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

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

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER, EXPEDITED DISCOVERY, AND ALTERNATIVE SERVICE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Plaintiff Radhika Advani ("Plaintiff"), by and through her undersigned counsel, Samuel D. Elswick, respectfully submits this Memorandum of Law in support of her application for a preliminary injunction and temporary restraining order, pursuant to Civil Practice Law and Rules ("CPLR") §§ 6301, 6312 and 6313, enjoining Defendants John Doe Nos. 1-25 (collectively, "Defendants"), from disposing of, processing, routing, facilitating, selling, transferring, encumbering, removing, paying over, conveying or otherwise interfering with Plaintiff's property, debts, accounts, receivables, rights of payment, or tangible or intangible assets of any kind, whether such property is located inside or outside of the United States, including, but not limited to, cryptocurrency or other digital assets held in the wallet addresses identified in Exhibit A and any accounts, sub-accounts, or exchange-hosted accounts associated with or linked to those wallet addresses of the proposed Order to Show Cause ("OSC") and Temporary Restraining Order ("TRO").

Pending this Court's hearing on the preliminary injunction motion in this matter, Plaintiff seeks temporary injunctive relief prohibiting Defendants from transferring the digital assets held in the wallet addresses listed in **Exhibit A** to the proposed OSC. The requested TRO does not transfer ownership of any property but merely preserves the *status quo* by preventing the dissipation of traceable cryptocurrency pending further proceedings.

PRELIMINARY STATEMENT

This action arises from a coordinated international cryptocurrency fraud scheme commonly referred to as "pig butchering," through which Defendants induced Plaintiff Radhika Advani to transfer approximately $168,000 in cryptocurrency, of which at least $163,618.94 has been traced through blockchain analysis to wallet addresses controlled by Defendants. Further, blockchain analysis confirms that the cryptocurrency transferred by Plaintiff remains identifiable and traceable through specific wallet addresses and intermediary transactions recorded on the public blockchain ledger.

Defendants contacted Plaintiff through social media and induced her to participate in what was represented as a legitimate work-from-home opportunity involving the creation of travel "trips" on an online platform purportedly associated with the international travel company Wendy Wu Tours. In reality, the platform was a fraudulent website designed to impersonate the legitimate business and induce victims to transfer cryptocurrency to wallet addresses controlled by Defendants.

After Plaintiff transferred cryptocurrency to Defendants' designated wallet addresses, the fraudulent platform displayed fabricated balances and commissions designed to create the illusion that Plaintiff was earning profits. Defendants repeatedly represented that Plaintiff's deposits and commissions would be returned once she completed a series of online "tasks." When Plaintiff attempted to withdraw her funds, Defendants demanded additional deposits and ultimately ceased communication.

Blockchain tracing demonstrates that Plaintiff's cryptocurrency was transferred through identifiable wallet addresses and subsequently routed through intermediary wallets designed to obscure the origin of the stolen assets. Because cryptocurrency can be rapidly transferred through multiple blockchain wallets and exchanges across international jurisdictions, there exists a substantial risk that Defendants will dissipate the stolen funds unless the Court immediately restrains the relevant wallet addresses and exchange accounts.

Plaintiff therefore seeks a temporary restraining order preventing the transfer of cryptocurrency traceable to Plaintiff's funds, expedited discovery directed to cryptocurrency exchanges and financial intermediaries to identify the individuals controlling the relevant wallet addresses, and authorization for alternative service upon the currently unidentified Defendants. The facts set forth herein are drawn from the Verified Complaint, the Affidavit of Radhika Advani, the Declaration of Maya Vick, and the Affirmation of Samuel D. Elswick.

