail.com
Sent: Friday, December 6, 2024 6:18 PM
Subject: Relayed: Hello from the NY Office of the Attorney General

Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:

wise071622@gmail.com (wise071622@gmail.com)

Subject: Hello from the NY Office of the Attorney General



Hello from the NY
Office of th...

Christie, Shantelee

From: Microsoft Outlook
To: cahneahneo1@gmail.com
Sent: Friday, December 6, 2024 6:15 PM
Subject: Undeliverable: Hello from the NY Office of the Attorney General



Your message to cahneahneo1@gmail.com couldn't be delivered.

cahneahneo1 wasn't found at [gmail.com](https://www.gmail.com).

Shamiso.Maswoswe**Office 365****cahneahneo1****Action Required**

Recipient

Unknown To address

How to Fix It

The address may be misspelled or may not exist. Try one or more of the following:

- Send the message again following these steps: In Outlook, open this non-delivery report (NDR) and choose **Send Again** from the Report ribbon. In Outlook on the web, select this NDR, then select the link "**To send this message again, click here.**" Then delete and retype the entire recipient address. If prompted with an Auto-Complete List suggestion don't select it. After typing the complete address, click **Send**.
- Contact the recipient (by phone, for example) to check that the address exists and is correct.
- The recipient may have set up email forwarding to an incorrect address. Ask them to check that any forwarding they've set up is working correctly.
- Clear the recipient Auto-Complete List in Outlook or Outlook on the web by following the steps in this article: [Fix email delivery issues for error code 5.1.1 in Office 365](#), and then send the message again. Retype the entire recipient address before selecting **Send**.

If the problem continues, forward this message to your email admin. If you're an email admin, refer to the **More Info for Email Admins** section below.

Was this helpful? [Send feedback to Microsoft.](#)

More Info for Email Admins

Status code: 550 5.1.1

This error occurs because the sender sent a message to an email address outside of Office 365, but the address is incorrect or doesn't exist at the destination domain. The error is reported by the recipient domain's email server, but most often it must be fixed by the person who sent the message. If the steps in the **How to Fix It** section above don't fix the problem, and you're the email admin for the recipient, try one or more of the following:

The email address exists and is correct - Confirm that the recipient address exists, is correct, and is accepting messages.

Synchronize your directories - If you have a hybrid environment and are using directory synchronization make sure the recipient's email address is synced correctly in both Office 365 and in your on-premises directory.

Errant forwarding rule - Check for forwarding rules that aren't behaving as expected. Forwarding can be set up by an admin via mail flow rules or mailbox forwarding address settings, or by the recipient via the Inbox Rules feature.

Mail flow settings and MX records are not correct - Misconfigured mail flow or MX record settings can cause this error. Check your Office 365 mail flow settings to make sure your domain and any mail flow connectors are set up correctly. Also, work with your domain registrar to make sure the MX records for your domain are configured correctly.

For more information and additional tips to fix this issue, see [Fix email delivery issues for error code 550 5.1.1 in Office 365.](#)

Original Message Details

Created Date: 12/6/2024 11:15:26 PM
Sender Address: Shamiso.Maswoswe@ag.ny.gov
Recipient Address: cahneahneo1@gmail.com
Subject: Hello from the NY Office of the Attorney General

Error Details

Error: *550-5.1.1 The email account that you tried to reach does not exist. Please try 550-5.1.1 double-checking the recipient's email address for typos or 550-5.1.1 unnecessary spaces. For more information, go to 550 5.1.1 <https://support.google.com/mail/?p=NoSuchUser41be03b00d2f7-7fd157f4100si5473082a12.744> - gsmtip*

Message rejected by: mx.google.com

Notification Details

Sent by: MW4PR09MB9219.namprd09.prod.outlook.com

Message Hops

HOP	TIME (UTC)	FROM	TO	WITH
1	12/6/2024 11:15:26 PM	SJ0PR09MB9222.namprd09.prod.outlook.com	SJ0PR09MB9222.namprd09.prod.outlook.com	mapi
2	12/6/2024 11:15:26 PM	SJ0PR09MB9222.namprd09.prod.outlook.com	MW4PR09MB9219.namprd09.prod.outlook.com	Microsoft SMTP Server cipher=TLS_ECDHE_R

Original Message Headers

ARC-Seal: i=1; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=none;

b=yNNRIq8cWbF0uc4wWgSjj21/yxauWwqaIqH/6xTnYMP2+UHNPF/hdlHGcqb21mJ81VdjT7Z0kkiwlWzdmILsA5RjxMEFMEo8j+myyZOPHkm4AK0mqlvgMXDcyuetPa4i3U3HD0xw35s1eeQjIsEidjGLEEBES4mCmSWk9pGN0FuGIx5tBjbv9SsSvEwwLwV6+ldTFhrIlGlJPDliWtoeu97n28mIgzUltPulKMERTUUYxckN4/k6CmGagVTX2TCprPckT2nER8tedyGwJdgt7ulxydmkfEbfslg/+IfVys5fz7py+fKXjFY3s7Qh5Z5zMmh2kQYJ7JbDnWLF5cF+g==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector10001;

h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1;

bh=bVQ/4OqFQppQ3cu9FJyWCmDn+4O8G1oIQB9L+KIavPc=;

b=TvR8E+zBBnkf3NuKPoBeJretRJKcIjN9n/6rv+SfOUdOn0yKXyFQQoCTDDJIQQTgrpp9YsimhrUuY5gdbjAJkjxq0fEEyZJRHZSXPAOWLVB41xdU1BmWh2NxLtPEdWTJc0iA0Re7VtqpH62r16IuSDnaLXvcn+dd/InzEYMnzCWENYYyb+6oz97683xaMuirWUmwmOKNP0d+pO6eZ947rcoUWSJC+fY/I+P8YJaGGUd3ZrnAZdWK4P55RHi07OuFb0abvWVbkbfbvw8yc7QooK8G/mSwpqVOQ3mPcrlqwbxQY1eKpGZbJU1RdaaG2xYOcHFk8SfrqsQQ3XOmVxs4A==

ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass smtp.mailfrom=ag.ny.gov; dmarc=pass action=none header.from=ag.ny.gov; dkim=pass header.d=ag.ny.gov; arc=none

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=ag.ny.gov; s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=bVQ/4OqFQppQ3cu9FJyWCmDn+4O8G1oIQB9L+KIavPc=;

b=gWZ3FCwvxNGY0ZjP5z/BSm0Lt/rhb9ZYWhKDJ+XqIcmS/W7Rv1FHXP33jvfUA1/bNBpkIZQuD9pWyu4A+iU8PHB6exSvslKQE3GWclmskSueB1cN5Cya2J+yFy4RcwhPADEOpvxvE/5kzeqjzE8dn/JmN1zx+u/k/rk+Et8eyZQ=

Received: from SJ0PR09MB9222.namprd09.prod.outlook.com (2603:10b6:a03:447::7) by MW4PR09MB9219.namprd09.prod.outlook.com (2603:10b6:303:1e7::17) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8230.12; Fri, 6 Dec 2024 23:15:26 +0000

Received: from SJ0PR09MB9222.namprd09.prod.outlook.com

([fe80::ab50:8672:a715:beeb]) by SJ0PR09MB9222.namprd09.prod.outlook.com ([fe80::ab50:8672:a715:beeb%3]) with mapi id 15.20.8230.010; Fri, 6 Dec 2024 23:15:26 +0000

From: "Maswoswe, Shamiso" <Shamiso.Maswoswe@ag.ny.gov>
To: "cahneahneol@gmail.com" <cahneahneol@gmail.com>
Subject: Hello from the NY Office of the Attorney General
Thread-Topic: Hello from the NY Office of the Attorney General
Thread-Index: AdtINLcEjXbTVITvQk+6lXvwMZl90w==
Disposition-Notification-To: "Maswoswe, Shamiso" <Shamiso.Maswoswe@ag.ny.gov>
Return-Receipt-To: <Shamiso.Maswoswe@ag.ny.gov>
Date: Fri, 6 Dec 2024 23:15:26 +0000

Message-ID: <SJ0PR09MB922232B374D246F851DCCD0BDF312@SJ0PR09MB9222.namprd09.prod.outlook.com>

Accept-Language: en-US

Content-Language: en-US

X-MS-Has-Attach:

