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

RADHIKA ADVANI,

Plaintiff,

v.

JOHN DOE NOS 1-25,

Defendants.

To the above named Defendant(s):

To the above named Defendant(s):

Index No.:
Date Index No. Purchased:

Plaintiff designates as the place of trial:
COUNTY OF NEW YORK

The basis of venue is:
Residence of a party and a substantial part of the events giving rise to the claim occurred in this county

Summons

You are hereby summoned to answer the Complaint in this action and to serve a copy of your Answer, on the Plaintiff's Attorney(s) within twenty (20) days after the service of this Summons, exclusive of the day of service (or within 30 days after the service is complete if this Summons is not personally delivered to you within the State of New York); and in case of your failure to Appear or Answer, Judgment will be taken against you by default for the relief demanded in the Complaint.

Dated: May 11, 2026

/s/ Samuel D. Elswick

Samuel D. Elswick, Esq.
ID No. 5037312
The Gori Law Firm, P.C.
122 E. 42nd Street, Suite 4700
New York, New York 10168
Tel: (321) 430-0860
selswick@gorilaw.com
Counsel for Plaintiff

DEFENDANTS

TO: JOHN DOE NOS 1-25

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

RADHIKA ADVANI, on behalf of herself and individuals similarly situated	)	Index No. _____
Plaintiff,	)	
-against-	)	**VERIFIED COMPLAINT**
JOHN DOE NOS. 1-25	)	
Defendants.	)	

Plaintiff Radhika Advani ("Plaintiff"), on behalf of herself and individuals similarly situated, by and through her undersigned counsel Samuel D. Elswick, brings this complaint for claims of conversion, money had and received, unjust enrichment and imposition of a constructive trust against Defendants, and alleges as follows:

INTRODUCTION

1. This action arises from a fraudulent cryptocurrency scheme through which Defendants stole more than $168,000 from Plaintiff through a deceptive online "task" platform falsely associated with the travel company Wendy Wu Tours. Defendants contacted Plaintiff through social media and induced her to participate in what was represented as a legitimate work-from-home opportunity involving the completion of online 'trip flow' booking tasks that would allegedly generate commissions. In reality, the purported platform was a sham designed to trick Plaintiff into repeatedly transferring cryptocurrency to wallet addresses controlled by Defendants.

2. Over a period of several weeks, Defendants systematically induced Plaintiff to transfer increasing amounts of cryptocurrency by falsely representing that the funds were required to complete "tasks" and that Plaintiff's deposits and commissions would be returned once certain milestones were met. The platform displayed fabricated account balances and commissions in

order to create the illusion of legitimate earnings while demanding additional deposits to unlock withdrawals.

3. In reliance on Defendants' misrepresentations, Plaintiff transferred more than $168,000 in cryptocurrency from her Coinbase account to wallet addresses provided by Defendants. When Plaintiff ultimately demanded the return of her funds, Defendants demanded she transfer increasing amounts of cryptocurrency to wallet addresses controlled by them, and when Plaintiff questioned the legitimacy of the platform, Defendants abruptly ceased all communication.

4. Plaintiff now brings this action to recover the stolen funds and to obtain equitable relief against the cryptocurrency wallets and financial intermediaries that received and continue to control the proceeds of Defendants' fraud.

PARTIES

5. Plaintiff, Radhika Advani, is a resident of Plainview, New York.

6. Defendants John Doe Nos. 1–25 (collectively, "Defendants") are individuals and/or entities whose true names and identities are presently unknown. Upon information and belief, Defendants participated individually and in concert in the fraudulent scheme described herein and exercised control over blockchain wallet addresses used to receive, transfer, route, and launder cryptocurrency belonging to Plaintiff. Defendants are grouped herein according to their apparent roles in the fraudulent scheme based on Plaintiff's communications with Defendants, documentary evidence provided by Plaintiff, and forensic blockchain analysis.

7. Defendant John Doe No. 1 is the individual who initially communicated with Plaintiff using the fictitious identity "Ramona Zagan." Acting as Plaintiff's primary contact on the fraudulent platform, this individual instructed Plaintiff regarding the operation of the purported

"trip flow" booking tasks, directed Plaintiff to purchase cryptocurrency through various exchanges and payment services, and provided the wallet addresses to which Plaintiff transferred cryptocurrency as part of Defendants' scheme.