FACTUAL BACKGROUND

I. Defendants' Cryptocurrency Fraud Scheme

On or about October 1, 2024, Plaintiff was contacted through Facebook by an individual allegedly named Ramona Zagan who claimed to be a representative of Wendy Wu Tours, a legitimate international travel company. (Advani Aff. ¶¶ 4–9). The individual offered Plaintiff a purported work-from-home opportunity involving participation in an online "Task Gig." (Advani Aff. ¶¶ 4–9; Vick Decl. ¶ 11). According to Defendants, participants could earn commissions by completing tasks associated with creating travel "trips" on a platform affiliated with Wendy Wu Tours. (Advani Aff. ¶¶ 4–9; Vick Decl. ¶ 11).

Defendants directed Plaintiff to websites located at the following URLs: https://www.wendywutours-tours.com and https://www.wendywutours-adventure.com, which were designed to appear affiliated with the legitimate travel company website https://www.wendywutours.com. (Advani Aff. ¶¶ 7–9; Vick Decl. ¶¶ 4–11).

In reality, the websites were fraudulent platforms created to impersonate the legitimate business. (Vick Decl. ¶¶ 4–11; Advani Aff. ¶ 9). Defendants also placed Plaintiff in a Telegram chat group containing other purported participants who claimed to earn substantial income through the platform. (Advani Aff. ¶¶ 10–11). These individuals described lavish lifestyles allegedly supported by their participation in the platform. (Advani Aff. ¶ 12). These communications were intended to create the false impression that the opportunity was legitimate and profitable. (Advani Aff. ¶ 13).

II. Plaintiff's Cryptocurrency Transfers

Defendants instructed Plaintiff to create a cryptocurrency account through Coinbase and informed her that she would need to transfer cryptocurrency to wallet addresses designated by Defendants in order to complete the tasks required by the platform. (Advani Aff. ¶¶ 14–15).

Defendants represented that certain tasks would generate commissions of approximately 0.75 percent while other tasks would generate returns of approximately six percent. (Advani Aff. ¶¶ 16–17). Defendants further represented that once Plaintiff completed thirty-six tasks, her entire investment and commissions would be returned. (Advani Aff. ¶¶ 18–20). Relying on these representations, Plaintiff began transferring cryptocurrency from her Coinbase account to wallet addresses provided by Defendants beginning on or about October 3, 2024. (Advani Aff. ¶ 22; Vick Decl. ¶¶ 11–16).

Between October 3, 2024 and November 27, 2024, Plaintiff completed eleven cryptocurrency transfers totaling more than $163,000 to wallet addresses controlled by Defendants. (Vick Decl. ¶¶ 11–16). After each transfer, the fraudulent platform displayed account balances that appeared to increase with each transaction. (Advani Aff. ¶ 25). These balances were fictitious. (Advani Aff. ¶ 26).

After completing multiple transfers, Plaintiff attempted to withdraw the funds reflected in her account. (Advani Aff. ¶ 27). Beginning on or about October 29, 2024, Plaintiff attempted to withdraw funds but was informed that her funds were "blocked" and that she needed to wait before attempting another withdrawal. (Advani Aff. ¶ 28). On or about November 22, 2024, Plaintiff again attempted to withdraw her funds after completing assigned tasks, but she was told that her account was subject to a $3,000 daily withdrawal limit unless she upgraded her membership level. (Advani Aff. ¶ 29).

However, on or about November 25, 2024, the platform allowed Plaintiff to withdraw $3,000 from her account while continuing to represent that larger withdrawals were restricted by membership limits. (Advani Aff. ¶ 30). Plaintiff now believes that this limited withdrawal was permitted in order to create the appearance that the platform was legitimate and to encourage Plaintiff to continue depositing cryptocurrency. (Advani Aff. ¶ 31).

When Plaintiff again attempted to withdraw funds on or about November 27, 2024, she was informed that her account's "credibility score" had fallen to 64% and that withdrawals could not be processed unless the score was restored to 100%, purportedly by transferring additional cryptocurrency to Defendants. (Advani Aff. ¶ 32). Shortly thereafter, Plaintiff was told that she needed to deposit an additional $60,000 in cryptocurrency in order to unlock her account and process the withdrawal. (Advani Aff. ¶ 33; Ex. A to Advani Aff.). Plaintiff refused, at which point Defendants ceased all communication. (Advani Aff. ¶¶ 34–35).

