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

SHAMEELA KARMALI-RAWJI, on behalf of herself and all others similarly situated, Plaintiff, v. TRUSTWAVE.TRADE, AVIV NAFTALI, JANE DOE 1 and JOHN DOE NOS. 1-10, Defendants.	Index No. 150162/2025

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

WALDEN MACHT HARAN & WILLIAMS LLP

By: /s/ *John Curran*
John Curran
Deanna M. Paul
Walden Macht Haran & Williams LLP
250 Vesey Street, 27th Floor
New York, New York 10281
(212) 335-2030
jcurran@wmhwlaw.com
dpaul@wmhlaw.com

BISHOP PARTNOY LLP

By: /s/ *Frank Partnoy*
Frank Partnoy
Robert Bishop
1717 K Street, NW Suite 900
Washington, DC 20006
(202) 787-5769
frank@bishoppartnoy.com
bobby@bishoppartnoy.com

Attorneys for Plaintiff

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

PRELIMINARY STATEMENT

This case concerns a sophisticated online theft scheme known as "pig butchering." Using fake identities and a fake cryptocurrency trading platform, Defendants perpetrated a scheme to steal over $1.5 million in cryptocurrency from Shameela Karmali-Rawji ("Plaintiff") and similarly situated individuals. Posing as investment advisors and representatives of a fake cryptocurrency trading platform, Trustwave.trade ("Trustwave"), Defendants promised to deliver substantial returns on cryptocurrency investments including by showing victims fabricated reports of false profits. Defendants' lies caused victims to invest significant amounts of money, to reasonably believe their money was secure and earning substantial profits, and to transfer additional cryptocurrency to Defendants. In reality, the returns were fake. Defendants stole and transferred the funds through a complicated series of crypto transactions to obscure the victims' assets.

Through efforts of Plaintiff and blockchain tracing experts, Plaintiff identified cryptocurrency "wallets" in which the ill-gotten gains of Defendants' scheme are *presently* held. Time is of the essence. Defendants can transfer the stolen cryptocurrency at a moment's notice, likely beyond the ability to trace and the reach of Plaintiff or the Court. Plaintiff thus seeks immediate injunctive relief, without notice to Defendants, freezing the cryptocurrency wallets in which the proceeds of the "pig butchering" scheme are presently held. Anything short of emergency relief will leave Plaintiff and her similarly situated class members chasing ghosts, and without an adequate remedy at law.

As explained below, Plaintiff, individually and on behalf of those similarly situated, is likely to prevail on the merits of her claims that Defendants perpetrated fraud and converted her funds and cryptocurrency. Plaintiff and the putative class members will suffer immediate and irreparable harm absent injunctive relief, as the aim of Defendants' scheme is to quickly and

irreversibly place assets out of Plaintiff's and this Court's reach, which they will accomplish without this Court's intervention. Absent an injunction, Plaintiff will be left with no remedy, let alone an adequate one. The Defendants' true identities are unknown as they used stolen identities throughout the scheme. Finally, the balancing of equities tilts heavily toward intervening to stop an ongoing criminal scheme and freezing assets pending a full and final disposition of the merits of this case. Absent immediate injunctive relief, Plaintiff and similarly situated class members will have no remedy or recourse for millions of dollars' worth of cryptocurrency stolen through Defendants' scheme.

New York courts have considered similar threats of cryptocurrency theft and have immediately enjoined defendants from transferring stolen property. See, e.g., Chait v. Lee, Index No. 159881/2024, NYSCEF Doc. No. 16 (N.Y. Sup. Ct. Oct. 25, 2024) (Kingo, J.) (issuing temporary restraining order freezing stolen crypto assets); Pouyafar v. John Doe Nos. 1-25, Index No. 654820/2023, NYSCEF Doc. No. 8 (N.Y. Sup. Ct. Sept. 29, 2023) (Silvera, J.) (issuing temporary restraining order freezing stolen crypto assets); id. at NYSCEF Doc. No. 17 (N.Y. Sup. Ct. Oct. 19, 2023) (Latin, J.) (issuing preliminary injunction order freezing crypto wallet); id. at NYSCEF Doc. No. 37 (N.Y. Sup. Ct. Dec. 18, 2023) (Latin, J.) (issuing temporary restraining order freezing an additional 24 wallets); id. at NYSCEF Doc. No. 47 (N.Y. Sup. Ct. Feb. 15, 2024) (Latin, J.) (issuing preliminary injunction order freezing same wallets); LCX AG v. John Doe Nos. 1-25, Index No. 154644/2022, NYSCEF Doc. No 15 (N.Y. Sup. Ct. June 2, 2022) (Masley, J.) (issuing temporary restraining order freezing stolen crypto assets). As in those cases, Plaintiff is entitled to a temporary restraining order ("TRO") and preliminary injunction to prevent Defendants from transferring assets in the crypto wallets listed in Appendix A of the Complaint (the "Deposit Wallets") and thereby forever depriving Plaintiff and putative class members of the Defendants'

stolen assets.