8. Defendant John Doe Nos. 2–10 are individuals and/or entities who operated, controlled, or materially assisted in operating the fraudulent websites located at wendywutours-tours.com and wendywutours-adventure.com, including the purported "trip flow" booking interface through which fabricated account balances, fictitious tasks, and purported rebates or profits were displayed to Plaintiff.

9. Defendant John Doe Nos. 11–20 are individuals and/or entities who controlled, directly or indirectly, the blockchain wallet addresses designated by Defendants to receive Plaintiff's cryptocurrency, including the "Intake Wallets" [1] identified in this Complaint and subsequent intermediary "Pivot Wallets" [2] through which Plaintiff's assets were routed.

10. Defendant John Doe Nos. 21–25 are individuals and/or entities who knowingly participated in or facilitated the laundering, redistribution, and transfer of Plaintiff's cryptocurrency into exchange-hosted deposit wallets identified through forensic blockchain tracing.

11. Upon information and belief, Defendants also utilized additional fictitious identities to lend legitimacy to the fraudulent scheme, including but not limited to "Glen Mintrim," purportedly identified as Chief Executive Officer of Wendy Wu Tours Ltd, and "Kenneth George," purportedly identified as a "Third Party Agent" of Wendy Wu Tours (Canada). Plaintiff is

[1] An "Intake Wallet" refers to the initial cryptocurrency wallet address provided by perpetrators for victims to deposit funds, serving as the first point of receipt in the fraud scheme before the assets are transferred to intermediary wallets.
[2] A "Pivot Wallet" refers to an intermediary cryptocurrency wallet used to aggregate funds from multiple victims before transferring those funds to additional wallets or exchanges, thereby linking otherwise separate victim transactions to a common fraud operation.

informed and believes that these identities were fabricated or misappropriated as part of the scheme to induce trust and reliance. Each Defendant aided, abetted, encouraged, directed, or otherwise participated in the wrongful conduct described herein.

12. Plaintiff further alleges that Defendants circulated documents, including a purported "Authorization Letter," representing that Wendy Wu Tours Ltd, identified therein as "Wendy Wu Tours Ltd, Newhams Yard, 151–153 Tower Bridge Road, London, SE1 3JE," had authorized Wendy Wu Tours Canada to act as its third-party agent. Upon information and belief, such documents were fraudulent, altered, or otherwise used without authorization to further Defendants' scheme.

13. Upon information and belief, Defendants acted in combination and concert with one another and with additional unidentified co-conspirators. Each Defendant aided, abetted, encouraged, directed, or otherwise participated in the wrongful conduct described herein.

14. Upon information and belief, one or more Defendants reside outside the United States and operate through anonymized digital infrastructure, including encrypted messaging applications, blockchain wallet addresses, decentralized exchanges, and exchange-hosted deposit accounts.

15. Plaintiff will amend this Complaint to substitute the true names of Defendants when their identities are ascertained through discovery, subpoena process, forensic analysis, or other investigative means.

16. The cryptocurrency exchanges referenced in this Complaint, including but not limited to Binance, BitGet, Crypto.com, HTX, Kraken, MaskEx, Newton Canada, OKX, Revolut, and Wealthsimple, are not presently named as defendants. Upon information and belief, exchange-

hosted deposit addresses identified herein serve as routing points through which funds are ultimately commingled into omnibus wallets.

17. Plaintiff seeks injunctive and equitable relief directed toward cryptocurrency traceable to Defendants and currently located within exchange-hosted deposit wallets, without alleging wrongdoing by the exchanges themselves at this time.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action because the New York Supreme Court is a court of general jurisdiction authorized to hear claims for conversion, money had and received, unjust enrichment, constructive trust, and related equitable relief.

19. This Court has personal jurisdiction over Defendants pursuant to CPLR § 302(a)(1) because Defendants transacted business within New York by directing fraudulent communications to a New York resident and by receiving and transferring cryptocurrency through financial intermediaries operating within New York, including transactions originating from Plaintiff's Coinbase account.

20. Personal jurisdiction is also proper pursuant to CPLR § 302(a)(3) because Defendants committed tortious acts outside the State that caused injury to Plaintiff within the State of New York, where Plaintiff resides and where the economic impact of Defendants' fraud was sustained.