Afterward, Plaintiff was unable to recover her stolen funds. Plaintiff promptly reported the scheme and theft of her cryptocurrency to the Nassau County District Attorney's Office, the Federal Trade Commission ("FTC"), and the Federal Bureau of Investigation ("FBI"), and submitted a complaint through the FBI's Internet Crime Complaint Center ("IC3"). (Advani Aff. ¶¶ 42–45). Plaintiff cooperated with law enforcement and provided the documentation and information available to her but was informed that because cryptocurrency fraud schemes frequently involve anonymous and international actors, recovery through law enforcement channels alone may be difficult. (Advani Aff. ¶¶ 46–47).

III. Blockchain Evidence Demonstrates Traceable Fraud Proceeds

Blockchain transaction records show that Plaintiff's cryptocurrency was transferred to identifiable wallet addresses controlled by Defendants. (Vick Decl. ¶¶ 12–40). Because blockchain transactions are permanently recorded on a public ledger, the movement of stolen cryptocurrency can be traced through successive wallet transfers and into exchange-hosted deposit accounts where the assets may be frozen pending further court order. (Vick Decl. ¶¶ 10–40, 48–49, 53). Because these transactions are permanently recorded on the blockchain ledger, the cryptocurrency transferred by Plaintiff remains identifiable and traceable through the wallet addresses and intermediary transactions described in the Vick Declaration.

Blockchain analysis further demonstrates that the wallet addresses receiving Plaintiff's funds are part of a structured laundering network used to aggregate and redistribute stolen cryptocurrency. (Vick Decl. ¶¶ 17–40). These intermediary consolidation wallets—referred to as Pivot Wallets—serve as aggregation points where funds from multiple victims are pooled together before being transferred to additional wallets or exchange accounts. (Vick Decl. ¶¶ 17–40, 41–43).

The presence of shared Pivot Wallets receiving deposits from multiple unrelated victims confirms that Defendants' scheme is part of a coordinated fraud network rather than an isolated theft. (Vick Decl. ¶¶ 41–43). Forensic analysis of deposits flowing into these Pivot Wallets indicates that victims collectively transferred approximately $31,077,915 in cryptocurrency into wallets controlled by the perpetrators of this scheme. (Vick Decl. ¶¶ 41–47, 48).

ARGUMENT

I. PLAINTIFF IS ENTITLED TO A TEMPORARY RESTRAINING ORDER

Under CPLR § 6301, a temporary restraining order may issue where the movant demonstrates (1) likelihood of success on the merits, (2) irreparable harm absent relief, and (3) that the balance of equities favors the movant. *Nobu Next Door, LLC v. Fine Arts Hous., Inc.,* 4 N.Y.3d 839, 840 [2005]. Each factor strongly supports the issuance of a temporary restraining order here.

A. Plaintiff Is Likely to Succeed on the Merits

Plaintiff's Verified Complaint asserts claims for conversion, money had and received, unjust enrichment, and the imposition of a constructive trust. The Verified Complaint and accompanying affidavits demonstrate a strong likelihood of success on each claim.

1. Conversion

Plaintiff has demonstrated a likelihood of success on her claim for conversion. The tort of conversion is established where a plaintiff shows "(1) plaintiff's possessory right or interest in the property and (2) defendant's dominion over the property or interference with it, in derogation of plaintiff's rights." *Colavito v. N.Y. Organ Donor Network, Inc.,* 8 N.Y.3d 43, 49-50 [2006] (internal citations removed). Conversion occurs where "one who owns and has the right to possession of personal property proves that the property is in the unauthorized possession of another who has acted to exclude the rights of the owner." *Dragons 516 Ltd. v. GDC 38 E 50 LLC*, 201 A.D.3d 463, 464 [1st Dep't 2022].

