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

RADHIKA ADVANI, on behalf of herself and individuals similarly situated	)	Index No. 156048/2026
Plaintiff,	)	
-against-	)	
JOHN DOE NOS. 1-25	)	
Defendants.	)	

AFFIDAVIT OF RADHIKA ADVANI

I, Radhika Advani, hereby make this affidavit based upon my personal knowledge

1. I am the Plaintiff in this action. I submit this declaration in support of my motion for a temporary restraining order, expedited discovery, and alternative service.

2. I am an adult resident of Plainview, New York.

3. I have personal knowledge of the facts stated in this declaration and could competently testify to them if called as a witness.

4. On or about October 1, 2024, I was contacted through Facebook by an individual using the name "Ramona Zagan." This person claimed to be associated with Wendy Wu Tours, which I understood to be a legitimate international travel company.

5. This individual told me about what was described as a work-from-home opportunity involving the completion of online "tasks" related to creating travel bookings through an online platform.

6. I was told that participants could earn commissions by completing tasks on the platform and that the opportunity was affiliated with Wendy Wu Tours.

7. I was directed to visit websites located at:

https://www.wendywutours-tours.com

https://www.wendywutours-adventure.com

8. At the time, I believed these websites were associated with the legitimate travel company Wendy Wu Tours, whose official website is located at https://www.wendywutours.com.

9. I later learned that the websites I was directed to use were fraudulent websites impersonating the legitimate Wendy Wu Tours business.

10. After I began communicating with individuals associated with the platform, I was placed into a Telegram chat group with other purported participants.

11. In that chat group, individuals claimed they were earning significant income through the platform.

12. Members of the group discussed luxury purchases, travel, and other lifestyles that they claimed were funded through earnings from the platform.

13. These communications led me to believe the opportunity was legitimate and profitable.

14. I was instructed to open cryptocurrency accounts with entities including Coinbase, Gemini, and Cash App in order to transfer cryptocurrency to the Defendants.

15. I was told that in order to complete tasks on the platform I would need to transfer cryptocurrency to wallet addresses provided by the platform.

16. I was told that the platform operated by generating “trip flow” booking transactions and that I could earn commissions by processing those transactions through the platform.

17. Defendants represented that certain tasks would generate commissions of approximately 0.75 percent while other tasks would generate returns of around six percent.

18. I was told that the platform required users to temporarily fund booking transactions so that the system could process them.

19. I was told that once a booking transaction was completed, my deposited funds would be returned together with a commission credited to my account.

20. I was further told that the platform operated in cycles of thirty-six tasks, and that once I completed the full sequence of tasks I would be able to withdraw both my deposits and the commissions shown in my account.

21. I was also told that certain tasks were referred to as "High Rebate Trips," which supposedly corresponded to larger travel bookings that generated higher commissions but required larger cryptocurrency deposits to complete.

22. Based on these representations, I began transferring cryptocurrency from my Coinbase account to wallet addresses provided by the individuals operating the platform.

23. Beginning on or about October 3, 2024, I transferred cryptocurrency to wallet addresses provided by the individuals operating the platform. In total, I transferred over $168,000 in cryptocurrency as part of the scheme.

24. Based on the blockchain tracing currently available, at least $163,000 of those transfers have been identified as having been sent to wallet addresses associated with Defendants between October 3, 2024 and November 27, 2024 through eleven cryptocurrency transactions. Additional transfers may be identified through further blockchain tracing and discovery directed to cryptocurrency exchanges.

25. After each transfer, the platform displayed account balances that appeared to increase and showed what appeared to be profits and commissions.

26. I later learned that these balances were fabricated.

27. After completing multiple transfers, I attempted to withdraw the funds reflected in my account.

28. Beginning on or about October 29, 2024, I attempted to withdraw funds but was informed that my funds were "blocked" and that I needed to wait before attempting another withdrawal.

29. I attempted again on or about November 22, 2024, after completing assigned tasks, but I was told that my account was subject to a $3,000 daily withdrawal limit unless I upgraded my membership level.

30. On or about November 22, 2024, the platform allowed me to withdraw approximately $3,000 through three separate transactions, while continuing to represent that larger withdrawals were restricted by membership limits.

31. I now believe that this limited withdrawal was permitted to create the appearance that the platform was legitimate and to encourage me to continue depositing cryptocurrency.

32. When I again attempted to withdraw funds on or about November 27, 2024, I was told that my account's "credibility score" had fallen to 64% and that withdrawals could not be processed unless the score was restored to 100%, which could only be done by transferring more cryptocurrency to Defendants.

33. Shortly thereafter, I was told that I needed to deposit an additional $60,000 in cryptocurrency in order to unlock my account and process the withdrawal. (*See* Exhibit A to this Declaration).

34. At that point, I became suspicious of the representations being made to me and refused to make that additional transfer.

35. After I refused to send additional cryptocurrency, the individuals operating the platform ceased communicating with me.

36. I was unable to recover the cryptocurrency that I had transferred.

37. At least $163,000 of the cryptocurrency I transferred to Defendants has been identified through blockchain tracing, representing a substantial portion of my financial resources.

38. The loss of these funds has caused me significant financial hardship.

39. The individuals who communicated with me used false identities and did not disclose their real names or locations.

40. My communications with these individuals occurred through Facebook, Telegram, and WhatsApp.

41. I do not know the true identities or physical locations of the individuals who received my cryptocurrency.

42. After discovering the fraud, I promptly reported the scheme to law enforcement.

43. I reported the matter to the Nassau County District Attorney's Office.

44. I also contacted the Federal Bureau of Investigation (FBI) and submitted a complaint through the Internet Crime Complaint Center (IC3).

45. I also reported the theft to the Federal Trade Commission (FTC).

46. I cooperated with law enforcement and provided the documentation and information available to me.

47. I was informed that because cryptocurrency fraud schemes frequently involve anonymous and international actors, recovery through law enforcement channels alone may be difficult.

48. I understand that cryptocurrency can be transferred rapidly across multiple blockchain wallets and exchanges. Such transfers can occur within minutes and can make recovery extremely difficult once the assets are moved through additional wallets or exchanges.

49. Based on what I have learned since discovering the fraud, I believe the individuals who took my cryptocurrency may attempt to transfer or conceal the assets through additional cryptocurrency wallets or exchanges.

50. If the cryptocurrency associated with my transfers is not promptly restrained, I believe the funds may be permanently lost.

51. Blockchain tracing conducted by Plaintiff's forensic expert has identified wallet addresses associated with cryptocurrency exchanges, including Binance, BitGet, Crypto.com, HTX, Kraken, MaskEx, Newton Canada, OKX, Revolut, and Wealthsimple, that received or currently hold cryptocurrency traceable to my transfers. I understand that these exchanges control custodial wallets capable of transferring cryptocurrency rapidly unless the assets are restrained. Without immediate relief from the Court, the cryptocurrency traceable to my transfers may be moved, dissipated, or concealed beyond recovery.

52. I respectfully request that the Court issue a temporary restraining order preventing further transfer of cryptocurrency traceable to my deposits.

53. I also request that the Court grant expedited discovery so that the identities of the individuals responsible for the fraud can be determined.

54. I respectfully request that the Court grant the relief requested in my motion papers.

Sworn to before me this 5th day of May, 2026

Christina Ambroise
Notary Public

CHRISTINA AMBROISE
NOTARY PUBLIC - STATE OF NEW YORK
No. 01AM6416443
Qualified in Nassau County
Commission Expires April 19, 2029

Radhika Advani
Radhika Advani