21. Defendants purposefully availed themselves of New York's financial and commercial infrastructure by receiving and laundering cryptocurrency through exchange accounts and blockchain wallet addresses connected to cryptocurrency exchanges that conduct business in New York and within the United States financial system.

22. In addition, Coinbase Global, Inc., through which Plaintiff transferred a portion of the stolen cryptocurrency, maintains a presence in New York, including employees and a consumer assistance mailing address located at 82 Nassau St. #61234, New York, NY 10038. Plaintiff also purchased cryptocurrency through payment-processing platforms that operate in conjunction with regulated virtual currency businesses authorized to conduct operations in New York, including transactions processed through Zero Hash LLC, a virtual currency business licensed by the New York State Department of Financial Services.

23. Upon information and belief, certain cryptocurrency purchases made by Plaintiff were processed through MoonPay, a cryptocurrency payment processor that utilizes Zero Hash LLC as its regulated liquidity provider for transactions involving New York residents. Zero Hash LLC is licensed by the New York State Department of Financial Services to engage in virtual currency business activity within the State of New York. These transactions therefore utilized New York's regulated digital asset infrastructure as part of the scheme that induced Plaintiff to transfer cryptocurrency to Defendants' wallet addresses.

24. Blockchain transaction records further permit identification of the cryptocurrency exchanges and intermediary platforms through which the stolen assets were subsequently transferred, enabling discovery directed to those entities to identify the individuals controlling the recipient wallet addresses.

25. At the time Defendants induced Plaintiff to transfer the cryptocurrency at issue, those digital assets were under the custody and control of financial intermediaries operating within New York and accessible through accounts maintained by Plaintiff in this State. The conversion of those assets occurred when Defendants caused Plaintiff to transfer cryptocurrency from those

accounts to wallet addresses controlled by Defendants, thereby misappropriating property situated in New York and causing direct economic injury within this State.

26. Venue is proper in New York County pursuant to CPLR § 503(a) because Defendants conducted transactions through financial intermediaries operating in New York County and the fraudulent transfers forming the basis of this action were processed through entities maintaining a presence in New York County.

STATEMENT OF FACTS

A. Defendants' Cryptocurrency Fraud Scheme

27. This action arises from a fraudulent cryptocurrency scheme through which Defendants stole more than **$168,000** from Plaintiff by impersonating a legitimate travel company and operating a sham online "task" platform designed to induce victims to transfer cryptocurrency. Forensic blockchain tracing has verified that between October 3 and November 27, 2024, Plaintiff transferred a total of **$163,618.94** across 11 cryptocurrency transactions to Intake Wallets—the first known scam-controlled addresses to which perpetrators directed Plaintiff to send assets.

28. On or about October 1, 2024, Plaintiff was contacted through Facebook by an individual claiming to be a representative of Wendy Wu Tours and offering Plaintiff a purported work-from-home opportunity. The opportunity was presented as a "Task Gig," in which participants could allegedly earn commissions by completing online tasks associated with creating travel "trips" on a platform affiliated with Wendy Wu Tours.

29. The individual represented that Plaintiff would earn commissions for completing these tasks and that the opportunity was a legitimate remote employment arrangement associated with the well-known travel company Wendy Wu Tours. In reality, the purported opportunity was

a fraudulent scheme designed to induce Plaintiff to transfer cryptocurrency to wallet addresses controlled by Defendants.

30. Defendants' actions followed the well-known "pig butchering" fraud model[3] used in cryptocurrency scams. First, Defendants created a false identity and impersonated a representative of Wendy Wu Tours, a legitimate international travel and tour planning company whose website is located at **https://www.wendywutours.com**. Defendants instead directed Plaintiff to imposter websites located at **https://www.wendywutours-tours.com** and **https://www.wendywutours-adventure.com**, which were designed to appear affiliated with the legitimate business and mimicked the legitimate businesses' appearance.

31. The alleged Wendy Wu representative then placed Plaintiff into a Telegram chat group containing other purported "Gig" workers. These individuals appeared to describe successful experiences with the platform and claimed to earn substantial income through their Wendy Wu "Task Gigs." Members of the chat group portrayed themselves as living lavish lifestyles allegedly supported by earnings from the platform. These representations were intended to create the false impression that the opportunity was legitimate and highly profitable.