FACTUAL BACKGROUND

The following facts are set forth in the Affirmations of Shameela Karmali-Rawji ("KA"), Adam Zarazinski ("ZA"), and John Curran ("CA").

A. "Pig Butchering" Explained

"Pig butchering" is a scheme in which scammers promise victims returns on cryptocurrency investments and then fabricate evidence of positive performance on those investments through fake websites made to look like functioning cryptocurrency trading venues or investment companies. The "butcherers" do so to entice victims to "invest" more money. Once victims have been sufficiently "fattened" with false profits, scammers steal the victims' cryptocurrency and cover their tracks by moving the stolen property through a maze of subsequent transactions. "Pig butchering" victims in the United States have lost billions of dollars and are the subject of state and federal investigations and prosecutions.

B. Defendants "Pig Butcher" Plaintiff

Plaintiff is a physician. (KA ¶ 3.) Plaintiff was the victim of a pig butchering scheme perpetrated by Defendants, in which Defendants induced Plaintiff to provide them with over $1.5 million U.S. dollars for investment by posing as financial advisors or representatives of a fake cryptocurrency investment platform. Between September 2024 and November 2024, Defendants instructed Plaintiff to engage in purportedly profitable cryptocurrency trades, which were in fact fictitious. When Plaintiff attempted to withdraw her funds, Defendants deployed several mechanisms to cover their tracks and delay Plaintiff from uncovering the fraud, including fabricating account compliance holds, demanding withdrawal fees, and returning counterfeit cryptocurrency assets called Classic USDC, which were designed to resemble legitimate coins but were valueless. On September

3, 2024, Plaintiff enrolled in an online cryptocurrency trading course offered by Coursados for $149 Canadian Dollars ("CAD"). (KA ¶ 4). Shortly after signing up, she received a call from Jane Doe 1, an individual falsely identifying herself as "Catherine Dubois" who claimed to represent Coursados and Trustwave. Id. Jane Doe 1 described Trustwave as a legitimate cryptocurrency trading platform, leveraging advanced Artificial Intelligence ("AI") technology and suggesting that Plaintiff apply her course fee toward Trustwave. Id. Jane Doe 1 introduced Plaintiff to an individual she called "Aviv Naftali," describing him as a licensed broker who would provide personalized investment guidance and direct access to Trustwave's platform. Id.

An individual falsely identifying himself as Aviv Naftali ("Defendant Naftali"), contacted Plaintiff via WhatsApp audio on September 4, 2024. (KA ¶ 5). He claimed to be a seasoned financial advisor and crypto strategist. Id. Later that day, Plaintiff received an email from "support@trustwave.trade" requesting feedback on her initial conversation with "Aviv Naftali, your broker at Trustwave." Id.

Between September 3, 2024, and November 19, 2024, Defendant Naftali cultivated Plaintiff's trust through frequent WhatsApp messages and hours-long phone calls. (KA ¶¶ 6-7). Defendant Naftali provided Plaintiff with step-by-step guidance on how to create accounts on legitimate cryptocurrency exchanges, including Newton Crypto Ltd. ("Newton"), Payward Inc. (d.b.a. "Kraken"), Coinbase Global, Inc. ("Coinbase") and Satstreet Trading Desk Inc. ("Satstreet"). Id. Defendant Naftali also instructed Plaintiff to transfer funds into a Ledger wallet, claiming it was critical for securing her investments. Id. Defendant Naftali later directed Plaintiff to purchase cryptocurrency on these legitimate exchanges, transfer those funds to her Ledger wallet, and subsequently transfer the funds into Trustwave for purported trading activity. Id. Then, Defendants returned a counterfeit cryptocurrency asset, "Classic USDC," to Plaintiff. Id. These

were necessary to the success of Defendants' fraudulent scheme, so Plaintiff could transfer fiat currency to these legitimate platforms and convert fiat currency into various cryptocurrencies, including stablecoins like USDC. Ultimately, at the behest of Defendants, Plaintiff transferred the cryptocurrencies to the fraudulent exchange they controlled named Trustwave. Id.

On October 14, 2024, Plaintiff made her first investment of $10,000 CAD, transferring funds to Trustwave for trading under Defendant Naftali's direction. (KA ¶ 8). Defendant Naftali shared a fabricated Client Report reflecting alleged profits, withdrawals, and trades, including a $533 USD gain. Id. The professional appearance of this report bolstered Plaintiff's trust in Defendant Naftali and confidence in Trustwave's legitimacy. Id.