X-MS-TNEF-Correlator:

authentication-results: dkim=none (message not signed) header.d=none;dmarc=none action=none header.from=ag.ny.gov;

x-ms-publictraffictype: Email

x-ms-traffictypediagnostic: SJ0PR09MB9222:EE_|MW4PR09MB9219:EE_

x-ms-office365-filtering-correlation-id: ee0173bf-4ab5-4984-b681-08dd164bde1d

x-ms-exchange-senderadcheck: 1

x-ms-exchange-antispam-relay: 0

x-microsoft-antispam: BCL:0;ARA:13230040|366016|1800799024|8096899003|38070700018;

x-microsoft-antispam-message-info: =?us-

ascii?Q?Wxiqi8q1CWelEUily0KfaIq4SxjmUnw2zdG8Pv8LzUPGLkhLPOJ95W9t+/EA?=
=?us-ascii?Q?gGeSnOS6esSJDx9IJjOwQ0zLr0sRgn1Knm14vVeW9ztuMZ0AJHO1SzOv9Wn?=
=?us-ascii?Q?tviS4nj3Rr1+CKdcouGdwuCM91GgKvf4gmFIRr8nWl1ftekj5zyzYQNsEJmk?=
=?us-ascii?Q?DfPAKbhk1xcKH3nFS06xbftb+TiPIJZlqhzWwuZSLyn5P0VMOH1BgtOVdNcU?=
=?us-ascii?Q?VxwklLOXfmuZMrPKn5n+/FfeBgwh0ONtAoTbFIKnpUc0CBMa2gbvB8ak0bLA?=
=?us-ascii?Q?u6teInyHmOhc/LOA+1ROOmW4GwoaLv5qr+cjvKPbpQ9kcCpYHVPYxSH7AxJf?=
=?us-ascii?Q?3PvwdRn0sgYxL2FaC3tflK6KGzeXjpfq2QjLAZc0NucBUoZnHflBhXuH1r7M?=
=?us-ascii?Q?1zDh7JvvNxqCGY1yntlOgtJ8/QE7Zn7OF7c+bhirva6ULLNI61Hj/+3HD69d?=
=?us-ascii?Q?/XpfpYpsJ+rrNGrZd618yLLuwJnadTrE/Zclee90OTMoA60238HH4vY/tQNJ?=
=?us-ascii?Q?atSNDyERhWu7saN+vfoOJS8pb/YylZXcJOSxhnUdm0SeMMmNRYT9bgAcCfIc?=
=?us-ascii?Q?fM5JF8OpcxekHa4DjvLfp0s5iEPW06+CeN3IrxpCp9NEHmOTgDKYl9pXI09L?=
=?us-ascii?Q?4PrRD4F3W9IESKTMOSiL/ohxFP641w1pBLuvEmT89HFEb3Ddj6nxdqFd0Y1j?=
=?us-ascii?Q?DJotkNGR1mfoWSE7pbP5YbJqQDjkb9ejg+f5n4d87JUvW0yGcKBI+XXEvEaM?=
=?us-ascii?Q?o9q16Sa7bEOpOKH7fFSbyDW8eQh1zS6Uy0C4unZV7xl2rMTq8X8r01AmlGbo?=
=?us-ascii?Q?Q3WnwosiIFZ44VBM8FGaOAuKa2L8hAGpVW2snGWycIUyyNyHWRpdrRNC+GLv?=
=?us-ascii?Q?TQaYh5AIsXTWQq8q1j0WM57KEV0gSUG9IY9aGKhYp5weYREcBaOgGsxwaKxo?=
=?us-ascii?Q?0iXRyhWBc4DscwgWUP1NEj10yRpy6HpMQN/Qk/q1toSt4eLsXC/X/lZfxjCq?=
=?us-ascii?Q?ACqYDsLtkMM82A65OeBeRg+Bc9cKJjnHODK05+Zf0gHH3DjfvzP0a64svFqM?=
=?us-ascii?Q?L79sz5qQ96P2RYZ74rYJH2nY3G41hZx55JFv9eUT15zi7p/PHNYUoAfr1DFG?=
=?us-ascii?Q?nU+NCX0WBauzkgYD8ntp00EKuVaGF/n2vfHoQbcXiGH3ut++RUHA+0koigxq?=
=?us-ascii?Q?/ROBaa7oGh5MyHst7LCpflpfp01+JjDTqJ7ux0CYArWOAzfWNTOSln9HAt55?=-

=?us-ascii?Q?wTIE/y5qMpKW2knjFLOYuGXMYcFj0V9HjWJXe17ujHsyinPiAV5Pr68w+Yr5?=
=?us-ascii?Q?3whMT8yMPTJPZpU8N40AwmKoFxy0waMR8qf0homwNhIFyR3K0xrpkmq+YlFM?=
=?us-ascii?Q?lEyRq4jHgtVMfZ1ug21B+aUQed4K6SkpRkutgH/jGx0I4ZG1qw=3D=3D?=
x-forefront-antispam-report:

CIP:255.255.255.255; CTRY:; LANG:en; SCL:1; SRV:; IPV:NLI; SFV:NSPM; H:SJ0PR09MB9222.namprd09.pr
od.outlook.com; PTR:; CAT:NONE; SFS:(13230040)(366016)(1800799024)(8096899003)(38070700018);
DIR:OUT; SFP:1101;

x-ms-exchange-antispam-messagedata-chunkcount: 1

x-ms-exchange-antispam-messagedata-0: =?us-

ascii?Q?8DpjWpaxa3uIqWBipmBuCo9pOp25CplX6fbB4dJ401BSODV8GHVO/3MR4R0X?=
=?us-ascii?Q?OP0mitXZowVbhCiITdPlwWjpAke0sSZHehMl9FGAbWLQyhiND2Xgy+kZsNmC?=
=?us-ascii?Q?ezodrRLRWlgFCd9q07oaJQheerGBbt15oZjBwbuaEwppQxPjDppsaK9VlL3e?=
=?us-ascii?Q?rMGumULfrXwJWAIGS/W6dCA5zUVclU9sgYoz1Q2IW29wR9UTxciwMo5CMEhc?=
=?us-ascii?Q?xsOsNA7mgCw+hg62uRZ5Kqavt2FG1jRup+bd0zGQC/H4oWdM6CJ9tLDYSyW1?=
=?us-ascii?Q?cMiXmWKORmBq+ImaUmMAwTPK5gvPbycKvJ7xQPdQjYr+p6ZxgoaC/A2ZVvO1?=
=?us-ascii?Q?IgHukms4RIHqKUszXCPlYaF6NL0oKohBIerDoEa4BAhhFZLcuY2tBD0RP8rZ?=
=?us-ascii?Q?mG9wqjPeOc6T2kYpR8abCZihWkZ3/lmpMbtbHu1SB115udSqkje2/IbARYa8?=
=?us-ascii?Q?n9qWN0YPYGjJVzYwFGUj2DHmJSzJRM0TDR07GENCFH7QDfYjLsDlu/1qjRrJ?=
=?us-ascii?Q?M4103zCpZQ84P+UiwG4nez4ZGxxiC0WXvWmL6wHBvWYDutFU+zYsCop+1YDe?=
=?us-ascii?Q?4fxFyVnMZeJME83fSeilt0ynrwlYEsj4iYf713XfCbYYREvUlmxDvnETbh2n?=
=?us-ascii?Q?8SASPCAsX6fEu32hB8VjJXQPNHpL9qkW5/n6lBk22I5u+5gbdpb91dic92n3?=
=?us-ascii?Q?CwtqScP9Se2uKodUHiSOW21E194jz38fWybHTA64000nvq82b6e6uoYOMgPL?=
=?us-ascii?Q?KWuozkG1fhqP4X4h3v2RwwekB8C6gK4nwtS6PplgewgKAKw5OGmkPNbsgk69?=
=?us-ascii?Q?g2V7ELnAg8NZ+PU1ZSuvEWlVblbXexrQkGo7EQoELtKb8ZqTVwAL0Q0GW1BL?=
=?us-ascii?Q?NgqthIuVdtOrF2nmcRiGmln3XgVSWz04AFyJNA7JnxVwoBQyhob+nKoagVTv?=
=?us-ascii?Q?B5bga/ih0e4+Kw5gP4xwkn04d3A10yPMCCqdZaLyFI4c1Spepr+pGAFPH4yg?=
=?us-ascii?Q?nDwFl4nvp6L+QL7EErcihxwTcoVJmNQVQz07DGJz1qaAusVf6UUH50ISeGpe?=
=?us-ascii?Q?d6Fgcb7d4cMPKN4IPWvG1103B1BzMkZDkz6iRoNjLhBkrKDgDJK6vVACW4q?=
=?us-ascii?Q?co8JVH1NsM8LOIsG3gqDdpKIxzJTPw+yICzYPFLH7IGECadEE4CHSTUW2n79?=
=?us-ascii?Q?/ImOyMfr4rm559gQgWT5JTG1+1ndMr32c0qdfQ+7wHQbbLrbiu2JuUuCAb5A?=
=?us-ascii?Q?J/uv9bLh5sMdvMJ9+8zdz+16ZkVwoTvrwk2VqXe7TU10/vlKT8Q0r+j569zZ?=
=?us-ascii?Q?j6Ho5EsMJaiIoKEihU1+vCDYSJYJDcoPRrWNzrdMVK/MWwK7zxDoRmcTrrzM?=
=?us-ascii?Q?f82MONTedCrfCkblL+93Q6oPycA/WPRaT/ycAdVZuluIwvllRRtMxh7QC+fu?=
=?us-ascii?Q?UNaXEIdeTI50KVvJ1jFsTeuaKUjU5xsZ3aoa1UPUL2ZqdCfB4EYpgyTjSNrn?=
=?us-ascii?Q?hf6XiAIwRm01749rHCSjFSaXWfw+w6IXwnLQh5XTagYzyNcFKrgh96vZomRN?=
=?us-ascii?Q?qtCnyQ61SJJbk/C15gFu5xc9vF5s1fpyENi4eYyF01Mo9GbQca9CmN0whPWj?=
=?us-ascii?Q?3Q=3D=3D?=
Content-Type: multipart/alternative;

boundary="_000_SJ0PR09MB922232B374D246F851DCCD0BDF312SJ0PR09MB9222nampr_"