B. The Fraudulent "Trip Flow" Platform and High Rebate Tasks

[3] ProPublica has published an in-depth investigation documenting the mechanics of so-called "pig butchering" scams—an increasingly common form of cryptocurrency fraud carried out by organized criminal syndicates, often operating from overseas compounds where individuals are trafficked or coerced into perpetrating the schemes. Investigative reporting and law-enforcement advisories describe a typical progression of the scam as follows: "(1) create a fake identity; (2) initiate contact; (3) gain the target's trust; (4) enroll the victim in a purported opportunity; (5) induce the victim to deposit real funds into a fraudulent account; (6) 'prove' the platform's legitimacy through fabricated balances or small withdrawals; (7) manipulate the victim into investing increasing amounts; (8) abruptly cut off communication; (9) exploit the victim's desperation to recover funds; and (10) disappear with the stolen assets." See Cezary Podkul, *What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One*, ProPublica (Sept. 19, 2022), https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one. Federal law-enforcement agencies, including the Federal Bureau of Investigation, have likewise warned that such "pig butchering" schemes are a rapidly growing form of cryptocurrency investment fraud targeting victims through social media and messaging platforms. As described below, Defendants' conduct closely followed this widely documented fraud methodology.

32. Defendants, including an individual using the name "Ramona Zagan," represented to Plaintiff that she could earn commissions by completing online "trip flow" tasks on what appeared to be a travel booking platform. Zagan instructed Plaintiff that each "trip flow" represented a travel booking transaction generated through the platform's internal system and that Plaintiff could earn commissions by processing those transactions through the platform interface.

33. Zagan further represented that the platform required users to temporarily fund booking transactions in order for the system to process them. Plaintiff was told that once a booking transaction was completed through the platform, the deposited funds would be returned together with a commission credited to her account.

34. Zagan explained that the platform operated in structured task cycles consisting of thirty-six "trip flow" transactions. Plaintiff was told that each completed task would generate a commission reflected in her account balance and that once the full sequence of thirty-six tasks was completed she would be permitted to withdraw both her deposited funds and the commissions displayed by the platform.

35. During these task cycles the platform periodically generated transactions described as "High Rebate Trips." Zagan represented that these transactions corresponded to larger travel bookings that produced higher commissions. Plaintiff was instructed that in order to process these higher-value bookings she was required to transfer larger deposits of cryptocurrency so that the system could complete the transaction. Zagan represented that these deposits were temporary funds required to process the booking transaction and that the funds would be returned together with the higher commission once the task was completed.

36. These representations were false. The purported booking transactions were fictitious and served only as a mechanism to induce Plaintiff to transfer cryptocurrency to wallet

addresses controlled by Defendants. The platform displayed increasing balances and commissions in order to create the illusion of legitimate earnings and to induce Plaintiff to continue depositing additional cryptocurrency in the belief that her deposits were temporary funds required to process booking transactions and that those funds would be returned upon completion of the task cycle.

C. Plaintiff's Cryptocurrency Transfers

37. Through these communications, Defendants instructed Plaintiff to create a Coinbase cryptocurrency account and informed her that she would need to transfer cryptocurrency to specific wallet addresses in order to complete the tasks required by the platform. According to Defendants, the cryptocurrency deposits were necessary to "back" or fund travel "trips" that Plaintiff created through the platform.

38. Defendants represented that certain trips would return commissions of approximately 0.75 percent of the cryptocurrency invested, while other trips would generate returns of approximately six percent. Plaintiff was further told that once she completed thirty-six trips, her entire investment would be returned along with the commissions she had earned.

39. Relying on these representations, Plaintiff began transferring cryptocurrency from her Coinbase account to Intake Wallet addresses provided by Defendants beginning on or about October 3, 2024. Between October 3, 2024 and November 27, 2024, Plaintiff completed eleven transactions transferring more than $168,000 in cryptocurrency to wallet addresses controlled by Defendants.

D. Escalating Withdrawal Restrictions

40. After transferring substantial cryptocurrency in reliance on Defendants' representations, Plaintiff attempted to withdraw the funds reflected in her account balance. Beginning on or about October 29, 2024, Plaintiff attempted to withdraw funds but was informed

that her funds were "blocked" and that she would need to wait before attempting another withdrawal.