On October 16, 2024, Defendant Naftali spent over two hours on a call with Plaintiff, guiding her through the purchase of $35,966.98 USDC on Newton and then directing her to transfer the full amount to Trustwave. (KA ¶ 9). Later that evening, during an additional one-hour call, Defendant Naftali walked Plaintiff through executing trades on Trustwave, reinforcing the appearance of the platform's legitimacy. Id.

Between October 17, 2024, and October 23, 2024, Plaintiff traveled from Canada to New York, where she stayed in New York County. (KA ¶ 10). During this period, Plaintiff conducted frequent trades on Trustwave under Defendant Naftali's guidance and direction. Id. Plaintiff withdrew genuine USDC from her Trustwave and transferred it to her ledger wallet ("Ledger Wallet"). Id. This reinforced Plaintiff's confidence in Defendants. Id. For example, on October 20, 2024, while located in New York, Plaintiff transferred $36,377.1 USDC from Ledger Wallet to Trustwave, during a two-hour phone call with Defendant Naftali, who assured her of increasing profits. Id. Later that day, at Defendant Naftali's direction, Plaintiff withdrew $36,914.85 USDC from Trustwave and sent it to Ledger Wallet; the amount reflected a trading profit of $537.75

USDC. Id. Similarly, on October 23, 2024, while located in New York, Plaintiff transferred an additional $36,914.85 USDC from Ledger Wallet to Trustwave, and continued trading under Defendant Naftali's guidance. Id. Later that day, at Defendant Naftali's direction, Plaintiff withdrew $37,103.56 USDC from Trustwave and sent it to Ledger Wallet; the amount reflected a trading profit of $188.76 USDC. Id.

Over October 31, 2024, and November 1, 2024, Defendants directed Plaintiff to transfer $1,500,277 in USDC from Ledger Wallet to Trustwave. (KA ¶ 11). Immediately thereafter, during multiple calls spanning four hours, Defendant Naftali directed Plaintiff's trading activity with those funds. Plaintiff advised Defendant Naftali that she intended to transfer USDC from her Trustwave accounts back to her Ledger Wallet. Id. Unbeknownst to Plaintiff and contrary to her instructions, between November 1, 2024, and November 5, 2024, Defendants returned Fantom USDC, a cryptocurrency asset designed to resemble genuine USDC but is worth a fraction of its value. Id.

On November 14, 2024, Plaintiff attempted to withdraw funds from Trustwave. (KA ¶ 12). Later that day, Plaintiff received a notification from Trustwave about strange activity occurring on Trustwave from her desktop and mobile devices. Id. Trustwave stated that it had to perform a compliance check and requested bank statements and identification, both of which Plaintiff provided. Id. Trustwave informed Plaintiff that it would place a compliance hold on her assets at Trustwave for several days, preventing her from recovering her assets, and requested a withdrawal fee (called "gas" in the crypto industry) from Plaintiff to facilitate the return of her assets. Id.

On November 16, 2024, after Plaintiff transferred the withdrawal fee of approximately $10,000 USD in crypto assets to Trustwave, Plaintiff attempted to withdraw the entire amount of

investment held at Trustwave, namely, $1,544,237 USDC. (KA ¶ 13). At the time, Plaintiff believed she had successfully withdrawn $1,544,237 USDC from her Trustwave account and transferred it to Ledger Wallet. (KA ¶ 14). In reality, Defendants replaced Plaintiff's $1,544,237 USDC with counterfeit Classic USDC, a fraudulent coin that lacked any actual market value, while Plaintiff's funds were in Trustwave's control. Id. Because Classic USDC appeared identical to genuine USDC, Plaintiff was deceived into believing that she securely held assets of value, while Defendants effectively concealed their theft. Id.

Blockchain analysis confirmed that the counterfeit Classic USDC tokens originated from a single wallet, Wallet 0x4db, which also sent Classic USDC to approximately 115 other wallets. (ZA ¶ 18).

In a November 14, 2024 email, the Swiss Financial Market Supervisory Authority ("FINMA") confirmed that (1) Trustwave.trade does not have a FINMA license; (2) the company number listed is not in the name of Trustwave.trade; and (3) there is no information or entry in the Swiss commercial register that would indicate a presence in Switzerland. (KA ¶ 16). This directly contradicts Trustwave's website, which says that Trustwave is registered in Switzerland under the name "Trustwave" with the company number CHE-476.213.688, and registered with FINMA under the number F01424921. Id.

Additionally, Plaintiff discovered other fraudulent and misleading representations made by Defendants, including fabricated personas and false contact information. (KA ¶ 17). For example, the Canadian contact number listed on Trustwave's website is inoperative, despite advertising 24/7 availability, and Trustwave lists an imaginary office address for its AI trading product. Id. Trustwave's website also misappropriates a photo of Rabbi Ari Shishler, referring to him as the

company founder and a legitimate financial advisor. Defendant Naftali sent Plaintiff a fake Israeli driver's license, bearing the same photo of Rabbi Ari Shishler, with the name Aviv Naftali. Id.