MIME-Version: 1.0

X-OriginatorOrg: ag.ny.gov

X-MS-Exchange-CrossTenant-AuthAs: Internal

X-MS-Exchange-CrossTenant-AuthSource: SJ0PR09MB9222.namprd09.prod.outlook.com

X-MS-Exchange-CrossTenant-Network-Message-Id: ee0173bf-4ab5-4984-b681-08dd164bde1d

X-MS-Exchange-CrossTenant-originalarrivaltime: 06 Dec 2024 23:15:26.0785

(UTC)

X-MS-Exchange-CrossTenant-fromentityheader: Hosted

X-MS-Exchange-CrossTenant-id: f0e46024-97df-431a-80d6-c0e744fd7a39

X-MS-Exchange-Transport-CrossTenantHeadersStamped: MW4PR09MB9219

EXHIBIT 1

5:41



+90 (008) 000 42 22 >

Text Message • SMS
Today 5:29 PM

[+1579-204-0513](tel:+15792040513) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1401-364-2565](tel:+14013642565) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1401-364-2565](tel:+14013642565) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1705-535-3810](tel:+17055353810) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline

[+1343-212-2551](tel:+13432122551) is a landline #.
Reply Y to send all TXT messages
to this # as voice messages for
0.25/msg.+ std msg fee. Details @
vtext.com, TexttoLandline



Text Message • SMS



5:41



+90 (008) 000 42 22 >

Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

[+1705-535-3810](tel:+17055353810) is a landline #. Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

[+1343-212-2551](tel:+13432122551) is a landline #. Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline


[+1778-924-7495](tel:+17789247495) is a landline #. Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

[+1778-924-7495](tel:+17789247495) is a landline #. Reply Y to send all TXT messages to this # as voice messages for 0.25/msg.+ std msg fee. Details @ vtext.com, TexttoLandline

The sender is not in your contact list.

[Report Junk](#)



Text Message • SMS 

5:42



+1 (626) 492-2024 >

iMessage
Today 5:35 PM

The Office of the Attorney General of the State of New York intends to file a lawsuit against you. Please provide your mailing address and confirm whether you are willing to accept service of process through this correspondence. Please let me know if you have any questions about this message. Thank you.

Delivered

Womp womp



iMessage



5:39



+1 (585) 420-6410 >

Text Message • SMS
Today 5:32 PM

The Office of the Attorney General of the State of New York intends to file a lawsuit against you. Please provide your mailing address and confirm whether you are willing to accept service of process through this correspondence. Please let me know if you have any questions about this message. Thank you.

This phone number is no longer in service.



Text Message • SMS



EXHIBIT 2

Christie, Shantelee

From: Microsoft Outlook
To: arrianesey@gmail.com
Sent: Friday, December 6, 2024 6:21 PM
Subject: Relayed: Hello from the NY Office of the Attorney General

Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:

arrianesey@gmail.com (arrianesey@gmail.com)

Subject: Hello from the NY Office of the Attorney General



Hello from the NY
Office of th...

Christie, Shantelee

From: postmaster@outlook.com
To: sulayjemalle@outlook.com
Sent: Friday, December 6, 2024 6:13 PM
Subject: Delivered: Hello from the NY Office of the Attorney General

Your message has been delivered to the following recipients:

[sulayjemalle@outlook.com \(sulayjemalle@outlook.com\)](mailto:sulayjemalle@outlook.com)

Subject: Hello from the NY Office of the Attorney General



Hello from the NY
Office of th...

Christie, Shantelee

From: Microsoft Outlook
To: wise071622@gmail.com
Sent: Friday, December 6, 2024 6:18 PM
Subject: Relayed: Hello from the NY Office of the Attorney General

Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server:

wise071622@gmail.com (wise071622@gmail.com)

Subject: Hello from the NY Office of the Attorney General



Hello from the NY
Office of th...

Christie, Shantelee

From: Microsoft Outlook
To: cahneahneo1@gmail.com
Sent: Friday, December 6, 2024 6:15 PM
Subject: Undeliverable: Hello from the NY Office of the Attorney General



Your message to cahneahneo1@gmail.com couldn't be delivered.

cahneahneo1 wasn't found at [gmail.com](https://www.gmail.com).

Shamiso.Maswoswe**Office 365****cahneahneo1****Action Required**

Recipient

Unknown To address

How to Fix It

The address may be misspelled or may not exist. Try one or more of the following:

- Send the message again following these steps: In Outlook, open this non-delivery report (NDR) and choose **Send Again** from the Report ribbon. In Outlook on the web, select this NDR, then select the link "**To send this message again, click here.**" Then delete and retype the entire recipient address. If prompted with an Auto-Complete List suggestion don't select it. After typing the complete address, click **Send**.
- Contact the recipient (by phone, for example) to check that the address exists and is correct.
- The recipient may have set up email forwarding to an incorrect address. Ask them to check that any forwarding they've set up is working correctly.
- Clear the recipient Auto-Complete List in Outlook or Outlook on the web by following the steps in this article: [Fix email delivery issues for error code 5.1.1 in Office 365](#), and then send the message again. Retype the entire recipient address before selecting **Send**.

If the problem continues, forward this message to your email admin. If you're an email admin, refer to the **More Info for Email Admins** section below.

Was this helpful? [Send feedback to Microsoft.](#)

More Info for Email Admins

Status code: 550 5.1.1

This error occurs because the sender sent a message to an email address outside of Office 365, but the address is incorrect or doesn't exist at the destination domain. The error is reported by the recipient domain's email server, but most often it must be fixed by the person who sent the message. If the steps in the **How to Fix It** section above don't fix the problem, and you're the email admin for the recipient, try one or more of the following:

The email address exists and is correct - Confirm that the recipient address exists, is correct, and is accepting messages.

Synchronize your directories - If you have a hybrid environment and are using directory synchronization make sure the recipient's email address is synced correctly in both Office 365 and in your on-premises directory.

Errant forwarding rule - Check for forwarding rules that aren't behaving as expected. Forwarding can be set up by an admin via mail flow rules or mailbox forwarding address settings, or by the recipient via the Inbox Rules feature.

Mail flow settings and MX records are not correct - Misconfigured mail flow or MX record settings can cause this error. Check your Office 365 mail flow settings to make sure your domain and any mail flow connectors are set up correctly. Also, work with your domain registrar to make sure the MX records for your domain are configured correctly.

For more information and additional tips to fix this issue, see [Fix email delivery issues for error code 550 5.1.1 in Office 365.](#)

Original Message Details

Created Date: 12/6/2024 11:15:26 PM
Sender Address: Shamiso.Maswoswe@ag.ny.gov
Recipient Address: cahneahneo1@gmail.com
Subject: Hello from the NY Office of the Attorney General

Error Details

Error: *550-5.1.1 The email account that you tried to reach does not exist. Please try 550-5.1.1 double-checking the recipient's email address for typos or 550-5.1.1 unnecessary spaces. For more information, go to 550 5.1.1 <https://support.google.com/mail/?p=NoSuchUser41be03b00d2f7-7fd157f4100si5473082a12.744> - gsmtip*

Message rejected by: mx.google.com

Notification Details

Sent by: MW4PR09MB9219.namprd09.prod.outlook.com

Message Hops

HOP	TIME (UTC)	FROM	TO	WITH
1	12/6/2024 11:15:26 PM	SJ0PR09MB9222.namprd09.prod.outlook.com	SJ0PR09MB9222.namprd09.prod.outlook.com	mapi
2	12/6/2024 11:15:26 PM	SJ0PR09MB9222.namprd09.prod.outlook.com	MW4PR09MB9219.namprd09.prod.outlook.com	Microsoft SMTP Server cipher=TLS_ECDHE_R

Original Message Headers

ARC-Seal: i=1; a=rsa-sha256; s=arcselector10001; d=microsoft.com; cv=none;

b=yNNRIq8cWbF0uc4wWgSjj21/yxauWwqaIqH/6xTnYMP2+UHNPF/hdlHGcqb21mJ81VdjT7Z0kkiwlWzdmILsA5RjxMEFMEo8j+myyZOPHkm4AK0mqlvgMXDcyuetPa4i3U3HD0xw35s1eeQjIsEidjGLEEBES4mCmSWk9pGN0FuGIx5tBjbbv9SsSvEwwLwV6+ldTFhrIlG1JPDliWtoeu97n28mIgzUltPulKMERTUUYxckN4/k6CmGagVTX2TCprPckT2nER8tedyGwJdgt7ulxydmkfEbfslg/+IfVys5fz7py+fKXjFY3s7Qh5Z5zMmh2kQYJ7JbDnWLF5cF+g==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector10001;

h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1;

bh=bVQ/4OqFQppQ3cu9FJyWCmDn+4O8G1oIQB9L+KIavPc=;

b=TvR8E+zBBnkf3NuKPoBeJretRjKcIjN9n/6rv+SfOUdoN0yKXyFQQoCTDDJIQQTgrpp9YsimhrUuY5gdbjAJkjxq0fEEyZJRHZSXPAOWLvb41xdU1BmWh2NxLtPEdWTJc0iA0Re7VtqpH62r16IuSDnaLXvcn+dd/InzEYMnzCWENYYyb+6oz97683xaMuirWUmwmOKNP0d+pO6eZ947rcoUWSJC+fY/I+P8YJaGGUd3ZrnAZdWK4P55RHi07OuFb0abvwVbkbfbvw8yc7QooK8G/mSwpqVOQ3mPcrlqwbxQY1eKpGZbJU1RdaaG2xYOcHFk8SfrqsQQ3XOmVxs4A==