41. Plaintiff attempted again on or about November 22, 2024, after completing assigned tasks, but was informed that her account was subject to a $3,000 daily withdrawal limit unless she upgraded her membership level. On or about November 25, 2024, the platform permitted Plaintiff to withdraw $3,000 while representing that larger withdrawals were restricted by membership limits. Upon information and belief, Defendants permitted this limited withdrawal as part of their scheme to create the appearance that the platform was legitimate and to induce Plaintiff to transfer additional cryptocurrency.

42. When Plaintiff again attempted to withdraw funds on or about November 27, 2024, the platform represented that Plaintiff's account "credibility score" had fallen to 64% and that withdrawals could not be processed unless the score was restored to 100%. Upon information and belief, this purported "credibility score" requirement was fictitious and was used by Defendants to block Plaintiff's withdrawal and pressure Plaintiff to transfer additional cryptocurrency.

43. Shortly thereafter, Defendants demanded that Plaintiff transfer an additional $60,000 in cryptocurrency in order to unlock the account and process the withdrawal. Plaintiff became suspicious of Defendants' representations and refused to make the requested transfer. After Plaintiff refused to send additional cryptocurrency, Defendants ceased communicating with Plaintiff, and Plaintiff was unable to recover the cryptocurrency she had previously transferred.

44. After discovering the fraud, Plaintiff acted diligently and promptly reported the scheme to the Nassau County District Attorney's Office. Plaintiff also contacted the Federal Bureau of Investigation ("FBI") and submitted a complaint through the FBI's Internet Crime Complaint Center ("IC3"), providing information regarding the fraudulent communications, the

imposter website, and the cryptocurrency transfers associated with the scheme. Plaintiff also reported the theft to the Federal Trade Commission ("FTC").

45. Plaintiff cooperated with law enforcement and provided the documentation and information available to her. Plaintiff was informed, however, that due to the anonymous and frequently international nature of cryptocurrency fraud schemes, recovery through law enforcement channels alone was unlikely. Plaintiff has therefore been compelled to pursue civil remedies in order to identify the individuals responsible for the scheme and trace and recover the stolen cryptocurrency.

46. Blockchain records associated with the transactions described above demonstrate that Plaintiff's cryptocurrency was transferred to identifiable blockchain wallet addresses controlled or used by Defendants. Because blockchain transactions are publicly recorded on an immutable ledger, the movement of Plaintiff's funds can be traced through subsequent wallet transfers and into accounts maintained with cryptocurrency exchanges or other financial intermediaries.

47. Certain exchange-hosted wallet addresses receiving Plaintiff's cryptocurrency have been identified through forensic blockchain tracing and are listed in **Exhibit A** to Plaintiff's Proposed Order to Show Cause and Temporary Restraining Order.

48. Cryptocurrency traceable to Plaintiff's transfers that remains within these wallet addresses or accounts constitutes identifiable property and proceeds of Defendants' fraud and is therefore subject to equitable relief, including injunctive restraint and the imposition of a constructive trust.

49. Blockchain transaction records further permit identification of the cryptocurrency exchanges and intermediary platforms through which the stolen assets were subsequently

transferred, enabling discovery directed to those entities to identify the individuals controlling the recipient wallet addresses.

50. Defendants presently remain unknown and are therefore sued herein as **John Doe Nos. 1–25**, including individuals or entities who controlled the wallet addresses receiving Plaintiff's cryptocurrency and any persons who knowingly assisted in the movement, concealment, or conversion of those funds. Plaintiff intends to identify these individuals through discovery directed to cryptocurrency exchanges, financial intermediaries, messaging platforms, and other third parties that facilitated or recorded Defendants' transactions and communications.

51. The cryptocurrency transferred by Plaintiff constitutes specific and identifiable property traceable on the blockchain. To the extent Plaintiff's funds were transferred through additional wallets, exchange accounts, or other digital asset repositories, those assets represent proceeds of Defendants' fraud and are subject to recovery. Plaintiff therefore seeks the imposition of a constructive trust and other equitable relief over any cryptocurrency or assets derived from Plaintiff's transfers that are presently held by or traceable to Defendants or their agents.

52. Because cryptocurrency transactions can be rapidly transferred across multiple wallets and exchanges, there exists a substantial risk that the fraud proceeds will be dissipated, transferred, or concealed if not promptly restrained. Without judicial intervention, Defendants may continue to move Plaintiff's cryptocurrency through additional blockchain wallets and exchanges beyond the reach of the Court.