C. Blockchain Expert Inca Digital Confirms the Scheme and Traces the Stolen Assets

After Plaintiff was unable to recover her funds, she contacted Inca Digital ("Inca"), a digital market investigation firm. Inca's investigation revealed that Defendants orchestrated a scheme to steal money from Plaintiff and similarly situated Class Members. (ZA ¶¶ 6-7). The investigation determined that these stolen funds were transferred to cryptocurrency wallets under Defendants' control, which are listed in Appendix A of the Complaint. Id.

Inca's investigation revealed that Defendants used Trustwave, a fictitious platform, to move and convert Class Members' assets, transferring the funds through a series of transactions designed to obscure their origins. (ZA ¶¶ 9-10). Inca's tracing analysis followed these transactions to cryptocurrency wallets held on the Binance cryptocurrency exchange. Those wallets are listed in Appendix A. Id.

Inca's investigation employed rigorous blockchain forensic techniques. Inca's "forward tracing" analysis began tracking the flow of funds by examining transfers from Plaintiff to the addresses given by Defendants, and then tracking subsequent transfers. (ZA ¶ 11). This process involved three steps: (1) identifying the addresses of wallets that initially received Plaintiff's assets; (2) tracking the subsequent transfer of those assets to intermediary addresses; and (3) determining that Plaintiff's assets were ultimately deposited into the wallets listed in Appendix A. Id.

Through this analysis, Inca uncovered further wallet addresses involved in the diversion of Plaintiff's funds, revealing a broader network of wallets involved in the scam. (ZA ¶ 12). The interactions between the wallets in the identified network are highly indicative of fraudulent

activity. (ZA ¶ 13). Specifically, the network contains wallets engaging in behavior that is associated with cryptocurrency fraud schemes and is rarely, if ever, associated with legitimate cryptocurrency transactions. Id. First, the network contains "Pivot Addresses," which mix funds and serve as hubs for numerous transport channels. Id. They accumulate funds from various transport nodes and forward larger amounts to 3-4 other transport nodes. Id. Typically, each scheme has only one to a handful of Pivot Addresses, and the funds this address receives eventually end up on exchange wallets after passing through a few additional wallets in the network. Id. Additionally, sources of funds for these addresses often include wallets already flagged for scam activity, gambling, darknet involvement, or inclusion in sanction lists. Id. Overall, the interactions between different wallets in the network provide a high degree of confidence that the entire network exists as part of the scam and is controlled by Defendants. Id. Second, "Transport Addresses" are present in the scam. (ZA ¶ 14). "Transport Addresses" are designed to forward everything they receive to frustrate tracing. Id.

Based on its analysis, and on information and belief, Inca concluded that the Class Members include approximately 115 wallets. (ZA ¶¶ 20-22).

The Zarazinski Affirmation sets forth an analysis of the methodology and support for Inca's conclusions concerning tracing Plaintiff's and the putative Class Members'. The bottom line is that Plaintiff's and the Class Members' funds stolen by Defendants were sent to the cryptocurrency wallets listed in Appendix A of the Complaint. (See also ZA at ¶ 7, Appendix A).

D. Plaintiff Files Her Complaint in This Action

On January 6, 2025, Plaintiff filed her Complaint on behalf of herself and other similarly situated victims of Defendants' scheme. (NYSCEF Doc. No. 1 (Summons and Complaint)). In it, Plaintiff asserts claims for (1) Declaratory Judgment; (2) Fraud; (3) Conversion; (4) Money Had and Received; and (5) Unjust Enrichment. (Id.)

LEGAL STANDARD

The Court may grant a preliminary injunction ("PI") where:

> [T]he defendant threatens or is about to do, or is doing or procuring or suffering to be done, an act in violation of the plaintiff's rights respecting the subject of the action, and tending to render the judgment ineffectual, or in any action where the plaintiff has demanded and would be entitled to a judgment restraining the defendant from the commission or continuance of an act, which, if committed or continued during the pendency of the action, would produce injury to the plaintiff.

CPLR § 6301.

The Court may grant a TRO pending a hearing for a preliminary injunction "where it appears that immediate and irreparable injury, loss or damage will result unless the defendant is restrained before the hearing can be had." Id.