As set forth in the Verified Complaint and supporting affidavits, Plaintiff transferred more than $168,000 in cryptocurrency to wallet addresses designated and controlled by Defendants through the fraudulent platform impersonating Wendy Wu Tours. (Advani Aff. ¶¶ 22–23). Plaintiff plainly possessed a superior right to those digital assets. Blockchain tracing further confirms that between October 3 and November 27, 2024, Plaintiff transferred $163,618.94 in cryptocurrency across eleven transactions to intake wallet addresses provided by Defendants. (Vick Decl. ¶ 11-12).

Defendants exercised dominion over Plaintiff's cryptocurrency by directing Plaintiff to transfer those assets to wallet addresses under their control. (Advani Aff. ¶¶ 22–24; Vick Decl. ¶¶ 11–16). Because Plaintiff possessed the right to the cryptocurrency and Defendants exercised unauthorized dominion over those assets in derogation of Plaintiff's ownership rights, Plaintiff has demonstrated a strong likelihood of success on her claim for conversion.

2. Money Had and Received

Second, Plaintiff has also demonstrated a likelihood of success on her claim for money had and received. The remedy is available "if one man has obtained money from another, through the medium of oppression, imposition, extortion, or deceit, or by the commission of a trespass." *Parsa v. State*, 64 N.Y.2d 143, 148 [1984].

As described in the Verified Complaint and supporting affidavits, Defendants orchestrated a scheme to induce Plaintiff to transfer cryptocurrency through a fraudulent online platform impersonating a legitimate travel company. (Advani Aff. ¶¶ 4–9, 15–24). Plaintiff transferred substantial cryptocurrency to wallet addresses controlled by Defendants based on false representations regarding investment returns and withdrawal rights. (Advani Aff. ¶¶ 15–24). Defendants therefore received Plaintiff's property through deception and continue to retain the proceeds of those transfers. (Advani Aff. ¶¶ 22–24; Vick Decl. ¶¶ 11–16).

Because Defendants possess assets that in equity and good conscience belong to Plaintiff, Plaintiff has demonstrated a strong likelihood of success on her claim for money had and received.

3. Unjust Enrichment

Plaintiff has likewise demonstrated a strong likelihood of success on her claim for unjust enrichment. Under New York law, a claim for unjust enrichment requires proof that (1) the defendant was enriched, (2) at the plaintiff's expense, and (3) equity and good conscience require restitution. *Mandarin Trading Ltd. v. Wildenstein*, 16 N.Y.3d 173, 182 [2011]; *Georgia Malone & Co. v. Rieder*, 19 N.Y.3d 511, 516 [2012]. Courts applying New York law routinely recognize unjust enrichment claims where defendants obtain and retain property "to which he or she is not entitled." *Corsello v. Verizon N.Y., Inc.*, 18 N.Y.3d 777, 790 [2012].

Here, Defendants were enriched when they received Plaintiff's cryptocurrency transfers through the fraudulent "task" platform described above. (Advani Aff. ¶¶ 22–24; Vick Decl. ¶¶ 11–16). Those transfers were made directly to blockchain wallet addresses controlled by Defendants. (Advani Aff. ¶¶ 22–23; Vick Decl. ¶¶ 11–16). Defendants' enrichment occurred directly at Plaintiff's expense because Plaintiff transferred the cryptocurrency in reliance on Defendants' representations that the deposits were required to complete platform tasks and would be returned with commissions upon completion of thirty-six trips. (Advani Aff. ¶¶ 16–24).

Equity and good conscience require restitution because Plaintiff's transfers were induced through impersonation of a legitimate travel company, fabricated investment returns, and false promises of withdrawal rights. Moreover, blockchain records demonstrate that the cryptocurrency transferred by Plaintiff can be traced through identifiable wallet addresses and intermediary wallets used to aggregate funds from multiple victims. (Vick Decl. ¶¶ 11–42, 45, 49–51). The existence of traceable blockchain transactions further supports Plaintiff's claim that Defendants unjustly received and continue to retain the proceeds of Plaintiff's transfers.