53. Blockchain tracing further indicates that portions of Plaintiff's stolen cryptocurrency were subsequently transferred through wallet addresses associated with cryptocurrency exchanges, including Coinbase, Binance, BitGet, Crypto.com, HTX, Kraken, MaskEx, Newton Canada, OKX, Revolut, Wealthsimple, and other centralized exchanges.

54. The cryptocurrency stolen from Plaintiff constitutes traceable digital property identifiable through blockchain records. To the extent such assets or their proceeds remain within identifiable wallet addresses, exchange accounts, or other digital asset repositories, those assets are subject to recovery, turnover, restitution, and equitable relief in favor of Plaintiff.

E. Structure of Defendants' Cryptocurrency Laundering Network

55. Blockchain analysis demonstrates that Defendants' scheme relied on a structured network of cryptocurrency wallets designed to receive, consolidate, and obscure stolen funds. In schemes of this type, victims are first instructed to transfer cryptocurrency to **initial Intake Wallets** controlled by the perpetrators. These intake wallets function as the first point of receipt for stolen funds.

56. From there, the stolen cryptocurrency is transferred into intermediary consolidation accounts commonly referred to as "Pivot Wallets." These wallets serve as aggregation points where funds from multiple victims are pooled together before being redistributed to additional wallets or exchange accounts.

57. After consolidation, the cryptocurrency is typically transferred through additional wallets or cryptocurrency exchanges in order to obscure the origin of the funds and facilitate laundering of the stolen assets. The presence of shared Pivot Wallets receiving deposits from numerous unrelated victims demonstrates the existence of a coordinated fraud operation rather than isolated theft.

58. As described below, forensic blockchain analysis confirms that the wallet infrastructure used to receive Plaintiff's funds also received deposits from numerous other victims following the same transaction patterns.

CLASS-WIDE IMPACT OF DEFENDANTS' FRAUD SCHEME

59. Forensic blockchain analysis confirms that the theft of Plaintiff's cryptocurrency was not an isolated incident but instead part of a coordinated and systematic fraud scheme designed to steal funds from numerous victims through the same online platform and laundering infrastructure.

60. Analysis of the blockchain transactions associated with Plaintiff's transfers reveals that the wallet addresses receiving Plaintiff's cryptocurrency were not standalone accounts but part of a broader network of intermediary wallets used to aggregate and redistribute stolen funds. These intermediary wallets, referred to by forensic analysts as Pivot Wallets function as consolidation points where cryptocurrency from multiple victims is pooled before being transferred to additional wallets or exchange accounts controlled by the perpetrators.

61. The presence of Pivot Wallets demonstrates that Defendants' conduct was not directed solely at Plaintiff but instead reflects a coordinated fraud operation targeting numerous victims using the same infrastructure. Unlike isolated thefts where funds follow unrelated transaction paths, the Pivot Wallets receiving Plaintiff's funds also contain structured inflows from multiple unrelated cryptocurrency wallets exhibiting identical transaction patterns. This consolidation confirms that funds from numerous victims were aggregated into the same intermediary wallets as part of a unified fraudulent scheme.

62. Through forensic tracing of blockchain transactions flowing into these Pivot Wallets, investigators identified numerous additional victim wallets that followed the same structured transaction pathways and laundering patterns as Plaintiff's transfers. These wallets exhibit identical characteristics, including the use of the same intermediary wallets, the same

aggregation structure, and the same onward movement of funds through laundering pathways designed to obscure the origin of the stolen cryptocurrency.

63. The consistent transaction behavior across these wallets confirms the existence of a coordinated fraud network in which Defendants used the same platform, the same laundering infrastructure, and the same intermediary wallets to misappropriate cryptocurrency from numerous victims.

64. Based on forensic analysis of deposits flowing into the identified Pivot Wallets, investigators estimate that victims collectively transferred approximately **$31,077,915** in cryptocurrency into wallets controlled by the perpetrators of this scheme.

65. Plaintiff therefore brings this action not only to recover her own stolen assets but also on behalf of similarly situated victims whose cryptocurrency was misappropriated through the same fraudulent platform and laundering infrastructure.