"A party seeking a preliminary injunction must demonstrate, by clear and convincing evidence, (1) a likelihood of success on the merits, (2) irreparable injury absent the granting of the preliminary injunction, and (3) a balancing of the equities in the movant's favor." Gilliland v. Acquafredda Enters., LLC, 92 A.D.3d 19, 24 (1st Dep't 2011).[1] "New York courts do not apply the three-prong test uniformly and mechanically. The analysis is one designed to be flexible and remedies are often tailored to the facts of a specific case." Destiny USA Holdings, LLC v. Citigroup Glob. Markets Realty Corp., 24 Misc. 3d 1222(A), at *8 (Sup. Ct. Onondaga Cnty. 2009). Ultimately, "[t]he decision to grant or deny a preliminary injunction lies within the sound discretion of the trial court." Gilliland, 92 A.D.3d at 24.

ARGUMENT

Plaintiff meets the requirements for a preliminary injunction and TRO because (1) Plaintiff is likely to succeed on the merits, (2) Plaintiff will almost certainly suffer the irretrievable loss of

[1] Unless noted otherwise, internal citations, quotation marks, alterations, and footnotes have been omitted.

her crypto assets if a TRO and preliminary injunction are not granted because Defendants can easily and instantaneously transfer the funds beyond the Court's or Plaintiff's reach, and (3) the balance of equities weighs in Plaintiff's favor due to (a) the enormous harm Plaintiff will suffer absent the sought relief, (b) that Defendants are engaged in a criminal enterprise to steal cryptocurrency from innocent victims, and (c) the minimal harm Defendants will suffer from the temporary freezing of their crypto assets.[2]

I. THIS COURT SHOULD GRANT A TEMPORARY RESTRAINING ORDER WITHOUT NOTICE AND ORDER DEFENDANTS TO SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE

A. Plaintiff and Other Class Members Have a High Probability of Success on the Merits.

1. Fraud

Plaintiff has demonstrated a high probability of success on the merits of her claim for fraud, which requires a showing that the Defendants made (1) a material misrepresentation of a fact, (2) knowledge of its falsity, (3) an intent to induce reliance by the plaintiff, and (4) damages. Eurycleia Partners, LP v. Seward & Kissel, LLP, 12 N.Y.3d 553, 559 (2009). Defendants defrauded Plaintiff by falsely representing that Trustwave was a legitimate cryptocurrency trading platform, fabricating personas and falsely holding themselves out to be legitimate representatives of Trustwave, and inducing Plaintiff to tender her cryptocurrency assets to Defendants. (KA at ¶¶ 6–18; ZA at ¶¶ 6–31). Defendants intended to induce reliance on these misrepresentations to deprive Plaintiff of her assets and successfully caused her damages. Accordingly, she has shown a high likelihood of success on her claim for fraud. See, e.g., Astrove, 2022 WL 2805315, at *2–3 (granting TRO to freeze cryptocurrency assets and holding that plaintiff adequately established

[2] In the unlikely event that any legitimately acquired crypto assets are inadvertently frozen, the Court could quickly unfreeze them.

claim for fraudulent inducement based on defendants' cryptocurrency scheme); Blum v. Defendant 1, 2023 WL 8880351, at *2–3 (granting preliminary injunction on similar basis).

2. Conversion

Plaintiff has demonstrated a high probability of success on the merits of her claim for conversion. According to the Court of Appeals, "conversion takes place when someone, intentionally and without authority, assumes or exercises control over personal property belonging to someone else, interfering with that person's right of possession." Colavito v. New York Organ Donor Network, Inc., 8 N.Y.3d 43, 49–50 (2006). To succeed on a claim for conversion, a plaintiff must prove "(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." Core Dev. Grp. LLC v. Spaho, 199 A.D.3d 447, 448 (1st Dep't 2021). Defendants' theft of cryptocurrency belonging to Plaintiff and putative class members (KA at ¶¶ 6–18; ZA at ¶¶ 6–31) and use of a complicated series of transactions to move that cryptocurrency beyond the reach of its rightful owners clearly establishes a conversion. Other courts addressing stolen cryptocurrency in similar circumstances have likewise found that plaintiffs met their burden of demonstrating a likelihood of success on their conversion claim. See, e.g., Chow v. Defendant 1, No. 24-CV-480, 2024 WL 1639029, at *2 (E.D. La. Apr. 16, 2024) (finding plaintiff demonstrated likelihood of success of New York law conversion claim on the merits and granting TRO freezing stolen crypto assets); Astrove v. Doe, No. 22-CV-80614-RAR, 2022 WL 2805315, at *2–3 (S.D. Fla. Apr. 22, 2022) (granting ex parte temporary restraining order in a cryptocurrency scheme, finding that the "[p]laintiff has shown a strong likelihood of success on the merits of his claims," including a claim for conversion); Blum v. Defendant 1, No. 3:23-cv-24734-MCR-HTC, 2023 WL 8880351, at *3 (N.D. Fla. Dec. 23, 2023) (granting preliminary injunction and holding that "[t]he stolen cryptocurrency assets are

specific and identifiable property and have been traced to Defendants' Destination Addresses"); Yogaratnam v. Dubois, No. CV 24-393, 2024 WL 758387, at *3 (E.D. La. Feb. 23, 2024) (plaintiff likely to succeed on merits of conversion claim because "[i]t appears from the record that Defendants have no right to claim either possession or ownership of the stolen assets, and Defendants' taking of the funds is clearly inconsistent with Plaintiff's rights of ownership").