ARC-Authentication-Results: i=1; mx.microsoft.com 1; spf=pass smtp.mailfrom=ag.ny.gov; dmarc=pass action=none header.from=ag.ny.gov; dkim=pass header.d=ag.ny.gov; arc=none

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=ag.ny.gov; s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=bVQ/4OqFQppQ3cu9FJyWCmDn+4O8G1oIQB9L+KIavPc=;

b=gWZ3FCwvxNGY0ZjP5z/BSm0Lt/rhb9ZYWhKDjXqIcmS/W7Rv1FHxPh33jvfUA1/bNBpkIZQuD9pWyu4A+iU8PHB6exSvslkQE3GWclmskSueB1cN5Cya2J+yFy4RcwhPADEOpvxvE/5kzeqjzE8dn/JmN1zx+u/k/rk+Et8eyZQ=

Received: from SJ0PR09MB9222.namprd09.prod.outlook.com (2603:10b6:a03:447::7) by MW4PR09MB9219.namprd09.prod.outlook.com (2603:10b6:303:1e7::17) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8230.12; Fri, 6 Dec 2024 23:15:26 +0000

Received: from SJ0PR09MB9222.namprd09.prod.outlook.com

([fe80::ab50:8672:a715:beeb]) by SJ0PR09MB9222.namprd09.prod.outlook.com
([fe80::ab50:8672:a715:beeb%3]) with mapi id 15.20.8230.010; Fri, 6 Dec 2024
23:15:26 +0000

From: "Maswoswe, Shamiso" <Shamiso.Maswoswe@ag.ny.gov>
To: "cahneahneol@gmail.com" <cahneahneol@gmail.com>
Subject: Hello from the NY Office of the Attorney General
Thread-Topic: Hello from the NY Office of the Attorney General
Thread-Index: AdtINLcEjXbTVITvQk+6lXvwMZl90w==
Disposition-Notification-To: "Maswoswe, Shamiso" <Shamiso.Maswoswe@ag.ny.gov>
Return-Receipt-To: <Shamiso.Maswoswe@ag.ny.gov>
Date: Fri, 6 Dec 2024 23:15:26 +0000

Message-ID:
<SJ0PR09MB922232B374D246F851DCCD0BDF312@SJ0PR09MB9222.namprd09.prod.outlook.com>

Accept-Language: en-US

Content-Language: en-US

X-MS-Has-Attach:

X-MS-TNEF-Correlator:

authentication-results: dkim=none (message not signed)
header.d=none;dmarc=none action=none header.from=ag.ny.gov;

x-ms-publictraffictype: Email

x-ms-traffictypediagnostic: SJ0PR09MB9222:EE_|MW4PR09MB9219:EE_

x-ms-office365-filtering-correlation-id: ee0173bf-4ab5-4984-b681-08dd164bde1d

x-ms-exchange-senderadcheck: 1

x-ms-exchange-antispam-relay: 0

x-microsoft-antispam: BCL:0;ARA:13230040|366016|1800799024|8096899003|38070700018;

x-microsoft-antispam-message-info: =?us-

ascii?Q?Wxiqi8q1CWelEUily0KfaIq4SxjmUnw2zdG8Pv8LzUPGLkhLPOJ95W9t+/EA?=
=?us-ascii?Q?gGeSnOS6esSJDx9IJjOwQ0zLr0sRgn1Knm14vVeW9ztuMZ0AJHO1SzOv9Wn?=
=?us-ascii?Q?tviS4nj3Rr1+CKdcouGdwuCM91GgKvf4gmFIRr8nWl1ftekj5zyzYQNsEJmk?=
=?us-ascii?Q?DfPAKbhk1xcKH3nFS06xbftb+TiPIJZlqhzWwuZSLyn5P0VMOH1BgtOVdNcU?=
=?us-ascii?Q?VxwklLOXfmuZMrPKn5n+/FfeBgwh0ONtAoTbFIKnpUc0CBMa2gbvB8ak0bLA?=
=?us-ascii?Q?u6teInyHmOhc/LOA+1ROOmW4GwoaLv5qr+cjvKPbpQ9kcCpYHVPYxSH7AxJf?=
=?us-ascii?Q?3PvwdRn0sgYxL2FaC3tflK6KGzeXjpfq2QjLAZc0NucBUoZnHflBhXuH1r7M?=
=?us-ascii?Q?1zDh7JvvNxcqCGY1yntlOgtJ8/QE7Zn7OF7c+bhirva6ULLNI61Hj/+3HD69d?=
=?us-ascii?Q?/XpfpYpsJ+rrNGrZd618yLLuwJnadTrE/Zclee90OTMoA60238HH4vY/tQNJ?=
=?us-ascii?Q?atSNDyERhWu7saN+vfoOJS8pb/YylZXcJOSxhnUdm0SeMMmNRYT9bgAcCfIc?=
=?us-ascii?Q?fM5JF8OpcxekHa4DjvLfp0s5iEPW06+CeN3IrxpCp9NEHmOTgDKYl9pXI09L?=
=?us-ascii?Q?4Prdd4F3W9IESKTMOSiL/ohxFP641wlpBLuvEmT89HFEb3Ddj6nxdqFd0Y1j?=
=?us-ascii?Q?DJotkNGR1mfoWSE7pbP5YbJqQDjkb9ejg+f5n4d87JUvW0yGcKBI+XXEvEaM?=
=?us-ascii?Q?o9q16Sa7bEOpOKH7fFSbyDW8eQh1zS6Uy0C4unZV7xl2rMTq8X8r01AmlGbo?=
=?us-ascii?Q?Q3WnwosiIFZ44VBM8FGaOAuKa2L8hAGpVW2snGWycIUyyNyHWRpdrRNc+GLv?=
=?us-ascii?Q?TQaYh5AIsXTWQq8q1j0WM57KEV0gSUG9IY9aGKhYp5weYREcBaOgGsxwaKxo?=
=?us-ascii?Q?0iXRyhWBc4DscwgWUP1NEj10yRpy6HpMQN/Qk/q1toSt4eLsXC/X/1ZfxjCq?=
=?us-ascii?Q?ACqYDsLtkMM82A65OeBeRg+Bc9cKJjnHODK05+Zf0gHH3DjfvzP0a64svFqM?=
=?us-ascii?Q?L79sz5qQ96P2RYZ74rYJH2nY3G41hZx55JFv9eUT15zi7p/PHNYUoAfr1DFG?=
=?us-ascii?Q?nU+NCX0WBauzkgYD8ntp0OEKuVaGF/n2vfHoQbcXiGH3ut++RUHA+0koigxq?=
=?us-ascii?Q?/ROBaa7oGh5MyHst7LCpflpfp01+JjDTqJ7ux0CYArWOAzfWNTOSln9HAt55?=-

=?us-ascii?Q?wTIE/y5qMpKW2knjFLOYuGXMYcFj0V9HjWJXe17ujHsyinPiAV5Pr68w+Yr5?=
=?us-ascii?Q?3whMT8yMPTJPZpU8N40AwmKoFxy0waMR8qf0homwNhIFyR3K0xrpkmq+YlFM?=
=?us-ascii?Q?lEyRq4jHgtVMfZ1ug21B+aUQed4K6SkpRkutgH/jGx0I4ZG1qw=3D=3D?=
x-forefront-antispam-report:

CIP:255.255.255.255; CTRY:; LANG:en; SCL:1; SRV:; IPV:NLI; SFV:NSPM; H:SJ0PR09MB9222.namprd09.pr
od.outlook.com; PTR:; CAT:NONE; SFS:(13230040)(366016)(1800799024)(8096899003)(38070700018);
DIR:OUT; SFP:1101;

x-ms-exchange-antispam-messagedata-chunkcount: 1

x-ms-exchange-antispam-messagedata-0: =?us-

ascii?Q?8DpjWpXaq3uIqWBipmBuCo9pOp25CplX6fbB4dJ401BSODV8GHVO/3MR4R0X?=
=?us-ascii?Q?OP0mitXZowVbhCiITdPlwWjpAke0sSZHehMl9FGAbWLQyhiND2Xgy+kZsNmC?=
=?us-ascii?Q?ezodrRLRWlgFCd9q07oaJQheerGBbt15oZjBwbuaEwppQxPjDppsaK9VlL3e?=
=?us-ascii?Q?rMGumULfrXwJWAIGS/W6dCA5zUVclU9sgYoz1Q2IW29wR9UTxciwMo5CMEhc?=
=?us-ascii?Q?xsOsNA7mgCw+hg62uRZ5Kqavt2FG1jRup+bd0zGQC/H4oWdM6CJ9tLDYSyW1?=
=?us-ascii?Q?cMiXmWKORmBq+ImaUmMAwTPK5gvPbycKvJ7xQPdQjYr+p6ZxgoaC/A2ZVvO1?=
=?us-ascii?Q?IgHukms4RIHqKUszXCPlYaF6NL0oKohBIeRDoEa4BAhhFZLcuY2tBD0RP8rZ?=
=?us-ascii?Q?mG9wqjPeOc6T2kYpR8abCZihWkZ3/lmpMbtbHu1SB115udSqkje2/IbARYa8?=
=?us-ascii?Q?n9qWN0YPYGjJVzYwFGUj2DHmJSzJRM0TDR07GENCFH7QDfYjLsDlu/1qjRrJ?=
=?us-ascii?Q?M4103zCpZQ84P+UiwG4nez4ZGxxiC0WXvWmL6wHBvWYDutFU+zYsCop+1YDe?=
=?us-ascii?Q?4fxFyVnMZeJME83fSeilt0ynrwlYEsj4iYf713XfCbYYREvUlmxDvnETbh2n?=
=?us-ascii?Q?8SASPCAsX6fEu32hB8VjJXQPnHpL9qkW5/n6lBk22I5u+5gbdpb91dic92n3?=
=?us-ascii?Q?CwtqScP9Se2uKodUHiSOW21E194jz38fWybHTA64000nvq82b6e6uoYOMgPL?=
=?us-ascii?Q?KWuozkG1fhqP4X4h3v2RwwekB8C6gK4nwtS6PplgewgKAKw5OGmkPNbsgk69?=
=?us-ascii?Q?g2V7ELnAg8NZ+PU1ZSuvEWlVblbXexrQkGo7EQoELtKb8ZqTVwAL0Q0GW1BL?=
=?us-ascii?Q?NgqthIuVdtOrF2nmcRiGmln3XgVSWz04AFyJNA7JnxVwoBQyhob+nKoagVTv?=
=?us-ascii?Q?B5bga/ih0e4+Kw5gP4xwkn04d3A10yPMCCqdZaLyFI4c1Spepr+pGAFPH4yg?=
=?us-ascii?Q?nDwFl4nvp6L+QL7EErcihxwTcoVJmNQVQz07DGJz1qaAusVf6UUH50ISeGpe?=
=?us-ascii?Q?d6Fgcb7d4cMPKN4IPWvG1103B1BzMKZDkz6iRoNjLhBkrKDgDJK6vVACW4q?=
=?us-ascii?Q?co8JVH1NsM8LOIsG3gqDdpKIxzJTPw+yICzYPFLH7IGEcadEE4CHSTUW2n79?=
=?us-ascii?Q?/ImOyMfR4rm559gQgWT5JTG1+1ndMr32c0qdfQ+7wHQbbLrbiu2JuUuCAb5A?=
=?us-ascii?Q?J/uq9bLh5sMdvMJ9+8zdz+16ZkVwoTvrwk2VqXe7TU10/vlKT8Q0r+j569zZ?=
=?us-ascii?Q?j6Ho5EsMJaiIoKEihU1+vCDYSJYJDcoPRrWNzrdMVK/MWwK7zxDoRmcTrrzM?=
=?us-ascii?Q?f82MONTedCrfCkblL+93Q6oPycA/WPRaT/ycAdVZuluIwvllRRtMxh7QC+fu?=
=?us-ascii?Q?UNaXEIdeTI50KVvJ1jFsTeuaKUjU5xsZ3aoa1UPUL2ZqdCfB4EYpgyTjSNrn?=
=?us-ascii?Q?hf6XiAIwRm01749rHCSjFSaXWfw+w6IXwnLQh5XTagYzyNcFKrgh96vZomRN?=
=?us-ascii?Q?qtCnyQ61SJJbk/C15gFu5xc9vF5s1fpyENi4eYyF01Mo9GbQca9CmN0whPWj?=
=?us-ascii?Q?3Q=3D=3D?=
Content-Type: multipart/alternative;

boundary="_000_SJ0PR09MB922232B374D246F851DCCD0BDF312SJ0PR09MB9222nampr_"

MIME-Version: 1.0

X-OriginatorOrg: ag.ny.gov

X-MS-Exchange-CrossTenant-AuthAs: Internal

X-MS-Exchange-CrossTenant-AuthSource: SJ0PR09MB9222.namprd09.prod.outlook.com

X-MS-Exchange-CrossTenant-Network-Message-Id: ee0173bf-4ab5-4984-b681-08dd164bde1d

X-MS-Exchange-CrossTenant-originalarrivaltime: 06 Dec 2024 23:15:26.0785

(UTC)

X-MS-Exchange-CrossTenant-fromentityheader: Hosted

X-MS-Exchange-CrossTenant-id: f0e46024-97df-431a-80d6-c0e744fd7a39

X-MS-Exchange-Transport-CrossTenantHeadersStamped: MW4PR09MB9219

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

THE PEOPLE OF THE STATE OF NEW YORK,
by LETITIA JAMES, Attorney General
of the State of New York,

Plaintiff,

- against -

Index No. _____
IAS Part _____
Assigned to Justice _____

Unknown Parties in Ownership and/or Control of
Digital Wallet Addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d,
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and
TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu,
and Unknown Others,

Defendants.

**PLAINTIFF’S MEMORANDUM OF LAW IN SUPPORT OF THE AFFIRMATION AND
PROPOSED ORDER TO SHOW CAUSE**

LETITIA JAMES
Attorney General of the State of New
York 28 Liberty Street
New York, NY 10005

Of Counsel:

SHANTELEE CHRISTIE
Assistant Attorney General

JONATHAN BASHI
Assistant Attorney General

KENNETH HAIM
Deputy Chief, Investor Protection Bureau

SHAMISO MASWOSWE
Chief, Investor Protection Bureau

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

FACTUAL BACKGROUND..... 2

ARGUMENT..... 4

 I. Service by NFTs and Website Posting is Sufficient and Appropriate Under These
 Circumstances 4

 A. Legal Standards..... 5

 B. OAG’s Service of the OAG Pleadings by NFTs and Website Posting Satisfies CPLR
 § 308(5) due to Defendants’ Anonymity 7

CONCLUSION..... 9

WORD COUNT CERTIFICATION PURSUANT TO NYCRR 202.8-B..... 10

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Bandyopadhyay v. Defendant 1</i> , 2022 U.S. Dist. LEXIS 212221 (S.D. Fla. Nov. 23, 2022)	7
<i>Bossuk v. Steinberg</i> , 58 N.Y.2d 916 (1st Dept. 1983)	5
<i>Chow v. Defendant 1</i> , 2024 U.S. Dist. LEXIS 71604 (E.D. La. Apr. 16, 2024)	6
<i>Dobkin v. Chapman</i> , 21 N.Y.2d 490 (1968)	6
<i>Harkness v. Doe</i> , 261 A.D.2d 846 (4th Dept. 1999).....	5
<i>Hollow v. Hollow</i> , 747 N.Y.S.2d 704 (Sup. Ct. Oswego Cnty. Aug. 19, 2002).....	8
<i>Jean v. Csencits</i> , 171 A.D.3d 1149 (2d Dept. 2019)	5
<i>LCX AG v. John Doe Nos. 1-25</i> , No. 154644/2022 (Sup. Ct. N.Y. Cnty. Filed 06/01/2022)	6,8
<i>Liebeskind v. Liebeskind</i> , 86 A.D.2d 207 (1st Dept., 1982)	5
<i>Markoff v. South Nassau Community Hosp.</i> , 91 A.D.2d 1064 (2d Dept. 1983)	5
<i>Meghji v. Wallet Owner 0X10F546A6F4D20D91E5A8506124384759C9F4BC79 (In re Celsius Network LLC)</i> , 2024 Bankr. LEXIS 2592 (U.S. Bankr. Ct., S.D.N.Y, Oct. 24, 2024)	6,8
<i>Polansky v. Defendant 1</i> , 2023 U.S. Dist. LEXIS 154930 (S.D. Fla, Aug. 31, 2024).....	6
<i>State St. Bank & Trust Co. v. Coakley</i> , 16 A.D.3d 403 (2d Dept. 2005)	5
<i>Synder v. Energy Inc.</i> , 19 Misc. 3d 954 (Civ. Ct., N.Y. Cnty., 2008)	5
 State Statutes	
New York Executive Law § 63(12).....	2
 Rules	
CPLR § 308.....	passim

Plaintiff, People of the State of New York by Letitia James, Attorney General of the State of New York (“OAG”), submits this memorandum of law pursuant to Civil Practice Law and Rule (“CPLR”) § 308(5) in support of OAG’s Proposed Order to Show Cause for alternative service of the OAG Pleadings upon Defendants by airdropping—*i.e.*, depositing—one of three separate non-fungible tokens (“NFTs”), each hyperlinked to the same website containing a copy of the OAG Pleadings, to each wallet identified in the caption.

PRELIMINARY STATEMENT

OAG’s diligent search for Defendants’ mailing addresses, places of business and residences has been unsuccessful. Defendants, unknown parties, employed an elaborate scheme to lure job-seeking individuals (the “Victims”), including New Yorkers, with the false promise of lucrative remote employment and deceived them into transferring cryptocurrency to digital wallets that Defendants owned and/or controlled. OAG has traced the Victims’ cryptocurrency to Defendants’ wallets but has no reliable information as to the identities or locations of Defendants, who used spoofed telephone numbers, seemingly defunct email addresses, and digital blockchain technology to remain anonymous.