Because Defendants obtained and retained Plaintiff's cryptocurrency through a fraudulent scheme, Plaintiff has demonstrated a strong likelihood of success on her claim for unjust enrichment.

4. Constructive Trust

Plaintiff has also demonstrated a likelihood of success on her claim for the imposition of a constructive trust over the cryptocurrency transferred to Defendants. A constructive trust is an equitable remedy designed to prevent unjust enrichment where property has been obtained under circumstances that make it inequitable for the holder to retain it. *Sharp v. Kosmalski*, 40 N.Y.2d 119, 121–123 [1976]; *Latham v. Father Divine*, 299 N.Y. 22, 26–27 [1949]. Courts commonly consider four factors in determining whether a constructive trust should be imposed: (1) a confidential or fiduciary relationship, (2) a promise, (3) a transfer made in reliance on that promise, and (4) unjust enrichment. *Sharp*, 40 N.Y.2d at 121. These factors are not rigid requirements, however, and the doctrine remains a flexible equitable remedy intended to prevent unjust enrichment.

Here, Defendants induced Plaintiff to transfer cryptocurrency to wallet addresses they controlled by falsely representing that the deposits were required to complete platform tasks and would be returned with commissions. (Advani Aff. ¶¶ 16–24; Vick Decl. ¶¶ 11–16). Blockchain records demonstrate that Plaintiff's cryptocurrency constitutes identifiable digital property traceable through specific wallet addresses and intermediary transactions. (Vick Decl. ¶¶ 12–40). Courts applying New York law recognize that constructive trusts may be imposed over identifiable assets or their proceeds where property has been obtained through fraud. *Counihan v. Allstate Ins. Co.*, 25 F.3d 109, 113 [2d Cir. 1994]. Because Defendants obtained and continue to control cryptocurrency traceable to Plaintiff's transfers through a fraudulent scheme, the imposition of a constructive trust and injunctive relief preserving those assets is appropriate.

II. PLAINTIFF WILL SUFFER IRREPARABLE HARM WITHOUT IMMEDIATE RELIEF

Plaintiff will suffer immediate and irreparable harm absent immediate injunctive relief. *See* CPLR §§ 6301, 6312, and 6313.

Because blockchain transactions are irreversible once completed, recovery of stolen cryptocurrency may become impossible or substantially impaired if the assets are transferred through additional wallets or exchanges. (Vick Decl. ¶ 52). Blockchain tracing further demonstrates that the wallets receiving Plaintiff's funds are connected to a broader laundering network involving pivot wallets that aggregate funds from multiple victims. (Vick Decl. ¶¶ 42–51). Without immediate restraint, Defendants may continue transferring Plaintiff's stolen cryptocurrency through additional wallets and exchanges, thereby frustrating Plaintiff's ability to recover the assets.

Because blockchain transactions are rapid, pseudonymous, and easily transferred across borders, New York courts recognize that digital assets are traceable and subject to immediate injunctive relief where a risk of dissipation exists. *See LCX AG v. 1.274M U.S. Dollar Coin*, 2022 N.Y. Misc. LEXIS 5852, at *8–11 (Sup. Ct. N.Y. Cnty. Aug. 21, 2022). As demonstrated in the Vick Declaration, cryptocurrency traceable to Plaintiff's transfers can be rapidly moved through additional wallets and exchanges, creating a substantial risk of dissipation absent immediate restraint. (Vick Decl. ¶¶ 5–10, 45–52).

III. THE BALANCE OF EQUITIES STRONGLY FAVORS PLAINTIFF

The balance of equities strongly favors Plaintiff. Plaintiff transferred more than $168,000 in cryptocurrency to wallet addresses designated and controlled by Defendants through the fraudulent "Wendy Wu Tours" platform. (Advani Aff. ¶¶ 22–23). Without immediate injunctive relief, there is a substantial risk that Defendants will transfer the cryptocurrency through additional blockchain transactions and dissipate the assets beyond the reach of this Court.