3. Money Had and Received

Plaintiff has similarly demonstrated a high probability of success on the merits of her claim for money had and received. "Although the action is recognized as an action in implied contract. . . it is an obligation which the law creates in the absence of agreement when one party possesses money that in equity and good conscience he ought not to retain and that belongs to another." Parsa v. State, 64 N.Y.2d 143, 148 (1984). "The elements of money had and received are (1) the defendant received money belonging to the plaintiff, (2) the defendant benefitted from receipt of the money, and (3) under principles of equity and good conscience, the defendant should not be permitted to keep the money." Cordaro v. AdvantageCare Physicians, P.C., 208 A.D.3d 1090, 1094 (1st Dep't 2022). For more than a century, the cause of action for "money had and received" has entitled a plaintiff who is the equitable owner of assets to recover from a defendant who possesses those assets. See Roberts v. Ely, 113 N.Y. 128, 131–32 (1889).

Here, Defendants received money that belonged to Plaintiff and putative class members (KA at ¶¶ 6–18; ZA at ¶¶ 6–31), and Defendants benefited from receipt of the cryptocurrency by misappropriating it. (Id.) In light of Defendants' criminal scheme, Plaintiff has demonstrated that principles of equity and good conscience demand that the cryptocurrency be returned to its rightful owners.

4. Unjust Enrichment

Finally, Plaintiff has demonstrated a high probability of success on her claim for unjust

enrichment. "Unjust enrichment lies as a quasi-contract claim and contemplates an obligation imposed by equity to prevent injustice" and is "rooted in the equitable principle that a person shall not be allowed to enrich themselves unjustly at the expense of another." Columbia Memorial Hosp. v. Hinds, 38 N.Y.3d 253, 275 (2022). To recover under a theory of unjust enrichment, a plaintiff must show that "(1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered." Id.

That standard is amply met: Defendants unjustly enriched themselves at Plaintiff's expense by misappropriating her cryptocurrency assets under false pretenses. Defendants have no legitimate claim of right to those assets, and it would violate equity and good conscience to permit Defendants to retain them. See, e.g., Blum v. Defendant 1, 2023 WL 8880351, at *3 (holding plaintiff established substantial likelihood of success on merits of unjust enrichment claim and awarding preliminary injunctive relief to freeze cryptocurrency assets); Astrove v. Doe, 2022 WL 2805315, at *2–3 (granting TRO on unjust enrichment claim and freezing cryptocurrency assets).

B. Plaintiff and Similarly Situated Class Members are Likely to Suffer Irreparable Harm Absent a TRO and Preliminary Injunction.

New York courts routinely find the risk that defendants will dispose of assets, thereby rendering judgment ineffective, constitutes irreparable harm. See, e.g., H.I.G. Cap. Mgmt., Inc. v. Ligator, 233 A.D.2d 270, 271 (1st Dep't 1996) ("The uncontrolled disposal of respondents' assets, which might render an award ineffectual, presents the risk of irreparable harm."); Zonghetti v. Jeromack, 150 A.D.2d 561, 562 (2d Dep't 1989) ("the uncontrolled sale and disposition by the defendants of their assets would threaten to render ineffectual any judgment which the plaintiffs might obtain"). That is especially true where the subject of the preliminary injunction is funds or property that defendant has allegedly converted from plaintiff. See Punwaney v. Punwaney, 148

A.D.3d 489, 489–90 (1st Dep't 2017) (preliminary injunction against transfer of funds in subject accounts); Republic of Haiti v. Duvalier, 211 A.D.2d 379, 386–87 (1st Dep't 1995) (same); see also Wallkill Med. Dev., LLC v. Catskill Orange Orthopaedics, P.C., 131 A.D.3d 601, 602–03, 605 (2nd Dep't 2015) (granting preliminary injunctions against defendants to prevent defendants from disposing of assets).