Alternative service using NFTs and website posting is necessary and appropriate under the circumstances of the present case where Defendants used the blockchain to carry out their scheme and, despite thorough and diligent efforts, OAG has been unable to obtain further contact information for Defendants. As a result, Plaintiff is unable to effectuate personal service of process or other service permissible by the CPLR and seeks relief pursuant to CPLR § 308(5) to serve Defendants via NFTs and website posting to their wallets. Such method is reasonably calculated to apprise Defendants of the commencement and pendency of the action and afford them an opportunity to be heard.

FACTUAL BACKGROUND

OAG filed the OAG Pleadings on January 9, 2025, against Defendants to, among other things, permanently enjoin them from engaging in fraudulent, deceptive, and illegal acts in violation of New York’s General Business Law (“GBL”) Articles 23-A (the “Martin Act”) and 22-A, and Executive Law § 63(12). Cmpl. ¶ 8.¹ Through this action, OAG seeks to recover the stablecoins, a type of cryptocurrency, currently frozen in the Wallets² Defendants used to steal stablecoins from New Yorkers and individuals across the country via fraudulent transfers:

- Approximately 219,840 USDC stablecoins located in Wallet 1 and valued at \$219,840 as of January 9, 2025;
- Approximately 862,347 USDT stablecoins located in Wallet 2 and valued at \$862,347 as of January 9, 2025; and
- Approximately 1,098,320 USDT stablecoins located in Wallet 3 and valued at \$1,097,320 as of January 9, 2025. Affn ¶ 2.³

Defendants defrauded New York residents and other individuals across the country into believing they were employed by various companies solely to defraud them of their cryptocurrency. “Cmpl.” ¶ 20. Defendants communicated with the Victims via SMS text messages and WhatsApp messenger chats using a collection of Telephone Numbers, the majority of which were either defunct or spoofed. Affn ¶¶ 4 and 10-11. On December 6, 9, and 10, 2024 OAG sent text messages to the Telephone Numbers informing each recipient of OAG’s intent to file a lawsuit against them and requesting a mailing address for service. Only two Telephone Numbers returned a response and neither provided a verifiable mailing

¹ References herein to “Cmpl. ¶” refer to paragraphs within the Complaint filed against the captioned defendants: Index No. not yet assigned.

² Capitalized terms not defined herein have the meanings attributed to them in the Affirmation.

³ References herein to “Affn ¶” refer to paragraphs within the Affirmation filed in support of OAG’s Proposed Order to Show Cause. Index No. not yet assigned.

address. *Id.* The remaining Telephone Numbers either provided no response or returned identical responses informing OAG that the Telephone Number was a landline. *Id.* at 11. Landlines do not natively support text messages and text messages sent to those Telephone Numbers could not be delivered without converting them to voice messages. *Id.* This suggests that Defendants used caller identification that mimicked landlines already in existence (i.e. spoofing) to mask their true identities.

OAG further investigated the four Email Addresses to whom Defendants directed one Victim to send U.S. dollars via a money services business. Affn ¶¶ 5 and 12. On December 6, 2024, OAG sent email messages to the Email Addresses but only one returned a “delivered” notice and OAG did not receive the requested mailing address. Affn ¶ 12. OAG’s messages to two other Email Addresses were “relayed” but their destination server did not send a “delivered” notice, and OAG’s email to the fourth Email Address generated a “not delivered” notice and labeled that Email Address as “not found at gmail.com,” its purported email domain. *Id.*

OAG traced millions of stablecoins to the Wallets. Affn ¶ 6. By April 1, 2024, over 2 million USDC was traced into Wallet 1, approximately 2 million of which was later exchanged for USDT traced into Wallets 2 and 3. Affn ¶ 6-8. OAG secured the freeze of the remaining 219,840 USDT Defendants left in Wallet 1. *Id.* at 7. After the exchange to USDT, Defendants divided the USDT and transferred approximately 990,000 and 1,098,320 to Wallets 2 and Wallet 3, respectively, and OAG secured their freeze on April 26, 2024. Affn ¶ 8.

While Defendants are unable to withdraw any USDT or USDC from the Wallets due to the freezes, they have continued to effect transactions and receive cryptocurrency in the Wallets. Affn ¶ 9. On April 12, 2024— one week after OAG obtained the USDC freeze— Defendants transferred other cryptocurrency out of Wallet 1 to a different wallet. *Id.* Wallet 1 also received airdropped NFTs between May 2, 2024 and August 30, 2024, and some cryptocurrency on September 7, 2024. *Id.* Defendants also transferred cryptocurrency from Wallet 2 to other wallets on April 30, 2024 and May 2, 2024 and continued to receive cryptocurrency in Wallets 2 and 3 between April 30, 2024 and December 4, 2024. *Id.*

Defendants unlawful conduct specifically concerns fraudulent, illegal, and deceptive acts and practices that were effected in the Wallets and through use of the Telephone Numbers and Email Addresses, none of which have provided OAG with verifiable information regarding Defendants' identities and location. *Id.* at 13. Despite diligent efforts, OAG currently cannot identify verifiable mailing addresses or other more conventional contact information for Defendants. Accordingly, OAG seeks permission to serve Defendants via NFTs airdropped to the Wallets. *Id.* at 14-17.

ARGUMENT

I. Service by NFTs and Website Posting is Sufficient and Appropriate Under These Circumstances

Given the limited knowable information about the identities and locations of Defendants, service via airdropped NFTs that are hyperlinked to a website containing the OAG Pleadings is the only reliable method reasonably calculated to ensure timely and proper notice of the proceedings and an opportunity for Defendants to appear and respond.

A. Legal Standards

Where service on a defendant via traditional means like personal service or service at the defendant's place of abode is impracticable, CPLR § 308 authorizes alternative methods for serving such defendants, including service "in such manner as the court, upon motion without notice, directs. . ." CPLR § 308(5). The meaning of "impracticable" is dependent on the facts and circumstances of the particular case, *see Markoff v. South Nassau Community Hosp.*, 91 A.D.2d 1064 (2d Dept. 1983) (citing *Liebeskind v. Liebeskind*, 86 A.D.2d 207, 229 (1st Dept., 1982)). The applicant is not required to demonstrate prior attempts of service upon the defendants or that service under the CPLR could not be made with due diligence. *See Liebeskind*, 86 A.D.2d at 210 (upholding alternative service where defendant went into hiding to avoid timely service of process); *State St. Bank & Trust Co. v. Coakley*, 16 A.D.3d 403, 403 (2d Dept. 2005) (affirming lower court order directing alternative service of process). Instead, "[a] plaintiff can demonstrate that service by conventional means is 'impracticable'" by making diligent, albeit unsuccessful, efforts to obtain information regarding a defendant's current residence, business address or place of abode." *Synder v. Energy Inc.*, 19 Misc. 3d 954, 959 (Civ. Ct., N.Y. Cnty., 2008) (authorizing alternative service via e-mail and ruling that plaintiffs need not wait for the CPLR to be amended in order to be able to resort to alternative service).

Due process requires that the proposed alternative method of service be made in a manner "reasonably calculated, under all of the circumstances, to apprise the defendant of the action." *Jean v. Csencits*, 171 A.D.3d 1149, 1150 (2d Dept. 2019) (upholding alternative service pursuant to CPLR § 308(5)). However, the method of service need not guarantee that Defendants will receive actual notice in order to be constitutionally adequate. *See Bossuk v. Steinberg*, 58 N.Y.2d 916, 918 (1st Dept. 1983) (affirming sufficiency of service of process on

the defendant); *Harkness v. Doe*, 261 A.D.2d 846, 847 (4th Dept. 1999) (same).

Courts, in evaluating whether forms of alternative service are appropriate, have wide latitude to fashion methods of service “adapted to the particular facts of the case before it.” *Dobkin v. Chapman*, 21 N.Y.2d 490 (1968) (affirming service via mail and delivery to auto insurance carrier as adequate to notify defendants of the lawsuit). For example, New York courts in similar circumstances have recently deemed service to an unknown wallet owner by NFT and website posting sufficient where service under CPLR §§ 308 (1), (2), and (4) was impracticable due to the plaintiff lacking contact information for the defendant. *See, e.g.*, Decision + Order on Motion at 7, *LCX AG v. John Doe Nos. 1-25*, No. 154644/2022 (Sup. Ct. N.Y. Cnty Filed 08/21/2022) (finding alternative service by NFT to be effective service and “especially necessary because of the anonymity of the Doe Defendants”).