Plaintiff's cryptocurrency constitutes identifiable property traceable through blockchain records and associated with specific wallet addresses. Plaintiff possessed an immediate and superior right to those assets. Defendants nevertheless exercised dominion and control over Plaintiff's cryptocurrency by directing Plaintiff to transfer those assets to wallets under their control and subsequently moving the funds through additional blockchain transactions designed to conceal their origin and location.

By contrast, the requested relief merely preserves cryptocurrency traceable to Plaintiff's transfers while the identities of the perpetrators are determined. The temporary restraining order does not transfer ownership of any assets to Plaintiff but simply prevents further movement of those assets pending further proceedings. In the unlikely event Defendants establish a legitimate entitlement to the restrained assets, those assets will remain preserved while Defendants present their arguments before this Court.

Accordingly, the balance of equities overwhelmingly favors issuance of a temporary restraining order preserving cryptocurrency traceable to Plaintiff's transfers.

IV. IMMEDIATE RELIEF IS NECESSARY TO PRESERVE TRACEABLE CRYPTOCURRENCY ASSETS

Plaintiff's cryptocurrency transfers have been traced through blockchain records to wallet addresses associated with Defendants' fraudulent scheme. (Vick Decl. ¶ 49). These assets are not merely associated with blockchain wallet addresses but are held within or routed through exchange-hosted accounts under custodial control, making them amenable to immediate restraint by this Court. Although the assets are traceable, Defendants retain the ability to transfer those assets at any time and without notice. (Vick Decl. ¶¶ 45–52).

Cryptocurrency can be transferred across multiple blockchain addresses within seconds and across international jurisdictions beyond the reach of this Court. (Vick Decl. ¶ 52). If Defendants move the assets through additional wallets or exchanges, Plaintiff may be unable to recover the stolen funds.

Defendants' conduct follows the pattern commonly associated with "pig butchering" schemes, in which perpetrators induce victims to transfer cryptocurrency through fraudulent platforms and then rapidly move those assets through networks of blockchain wallets designed to conceal and dissipate the proceeds. (Vick Decl. ¶¶ 4–10, 45–52).

Absent immediate injunctive relief, there is a substantial risk that cryptocurrency traceable to Plaintiff's deposits will be transferred through additional wallets or exchange accounts, permanently frustrating recovery.

Accordingly, the Court should issue a temporary restraining order preserving cryptocurrency traceable to Plaintiff's transfers pending further proceedings in this action. Because the cryptocurrency traceable to Plaintiff's transfers constitutes identifiable property subject to equitable relief, immediate restraint of the wallet addresses listed in **Exhibit A** of the OSC and TRO is necessary to preserve the Court's ability to grant effective relief. New York courts have specifically recognized that cryptocurrency constitutes identifiable, traceable property subject to injunctive relief and restraint. *See LCX AG v. 1.274M U.S. Dollar Coin*, 2022 N.Y. Misc. LEXIS 5852, at *8–11. As explained in the Vick Declaration, Plaintiff's cryptocurrency is not only traceable but has been identified within exchange-hosted deposit wallets subject to custodial control, making immediate injunctive relief both necessary and effective.

V. ANY UNDERTAKING SHOULD BE MINIMAL

Under CPLR § 6312(b), the Court may require an undertaking to cover potential damages sustained if it is later determined that the injunction was improperly granted. However, courts retain broad discretion to set the amount of the undertaking based on the equities of the case. *See In re Total MRI Mgmt., LLC*, 11 Misc. 3d 1062(A) [Sup. Ct. Nassau Cnty. Feb. 24, 2006] (setting undertaking at $2,500); *Lelekakis v. Kamamis*, 303 A.D.2d 380, 381 [2d Dep't 2003] (trial courts possess broad discretion in fixing the amount of an undertaking). Here, any undertaking should be minimal. Similarly, a court may, in its discretion, require an undertaking before issuing a temporary restraining order. *See* CPLR § 6313(c).