Courts in other jurisdictions have repeatedly held that cryptocurrency theft schemes threaten imminent and irreparable loss absent injunctive relief. As the court in Jacobo v. Doe noted, "courts have found [] the risk of irreparable harm to be likely in matters concerning fraudulent transfers of cryptocurrency due to the risk of anonymous and speedy asset dissipation." No. 1:22-cv-00672-DAD-BAK (BAM), 2022 WL 2052637, at *5 (E.D. Cal. June 7, 2022). That is because "it would be a simple matter for [defendant] to transfer" cryptocurrency "to unidentified recipients outside the traditional banking system . . . and effectively place the assets at issue in this matter beyond the reach of this court." Id.; see also Gaponyuk v. Alferov, No. 2:23-cv-01317-KJM-JDP, 2023 WL 4670043, at *3 (E.D. Cal. July 20, 2023) (same); Blum v. Defendant 1, 2023 WL 8880351, at *3 ("Given the speed with which cryptocurrency transactions are made as well as the anonymous nature of those transactions, the Defendants could abscond with or dissipate the cryptocurrency assets they fraudulently obtained before [plaintiff] can otherwise obtain the equitable relief he seeks in the Complaint."); Bullock v. Doe, No. 23-CV-3041 CJW-KEM, 2023 WL 9503380, at *5 (N.D. Iowa Nov. 3, 2023) ("[O]nce defendants are served, it is near certain that they will convert the stolen cryptocurrency into an untraceable currency, send it to other addresses, or transfer it beyond the reach of any forensic methods for recovery."); Hikmatullaev v. Villa, No. 23-cv-22338-ALTMAN/Reid, 2023 WL 4373225, at *3 (S.D. Fla. June 28, 2023), report and recommendation adopted, No.

23-CV-22338, 2023 WL 4363566 (S.D. Fla. July 6, 2023) (finding irreparable harm because of the "likely danger that if Defendants' assets are not frozen, the cryptocurrency assets Defendants fraudulently obtained and still retain may be absconded with or otherwise dissipated before Plaintiffs can obtain the relief sought in the Complaint"); Astrove v. Doe, 2022 WL 2805315, at *3 (granting TRO and finding "it is imperative to freeze [defendants' crypto wallets] to maintain the *status quo* to avoid dissipation of the money illegally taken from Plaintiff"); Heissenberg v. Doe, No. 21-CIV-80716-ALTMAN/Brannon, 2021 WL 8154531, at *2 (S.D. Fla. Apr. 23, 2021) ("Plaintiff has good reason to believe the Defendant will hide or transfer his ill-gotten gains beyond the jurisdiction of this Court unless those assets are restrained."); Fitzgerald v. Defendant 1, No. 24-21925-CV, 2024 WL 3537916, at *2 (S.D. Fla. June 12, 2024) ("the verified complaint establishes that the stolen assets could be transferred from the Destination Addresses at any time, making time of the essence"); Chow v. Defendant 1, 2024 WL 1639029, at *2 ("because of the anonymity and speed at which cryptocurrency transactions have the potential to be made, a TRO is necessary to prevent Defendant 1 from transferring Plaintiff's allegedly stolen assets into unreachable or unidentifiable digital wallets") Yogaratnam v. Dubois, 2024 WL 758387, at *4 ("Plaintiff's potential recovery of assets will disappear if Defendants transfer the allegedly stolen assets into inaccessible digital wallets, which could occur at any moment.").

Courts have similarly held that a money judgment is an *inadequate* legal remedy based both on the defendants' anonymity and the difficulty of tracing cryptocurrency transfers. See, e.g., Bullock v. Doe, 2023 WL 9503380, at *5. As the Bullock Court reasoned, "[i]f defendants will likely convert the crypto to a place where plaintiff can no longer find it or find defendants themselves, plaintiff in fact likely does not have an adequate legal remedy, because a money damages judgment would be essentially meaningless." Id. (holding "plaintiff has shown he will

suffer irreparable harm absent a TRO" in such circumstances). The Court noted that this was particularly the case where "plaintiff has been unable to identify the people behind the alleged scheme." Id.

The same is true here. Defendants' identities are either unknown or false. As in Bullock, a money judgment against them is meaningless. Absent an injunction, Defendants can be expected to continue to transfer Plaintiff's and the other Class Members' cryptocurrency beyond the reach of discovery and this Court. Absent a TRO and preliminary injunction, Plaintiff and the other Class Members will be left with no adequate legal remedy.

C. The Balance of Equities Favors Plaintiff.

The balance of equities favors Plaintiff and putative class members. First, Plaintiff and putative class members will suffer extraordinary harm from the failure to preserve the status quo because Defendants will almost certainly move the stolen cryptocurrency beyond the reach of the Court absent a TRO and preliminary injunction. Defendants will suffer only the inconvenience of having the cryptocurrency temporarily frozen—which can be addressed if any Defendant appears and presents evidence of ownership—pending the final disposition of this matter. New York courts have found the equities to tilt in favor of a preliminary injunction where the relative harm weighs so clearly in Plaintiff's favor. See Kurtz v. Zion, 61 A.D.2d 778, 778 (1st Dep't 1978) ("damage to plaintiffs from denial of the preliminary injunction and delivery of the stock out of escrow to defendants . . . would cause substantially greater harm to plaintiffs if they are ultimately proved right in this action, than the harm that would be caused to said defendants by the granting of the preliminary injunction if the defendants are ultimately proved right"); Clarion Assocs., Inc. v. D.J. Colby Co., 276 A.D.2d 461, 463 (2d Dep't 2000) (granting preliminary injunction where "failure to grant preliminary injunctive relief would cause greater injury to it than the imposition of the injunction would cause to the defendant").