Likewise, in *Meghji v. Wallet Owner 0X10F546A6F4D20D91E5A8506124384759C9 F4BC79 (In re Celsius Network LLC)*, where the plaintiff sought to recover cryptocurrency misappropriated and transferred to wallets owned or controlled by defendants that the plaintiff could not identify or contact and knew nothing about, the Court granted a motion for alternative service by airdropping NFTs linked to a service website that contained copies of the complaint to the cryptocurrency wallets of the defendants. 2024 Bankr. LEXIS 2592, at 4-8 (U.S. Bankr. Ct., S.D.N.Y., Oct. 24, 2024). The *Meghji* Court held that the defendants’ unknown identities and locations rendered service pursuant to CPLR §§ 308(1)-(2) and (4) impracticable and found that “[r]egardless of the [d]efendants’ geographic location,” it had authority to allow alternative service as the defendants could not be located or identified. *Id.* at 10-11.⁴

⁴ Courts elsewhere in the country have held service by NFT as a valid and effective means of service on digital

OAG similarly seeks to recover stolen cryptocurrency from Defendants for whom OAG has had no success in obtaining their identities or locations to enable personal delivery. Like the circumstances highlighted in *Meghji*, service, herein, via the traditional methods of CPLR § 308 (1), (2), and (4) is impracticable as Defendants' identities and locations remain unknown, rendering service via NFTs and website posting of the OAG Pleadings warranted, sufficient, and appropriate under the circumstances.

B. OAG's Service of the OAG Pleadings by NFTs and Website Posting Satisfies CPLR § 308(5) due to Defendants' Anonymity

With no known identities and locations for Defendants, service upon the Wallets, which pseudonymously identify their wallet-holder, is the *only* method presently available to OAG to effect service of the OAG Pleadings. Given that only individuals who possess a private key to a given wallet can access and transfer cryptocurrency out of that wallet, service on the Wallets—in which Defendants continued transacting on the blockchain after the subject stablecoins were frozen—is reasonably calculated to give Defendants notice of OAG's action.

OAG has contacted Defendants via the Telephone Numbers on three different days, sent email messages to the Email Addresses, *see* Affn ¶¶ 10-12, and sought Know-Your-Customer information about the Wallets in an effort to identify the identities and locations of Defendants. *Id.* at 7. Despite these efforts, OAG has obtained no verifiable information regarding Defendants' location, making it *per se* impossible to serve Defendants using the methods set forth in CPLR § 308(1) – (2), and (4). OAG must therefore resort to alternative methods to serve Defendants with the OAG Pleadings—*i.e.* airdropping NFTs to the Wallets,

wallet. *See, e.g., Polansky v. Defendant 1*, 2023 U.S. Dist. LEXIS 154930 (S.D. Fla, Aug. 31, 2024) (permitting service via NFT and finding that service method via this method is “likely to reach Defendants...”); *Chow v. Defendant 1*, 2024 U.S. Dist. LEXIS 71604 (E.D. La. Apr. 16, 2024) (ordering that service by NFT electronic transfer and website posting is reasonably calculated to give notice to Defendant); *Bandyopadhyay v. Defendant 1*, 2022 U.S. Dist. LEXIS 212221 (S.D. Fla. Nov. 23, 2022) (ruling that NFT and posting on a designated website are reasonably calculated to give notice to Defendants).

with each NFT hyperlinked to the same website containing copies of the OAG Pleadings.

OAG's proposed method of service is reasonably calculated to provide notice to Defendants and comports with due process. Defendants continue to access and otherwise use the Wallets in spite of the freezes. Affn ¶ 9. The airdrop process is automatic and does not require Defendants to take action to receive the NFTs. *See Meghji*, 2024 Bankr. LEXIS 2592 at 5. Cryptocurrency is still being sent to the Wallets, and in the case of Wallet 1, NFTs repeatedly have been airdropped into the wallet in the past. This activity makes it likely that Defendants will continue returning to the Wallets and that service of the OAG Pleadings in those same Wallets is reasonably calculated to be received by Defendants. *See Hollow v. Hollow*, 747 N.Y.S.2d, 704,708 (Sup. Ct. Oswego Cnty. Aug. 19, 2002) (approving alternative service of process via a communication method favored by the intended recipient); *LCX AG*, 154644/2022, (finding that service via the blockchain was reasonably calculated, under all of the circumstances, to apprise the defendant of the action); *Meghji*, 2024 Bankr. LEXIS 2592 at 18-19 (finding that service via NFT, where no identifying information beyond wallet addresses is known, is permissible, even if Defendants are outside of the United States).

That the Wallets still hold over \$2 million worth of currently-frozen stablecoins serves as an incentive for Defendants to continue to monitor the Wallets and to make OAG's proposed methods of service reasonably calculated to give notice to Defendants. Furthermore, Defendants, like the *LCX AG* defendants, are anonymous fraudsters who continue to use the Wallets, which remain active on the blockchain. Affn ¶ 9. The blockchain facilitated Defendants' fraud against Victims in that the anonymity it provides allowed Defendants to remain unknown and is now preventing OAG from learning their identify and location. It is therefore reasonable for OAG to provide notice to Defendants via airdropped NFTs.

CONCLUSION

For the above reasons, the Court should enter an order, pursuant to CPLR § 308(5), in the form of the Proposed Order, permitting service of the OAG Pleadings via the NFTs and any other such relief that the court deems just and proper.

Dated: January 9, 2025
New York, New York

Respectfully submitted,

LETITIA JAMES
Attorney General of the State of New York
Attorney for Plaintiff
28 Liberty Street, N.Y., N.Y.

By:



Shantelee Christie
Assistant Attorney General
Tel: 212-416-8355
shantelee.christie@ag.ny.gov

Word Count Certification Pursuant to NYCRR 202.8-b

I, Shantelee Christie, hereby certify that the word count of this document, as calculated by Microsoft Office, exclusive of the caption, table of contents, table of authorities, and signature block, is 2,493 words.

By: 

Shantelee Christie



REQUEST FOR JUDICIAL INTERVENTION SUPREME COURT, COUNTY OF QUEENS

UCS-840 (rev. 02/01/2024)

Index No: _____ Date Index Issued: _____

For Court Use Only:

CAPTION Enter the complete case caption. Do not use et al or et ano. If more space is needed, attach a caption rider sheet.

IAS Entry Date

People of the State of New York, by Letitia James, Attorney General of the State of New York

Plaintiff(s)/Petitioner(s)

Judge Assigned

-against-

Unknown Parties in Ownership and/or Control of Digital Wallet Addresses 0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d, TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu; and Unknown Others.

Defendant(s)/Respondent(s)

RJI Filed Date

NATURE OF ACTION OR PROCEEDING Check only one box and specify where indicated.

COMMERCIAL

- Business Entity (includes corporations, partnerships, LLCs, LLPs, etc.)
Contract
Insurance (where insurance company is a party, except arbitration)
UCC (includes sales and negotiable instruments)
Other Commercial (specify): NY GBL §§ 349 & 350, Martin Act § 352 et seq, Executive Law § 63(12)
NOTE: For Commercial Division assignment requests pursuant to 22 NYCRR 202.70(d), complete and attach the COMMERCIAL DIVISION RJI ADDENDUM (UCS-840C).

MATRIMONIAL

- Contested
NOTE: If there are children under the age of 18, complete and attach the MATRIMONIAL RJI ADDENDUM (UCS-840M).
For Uncontested Matrimonial actions, use the Uncontested Divorce RJI (UD-13).

REAL PROPERTY Specify how many properties the application includes: _____

- Condemnation
Mortgage Foreclosure (specify): Residential Commercial
Property Address: _____
NOTE: For Mortgage Foreclosure actions involving a one to four-family, owner-occupied residential property or owner-occupied condominium, complete and attach the FORECLOSURE RJI ADDENDUM (UCS-840F).
Partition
NOTE: Complete and attach the PARTITION RJI ADDENDUM (UCS-840P).
Tax Certiorari (specify): Section: _____ Block: _____ Lot: _____
Tax Foreclosure
Other Real Property (specify): _____

TORTS

- Asbestos
Environmental (specify): _____
Medical, Dental or Podiatric Malpractice
Motor Vehicle
Products Liability (specify): _____
Other Negligence (specify): _____
Other Professional Malpractice (specify): _____
Other Tort (specify): _____

SPECIAL PROCEEDINGS

- Child-Parent Security Act (specify): Assisted Reproduction Surrogacy Agreement
CPLR Article 75 - Arbitration [see NOTE in COMMERCIAL section]
CPLR Article 78 - Proceeding against a Body or Officer
Election Law
Extreme Risk Protection Order
MHL Article 9.60 - Kendra's Law
MHL Article 10 - Sex Offender Confinement (specify): Initial Review
MHL Article 81 (Guardianship)
Other Mental Hygiene (specify): _____
Other Special Proceeding (specify): _____

OTHER MATTERS

- Certificate of Incorporation/Dissolution [see NOTE in COMMERCIAL section]
Emergency Medical Treatment
Habeas Corpus
Local Court Appeal
Mechanic's Lien
Name Change/Sex Designation Change
Pistol Permit Revocation Hearing
Sale or Finance of Religious/Not-for-Profit Property
Other (specify): _____

STATUS OF ACTION OR PROCEEDING Answer YES or NO for every question and enter additional information where indicated.

Table with 2 columns: YES, NO. Rows: Has a summons and complaint or summons with notice been filed? (YES checked), Has a summons and complaint or summons with notice been served? (NO checked), Is this action/proceeding being filed post-judgment? (NO checked).

NATURE OF JUDICIAL INTERVENTION Check one box only and enter additional information where indicated.