The requested relief merely preserves cryptocurrency traceable to Plaintiff's transfers while the identities of the perpetrators of the fraudulent scheme are determined. The temporary restraining order does not transfer ownership of any assets to Plaintiff, does not impose any financial obligation on Defendants, and does not impose any restraint on assets unrelated to Plaintiff's transfers. Instead, it simply prevents further movement of cryptocurrency traceable to the proceeds of Defendants' alleged fraud.

Moreover, in the unlikely event that Defendants ultimately establish that they are entitled to the restrained assets, those assets will remain preserved and available pending further proceedings before this Court. Accordingly, the Court should set only a minimal undertaking, particularly where relief preserves specific, identifiable property rather than restraining general assets.

VI. PLAINTIFF SHOULD BE PERMITTED TO SERVE DEFENDANTS THROUGH APPROPRIATE ELECTRONIC MEANS

A. Alternative Service of Notice on Account Holders

Plaintiff respectfully requests authorization to serve Defendants by alternative means pursuant to CPLR § 308(5). That provision permits a court to authorize service in a manner reasonably calculated to provide notice where traditional service methods are impracticable. See *Contimortgage Corp. v. Isler*, 48 A.D.3d 732, 734 [2nd Dep't 2008]. Alternative service is particularly appropriate where defendants operate through pseudonymous blockchain wallet addresses that function as the primary means by which they receive and control the stolen assets.

New York courts have repeatedly authorized alternative electronic service where defendants operate through online or anonymous digital infrastructure. *See Baidoo v. Blood-*

Dzraku, 48 Misc.3d 309, 317 [Sup. Ct. N.Y. Cnty. 2015] [authorizing service through Facebook); *LCX AG v. 1.274M U.S. Dollar Coin*, 2022 N.Y. Misc. LEXIS 5852, at *1-4, *8-11 [Sup. Ct. N.Y. Cnty. August 21, 2022] (Decision/Order authorizing service through blockchain wallet notification).

Courts addressing cryptocurrency fraud schemes have likewise recognized that perpetrators frequently operate anonymously through blockchain wallet infrastructure and intentionally conceal their identities. *Jacobo v. Doe*, 2022 U.S. Dist. LEXIS 101504, at *15-16 [E.D. Cal. June 7, 2022]; *Heissenberg v. Doe*, 2021 U.S. Dist. LEXIS 257218, at *8 [S.D. Fla. April 22, 2021]. In such circumstances, courts have authorized service methods designed to provide notice through the same digital infrastructure used to perpetrate the fraud. *See Jacobo,* 2022 U.S. Dist. LEXIS 101504, at *19-20 (allowing plaintiff to serve expedited discovery on non-party exchanges to obtain defendants' identities and electronically serve defendants); *Heissenberg,* 2021 U.S. Dist. LEXIS 257218, at *10-11 (same).

Here, Defendants are anonymous actors operating through cryptocurrency wallets and encrypted messaging platforms, making traditional service impracticable. (Elswick Affirm. ¶ 5). Defendants communicated with Plaintiff exclusively through online messaging platforms, including Facebook, Telegram, and WhatsApp, and conducted the fraudulent scheme through a website impersonating Wendy Wu Tours. (Advani Aff. ¶¶ 4-9).

Plaintiff therefore requests authorization to serve the Order to Show Cause, Temporary Restraining Order ("TRO"), Verified Complaint, Summons, and all supporting papers upon the persons controlling the wallet addresses identified in Exhibit A and any accounts, sub-accounts, or exchange-hosted accounts associated with or linked to those wallet addresses to the proposed

OSC through the delivery of a special-purpose blockchain token or similar digital notification transmitted to those wallet addresses. (Elswick Affirm. ¶ 6).

Each service token will contain a hyperlink directing the recipient to a secure website maintained by Plaintiff's counsel containing the Court's OSC and all associated filings. (Elswick Affirm. ¶ 7). The hyperlink will include tracking functionality capable of confirming when the recipient accesses the documents. (Elswick Affirm. ¶ 7).