66. The structure and scale of the wallet activity described above demonstrate that Defendants' conduct was not directed solely at Plaintiff but instead part of an ongoing scheme targeting members of the public at large. Defendants' use of a repeatable platform, shared wallet infrastructure, and coordinated communications reflects a systemic pattern of misconduct designed to defraud numerous victims.

67. Defendants' conduct was willful, malicious, and undertaken with a high degree of moral culpability and reckless disregard of Plaintiff's rights, warranting the imposition of punitive damages.

CLASS ACTION ALLEGATIONS

68. Plaintiff brings this action pursuant to **CPLR Article 9** on behalf of herself and a class of similarly situated persons.

69. The proposed class consists of all persons who transferred cryptocurrency to wallet addresses associated with the fraudulent "Wendy Wu Tours" task platform, where such funds were subsequently traced, through blockchain analysis, to intermediary wallets (the "Pivot Wallets") and ultimately to deposits into the exchange wallet addresses identified in Exhibit A to Plaintiff's Proposed Order to Show Cause and Temporary Restraining Order.

70. Excluded from the Class are Defendants, their agents, employees, and affiliates, any entities controlled by Defendants, and the Court and its personnel.

71. The members of the Class are so numerous that joinder of all members is impracticable. Forensic blockchain analysis of the Pivot Wallets receiving victim deposits reveals that numerous unrelated wallets transferred cryptocurrency into the same intermediary wallets used to receive and redistribute Plaintiff's funds. Based on deposits traced into these Pivot Wallets, investigators estimate that victims collectively transferred **approximately $31,077,915 in cryptocurrency** into wallets controlled by Defendants.

72. Questions of law and fact common to the Class predominate over questions affecting individual members. These common questions include, among others:

a. whether Defendants operated a fraudulent online platform impersonating Wendy Wu Tours;

b. whether Defendants induced victims to transfer cryptocurrency through misrepresentations regarding "Task Gigs" and purported investment returns;

c. whether Defendants used shared cryptocurrency wallet infrastructure, including Intake Wallets and Pivot Wallets, to receive and launder victim funds;

d. whether Defendants' conduct constitutes fraud, conversion, and unjust enrichment; and

e. whether victims are entitled to restitution and equitable relief for the recovery of stolen cryptocurrency.

73. Plaintiff's claims are typical of the claims of the Class. Like other Class members, Plaintiff transferred cryptocurrency to wallet addresses associated with the fraudulent platform and suffered losses when Defendants misappropriated those funds through the same wallet infrastructure and laundering process.

74. Plaintiff will fairly and adequately represent the interests of the Class. Plaintiff has no interests antagonistic to those of other Class members and seeks to recover the same category of damages and equitable relief as other victims of Defendants' scheme.

75. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The losses suffered by many victims are dispersed across numerous jurisdictions, while Defendants used the same fraudulent platform and wallet infrastructure to perpetrate the scheme. Resolving these claims in a single proceeding will promote judicial efficiency and avoid inconsistent results.

FIRST CAUSE OF ACTION
Conversion

76. Plaintiff repeats and realleges the allegations contained in all preceding paragraphs as if fully set forth herein.

77. Plaintiff's stolen cryptocurrency constitutes identifiable intangible property that is traceable through blockchain records and associated with specific, identifiable blockchain wallet addresses.

78. Plaintiff had an immediate possessory right to the cryptocurrency transferred from her accounts.

79. Defendants intentionally exercised unauthorized dominion and control over Plaintiff's cryptocurrency by directing Plaintiff to transfer the assets to wallet addresses controlled by Defendants and thereafter transferring those assets through additional blockchain transactions in an effort to conceal their origin and current location.

80. Defendants' dominion and control over Plaintiff's cryptocurrency was inconsistent with and in derogation of Plaintiff's rights and deprived Plaintiff of the use, possession, and benefit of her property.

81. As a direct and proximate result of Defendants' conduct, Plaintiff has suffered damages in an amount to be determined at trial but believed to exceed **$168,000**, together with interest and other appropriate relief.

SECOND CAUSE OF ACTION
Money Had And Received

82. Plaintiff repeats and realleges the allegations contained in all preceding paragraphs as if fully set forth herein.

83. Defendants received Plaintiff's cryptocurrency through the fraudulent "pig butchering" scheme described above.

84. Defendants obtained and retained Plaintiff's assets under circumstances in which equity and good conscience require restitution.