- Infant's Compromise
Extreme Risk Protection Order Application
Note of Issue/Certificate of Readiness
Notice of Medical, Dental or Podiatric Malpractice Date Issue Joined: _____
Notice of Motion Relief Requested: _____ Return Date: _____
Notice of Petition Relief Requested: _____ Return Date: _____
Order to Show Cause Relief Requested: Alternative Service Return Date: _____
Other Ex Parte Application Relief Requested: _____
Partition Settlement Conference
Poor Person Application
Request for Preliminary Conference
Residential Mortgage Foreclosure Settlement Conference
Writ of Habeas Corpus
Other (specify): _____

NYSCEF DOC NO. 8
RELATED CASES

List any related actions. For Matrimonial cases, list any related criminal or Family Court cases. If none, leave blank. RECEIVED NYSCEF: 01/09/2025

If additional space is required, complete and attach the **RJI ADDENDUM (UCS-840A)**.

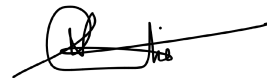
Case Title	Index/Case Number	Court	Judge (if assigned)	Relationship to instant case

PARTIES For parties without an attorney, check the "Un-Rep" box and enter the party's address, phone number and email in the space provided. If additional space is required, complete and attach the **RJI ADDENDUM (UCS-840A)**.

Un-Rep	Parties List parties in same order as listed in the caption and indicate roles (e.g., plaintiff, defendant, 3 rd party plaintiff, etc.)	Attorneys and Unrepresented Litigants For represented parties, provide attorney's name, firm name, address, phone and email. For unrepresented parties, provide party's address, phone and email.	Issue Joined For each defendant, indicate if issue has been joined.	Insurance Carriers For each defendant, indicate insurance carrier, if applicable.
<input type="checkbox"/>	Name: People of the State of New York Role(s): Plaintiff	Shantelee Christie, Office of the New York State Attorney General 28 Liberty Street, New York, NY 10005; (212) 416-8355; shantelee.christie@ag.ny.gov	<input type="radio"/> YES <input type="radio"/> NO	
<input checked="" type="checkbox"/>	Name: Unknown Parties in Ownership or Control of Digital Wallets Role(s): Defendant		<input type="radio"/> YES <input checked="" type="radio"/> NO	
<input checked="" type="checkbox"/>	Name: Other Unknown Parties Role(s): Defendant		<input type="radio"/> YES <input checked="" type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	
<input type="checkbox"/>	Name: Role(s):		<input type="radio"/> YES <input type="radio"/> NO	

I AFFIRM UNDER THE PENALTY OF PERJURY THAT, UPON INFORMATION AND BELIEF, THERE ARE NO OTHER RELATED ACTIONS OR PROCEEDINGS, EXCEPT AS NOTED ABOVE, NOR HAS A REQUEST FOR JUDICIAL INTERVENTION BEEN PREVIOUSLY FILED IN THIS ACTION OR PROCEEDING.

Dated: 01/09/2025



Signature

5304662

Shantelee Christie

Attorney Registration Number

Print Name



**Office of the New York State
Attorney General**

**Letitia James
Attorney General**

January 9, 2025

By NYSCEF

Clerk of the Court
Supreme Court, Queens County
88-11 Sutphin Blvd.
Jamaica, NY 11435

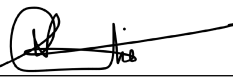
Re: *People of the State of New York v. Unknown Parties in Ownership and/or Control of Digital Wallet Addresses 0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d, TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu, and Unknown Others*

Dear Clerk of the Court:

Please waive the collection of all fees for the Office of the Attorney General of the State of New York in connection with the above-captioned action. The Office of the Attorney General is exempt from the payment of fees pursuant to CPLR 8017 and New York Executive Law § 161.

Respectfully submitted,

LETITIA JAMES
Attorney General of the State of New York

By: 
Shantelee Christie
Assistant Attorney General
shantelee.christie@ag.ny.gov

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

THE PEOPLE OF THE STATE OF NEW YORK,
by LETITIA JAMES, Attorney General of the
State of New York,

Plaintiff,

-against-

NOTICE OF APPEARANCE

Index No. 700647/2025

Unknown Parties in Ownership and/or Control of
Digital Wallet Addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d,
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and
TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu,
and Unknown Others.

Defendants.

PLEASE TAKE NOTICE that the undersigned hereby enters an appearance in
the above- captioned proceeding as counsel for Petitioner Letitia James, the Attorney General of
the State of New York.

Dated: January 9, 2025
New York, New York

Respectfully submitted,

LETITIA JAMES
Attorney General of the State of New York

By: /s/ Jonathan Bashi
Assistant Attorney General
Office of the New York State Attorney General
Investor Protection Bureau
28 Liberty Street
New York, New York 10005
Tel. (212) 416-8564
Email: jonathan.bashi@ag.ny.gov

Sequence # 1

At IAS Part 24 of the Supreme Court of the State of New York, held in and for the County of Queens, at the Courthouse thereof, 25-10 Court Square, Long Island City, New York, on the 10 day of January, 2025

PRESENT:
Honorable Karen Lin, JSC
Justice Presiding

-----X
THE PEOPLE OF THE STATE OF NEW YORK
By LETITIA JAMES,
Attorney General of the State of New York,

Plaintiff,

ORDER TO SHOW CAUSE

-against-

Index No. 700647/2025

Motion Sequence No. 1

Unknown Parties in Ownership and/or Control of Digital Wallet Addresses
0xD7648FffA48e06b0107435a966F3F1e9DBe10B7d,
TCfr5oZp8qJJwarum6kjt4o23wTNhi1ss8, and
TDvRhqyGMW5NuZjhiAmEm YuXrSZ4bdZtmu,
and Unknown others,

Defendants.

-----X
Upon reading the affirmation of Assistant Attorney General Shantelee Christie together with the exhibit(s) annexed thereto (the "Affirmation") and the accompanying memorandum of law; and upon the application of the Office of the New York State Attorney General ("OAG") for an order permitting alternative service of process of the Summons, Complaint, this [Proposed] Order to Show Cause, the Affirmation, memorandum of law in support thereof and all documents submitted contemporaneously therewith (collectively, the "OAG Pleadings") upon Defendants by airdropping—i.e., depositing to each of the digital wallets listed in the caption—one of three separate non-fungible tokens ("NFTs") with each NFT to be hyperlinked to the same website containing the OAG Pleadings;

Let Defendants, or their attorneys show cause at I.A.S. Part 24, Room G-40, of this Court, at the Courthouse, 25-10 Court Square, Long Island City, New York 11101, on the 13 day of February, 2025, at 9 : 30 A.M., in-person, or as soon as the parties to this proceeding may be heard why an order should not be entered herein, pursuant to CPLR § 308(5), permitting service of the OAG Pleadings upon the Defendants by airdropping one of three separate NFTs to each of the digital wallets listed in the caption, and with each NFT hyperlinked to the same website containing the OAG Pleadings; and it is further

ORDERED that service of a copy of this order together with the Summons and Complaint, Attorney Affirmation, and Exhibits annexed thereto, Memorandum of Law in support of this order, and all documents submitted contemporaneously therewith, upon the Defendants by airdropped NFTs into each of the wallets identified in the caption, with each NFT hyperlinked to the same website directing persons to the webpage wherein OAG will publish the order to show cause and the papers upon which it is based, on or before the 24 day of January, 2025, is deemed good and sufficient service thereof. An affidavit or other proof of service shall be presented to this Court on or before the return date fixed above; and it is further

ORDERED that the application brought on by this order to show cause shall not be orally argued unless counsels are notified to the contrary by the Clerk of the Court.

Dated: January 10, 2025
Long Island City, New York

SMG FILED
1/10/2025
COUNTY CLERK
QUEENS COUNTY

ENTER: 
HON. KAREN LIN, J.S.C.

To find legal information to help you represent yourself visit www.nycourthelp.gov

Information for Attorneys

An attorney representing a party who is served with this notice must either consent or decline consent to electronic filing and service through NYSCEF for this case.

Attorneys registered with NYSCEF may record their consent electronically in the manner provided at the NYSCEF site. Attorneys not registered with NYSCEF but intending to participate in e-filing must first create a NYSCEF account and obtain a user ID and password prior to recording their consent by going to www.nycourts.gov/efile

Attorneys declining to consent must file with the court and serve on all parties of record a declination of consent.

For additional information about electronic filing and to create a NYSCEF account, visit the NYSCEF website at www.nycourts.gov/efile or contact the NYSCEF Resource Center (phone: 646-386-3033; e-mail: nyscef@nycourts.gov).

Dated: January 14, 2025

Shantelee Christie, Assistant Attorney 
Name
Office of the New York State Attorney
General
Firm Name 

28 Liberty Street
Address
New York, New York 10005
212-416-8355
Phone
shantelee.christie@ag.ny.gov
E-Mail

To: Unknown Parties in Ownership and/or Control of Digital Wallet Addresses

0xD7648FfA48e06b0107435a966F3F1e9DBe10B7d, TCfr5oZp8qJJwarum6kij4o23wTNhi1ss8

and TDvRhqyGMW5NuZjhiAmEmYuXrSZ4bdZtmu, and Unknown Others

6/6/18