Because Defendants used blockchain wallet addresses and online messaging platforms to conduct the fraudulent scheme, service through those same digital channels is reasonably calculated to provide actual notice. (Elswick Affirm. ¶ 8). Accordingly, Plaintiff respectfully requests that the Court authorize alternative service through the wallet addresses identified in Exhibit A and any accounts, sub-accounts, or exchange-hosted accounts associated with or linked to those wallet addresses of the OSC, as well as through any electronic messaging platforms associated with Defendants' communications with Plaintiff. (Elswick Affirm. ¶ 9).

B. Notice by Non-Party Exchanges

Plaintiff respectfully requests that the Court direct the following cryptocurrency exchanges—Binance, BitGet, Crypto.com, HTX, Kraken, MaskEx, Newton Canada, OKX, Revolut, and Wealthsimple—and their respective agents, servants, employees, attorneys, affiliates, subsidiaries, successors, assigns, and all persons acting in concert or participation with them who receive actual notice of this OSC, to provide notice of this OSC within forty-eight (48) hours to any account holder associated with the wallet addresses identified in Exhibit A and any accounts, sub-accounts, or exchange-hosted accounts associated with or linked to those wallet addresses to the proposed OSC.

Specifically, Plaintiff requests that such exchanges be directed to:

a. Provide notice of this OSC to any customer or account holder associated with the wallet addresses identified in Exhibit A and any accounts, sub-accounts, or exchange-hosted accounts associated with or linked to those wallet addresses, including Defendants John Doe Nos. 1–25; and

b. Provide counsel for Plaintiff with a copy of such notice confirming that the notice has been transmitted.

VII. EXPEDITED DISCOVERY IS WARRANTED

Plaintiff further requests the Court allow her to serve expedited discovery on the non-party cryptocurrency exchanges: Binance, BitGet, Crypto.com, HTX, Kraken, MaskEx, Newton Canada, OKX, Revolut, and Wealthsimple for the limited purpose of identifying the account holders associated with the wallet addresses listed in **Exhibit A** of the OSC and TRO and tracing the movement of the misappropriated cryptocurrency.

Plaintiff seeks records sufficient to identify the account holders, including customer identification and know-your-customer ("KYC") documentation, associated accounts or wallet addresses reasonably believed, based on exchange records, to be controlled by the same user, transaction records reflecting transfers to or from the identified wallets, and related account access information such as IP logs and login history. (Vick Decl. ¶¶ 31–34; Elswick Affirm. ¶¶ 10-11). Expedited discovery is necessary to identify Defendants and trace the stolen assets before they can be further transferred or dissipated.

CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court grant Plaintiff's application and enter an Order to Show Cause and Temporary Restraining Order:

1. Restraining Defendants from transferring, dissipating, or otherwise disposing of cryptocurrency traceable to Plaintiff's transfers and identified in Exhibit A, including any

accounts, sub-accounts, or exchange-hosted accounts associated with or linked to those wallet addresses;

2. authorizing expedited discovery directed to cryptocurrency exchanges and financial intermediaries for the purpose of identifying the individuals controlling the relevant wallet addresses and tracing the stolen assets;
3. authorizing alternative service upon Defendants through electronic means reasonably calculated to provide notice;
4. Setting a minimal undertaking; and
5. granting such other and further relief as the Court deems just and proper.

Dated: New York, New York
May 13, 2026

Respectfully submitted,

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
Attorney for Plaintiff

Certification Pursuant to 22 NYCRR § 202.8-b

I, Samuel D. Elswick, an attorney duly admitted to practice law before the courts of the State of New York, hereby certifies that the Memorandum of Law submitted herein contains 3,150 words, excluding the parts exempted by § 202.8-b(b), and therefore complies with the word count limit set forth in 22 NYCRR § 202.8-b(a).

Dated: New York, New York
May 13, 2026

By: Samuel D. Elswick
Samuel D. Elswick