85. Defendants benefited from receiving Plaintiff's cryptocurrency by transferring those assets into wallet addresses under Defendants' control and by retaining or further transferring those assets for their own benefit.

86. In equity and good conscience, Defendants should not be permitted to retain Plaintiff's stolen cryptocurrency or its proceeds.

87. Plaintiff therefore seeks restitution of the cryptocurrency transferred to Defendants, or the value thereof, together with interest and such other equitable relief as the Court deems just and proper.

THIRD CAUSE OF ACTION
Unjust Enrichment

88. Plaintiff repeats and realleges the allegations contained in all preceding paragraphs as if fully set forth herein.

89. Defendants were enriched by receiving Plaintiff's cryptocurrency through the fraudulent scheme described above.

90. Defendants' enrichment occurred at Plaintiff's expense because Plaintiff transferred her cryptocurrency in reliance on Defendants' fraudulent representations.

91. It would be against equity and good conscience for Defendants to retain the cryptocurrency or any proceeds derived from those assets.

92. Plaintiff therefore seeks restitution of the cryptocurrency transferred to Defendants, or the value thereof, together with interest and such other equitable relief as the Court deems just and proper.

FOURTH CAUSE OF ACTION
Constructive Trust

93. Plaintiff repeats and realleges the allegations contained in all preceding paragraphs as if fully set forth herein.

94. Defendants obtained Plaintiff's cryptocurrency through fraud and wrongful conduct.

95. The cryptocurrency transferred by Plaintiff constitutes identifiable and traceable digital property recorded on the blockchain.

96. Equity requires that Defendants not be permitted to retain the stolen cryptocurrency or any assets derived from those transfers.

97. Plaintiff therefore seeks the imposition of a constructive trust over any cryptocurrency or assets traceable to Plaintiff's transfers that remain in wallet addresses, exchange accounts, or other digital repositories controlled by Defendants or their agents.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and grant the following relief:

1. A judgment against Defendants for damages in an amount to be determined at trial, including but not limited to the value of Plaintiff's stolen cryptocurrency and the cryptocurrency transferred by Class members, together with pre- and post-judgment interest.

2. Restitution and disgorgement of all cryptocurrency and other assets obtained by Defendants through the fraudulent scheme described herein.

3. The imposition of a constructive trust and equitable lien over any cryptocurrency or assets traceable to Plaintiff's transfers and the transfers of Class members, including assets presently held in cryptocurrency wallets, exchange accounts, or other digital repositories controlled by Defendants or their agents.

4. An order requiring the identification of the individuals or entities controlling the cryptocurrency wallet addresses that received Plaintiff's funds, including through discovery directed to cryptocurrency exchanges, financial intermediaries, and messaging platforms that facilitated Defendants' transactions and communications.

5. An order directing the preservation and production of records relating to the cryptocurrency wallets and accounts that received Plaintiff's funds and the funds of Class members.

6. An order granting such equitable relief as necessary to trace and recover cryptocurrency or assets derived from Defendants' fraudulent scheme.

7. Certification of this action as a class action pursuant to CPLR Article 9, appointment of Plaintiff as Class Representative, and appointment of Plaintiff's counsel as Class Counsel.

8. An award of Plaintiff's costs and disbursements incurred in this action, including reasonable attorneys' fees to the extent permitted by law.

9. An award of punitive damages in an amount sufficient to punish Defendants for their willful, wanton, and egregious misconduct and to deter similar conduct in the future.

10. Such other and further relief as the Court deems just and proper.

Dated: New York, New York
May 11, 2026

THE GORI LAW FIRM, P.C.
Attorneys for Plaintiff

/s/ Samuel D. Elswick
Samuel D. Elswick, Esq.
The Gori Law Firm, P.C.
122 East 42nd Street, Suite 4700
New York, New York 10168
Phone: (321) 430-0860
Email: selswick@gorilaw.com

VERIFICATION

STATE OF NEW YORK)
) ss.:
COUNTY OF NASSAU)

I am the Plaintiff in this action. I have read the foregoing Complaint and know the contents thereof. The same is true to my knowledge except as to matters stated to be alleged upon information and belief, and as to those matters I believe them to be true.

Dated: New York, New York

May 5th, 2026

Radhika Advani
Radhika Advani

Notary Public

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