Second, Plaintiff and putative class members are victims of Defendants' criminal scheme to steal cryptocurrency. New York courts routinely find the balance of equities tip in plaintiff's favor when the defendant is allegedly engaged in illegal conduct. See, e.g., Williams v. Hertzwig, 251 A.D.2d 655, 656 (2d Dep't 1998) (balance of equities tipped in favor of plaintiff where defendant was operating illegal dog kennel); City of New York v. Smart Apartments LLC, 39 Misc. 3d 221, 233 (Sup. Ct. N.Y. Cnty. 2013) ("the equities lie in favor of shutting down an illegal, unsafe, deceptive business practice, rather than in allowing said business to continue to operate (to defendants' presumed financial advantage)"); Banana Kelly Cmty. Imp. Ass'n v. Schur Mgmt. Co., 34 Misc. 3d 1207(A) (Sup. Ct. Bronx Cnty. 2012) (granting preliminary injunction where plaintiff argued that "the balance of the equities favor them in that without a preliminary injunction, [defendant] will continue its illegal conversion of rents due to [plaintiff] during the crucial early month rent collection period"); City of New York v. Land & Bldg. Known as 634 Nostrand Ave., 81 Misc. 3d 1224(A) (N.Y. Sup. Ct. Kings Cnty. 2023) ("the equities favor the City, especially since this case involves the alleged illegal sale of marijuana to minors").

Courts in other jurisdictions that have directly addressed cryptocurrency theft have weighed the respective harms to plaintiffs and defendants and found in favor of a preliminary injunction. As the Court in Jacobo held, balancing of these harms favors Plaintiff: "A delay in defendant's ability to transfer the assets only minimally prejudices defendant, whereas withholding injunctive relief would severely prejudice plaintiff by providing defendant time to transfer the allegedly purloined assets into other accounts beyond the reach of this court." 2022 WL 2052637, at *6; see also Blum v. Defendant 1, 2023 WL 8880351, at *3 ("It is perhaps [plaintiff's] only realistic chance at a future recovery in this case, and Defendants will suffer at

worst a temporary inability to move assets that it appears they have no right to possess."); Fitzgerald v. Defendant 1, 2024 WL 3537916, at *3 ("Maintaining the assets at the Destination Addresses may be Plaintiff's only chance at a future recovery in this case, and Defendants will suffer no more than a temporary inability to move assets that it appears they do not have a right to possess."); Gaponyuk v. Alferov, 2023 WL 4670043, at *3 ("[A] short-term freeze is unlikely to present any great harms. The court can lift this order if the defendants appear and show a continuing injunction would cause them prejudice.") Heissenberg v. Doe, 2021 WL 8154531, at *2 (balance of hardships favors granting TRO); Hikmatullaev v. Villa, 2023 WL 4373225, at *3, report and recommendation adopted, 2023 WL 4363566 (same); Astrove v. Doe, 2022 WL 2805315, at *3 (same); Bullock v. Doe, 2023 WL 9503380, at *6 (same); Chow v. Defendant 1, 2024 WL 1639029, at *2 (same); Yogaratnam v. Dubois, 2024 WL 758387, at *4 (same).

Because the relative harm Plaintiff and putative class members would suffer is so great and because Defendants are engaged in a criminal scheme to steal cryptocurrency, the balancing of equities tilts in favor of Plaintiff and granting a preliminary injunction.

D. A Temporary Restraining Order Without Notice is Necessary to Preserve the Status Quo.

The Court should grant Plaintiff's motion for a TRO without notice because notice to Defendants would almost certainly cause Defendants to move the stolen cryptocurrency out of the wallets identified by Plaintiff, making it extraordinarily unlikely that it would ever be recovered and returned to its rightful owners. (ZA at ¶ 5.) Recognizing that absent a TRO any further relief granted by the court would be meaningless in these circumstances, New York courts considering similar threats of cryptocurrency theft have previously responded immediately to freeze the offending crypto wallets without notice to defendants. See, e.g., Chait v. Lee, Index No. 159881/2024, NYSCEF Doc. No. 16 (N.Y. Sup. Ct. Oct. 25, 2024) (Kingo, J.) (issuing temporary

restraining order freezing stolen crypto assets); Pouyafar v. John Doe Nos. 1-25, Index No. 654820/2023, NYSCEF Doc. No. 8 (N.Y. Sup. Ct. Sept. 29, 2023) (Silvera, J.) (issuing temporary restraining order freezing stolen crypto assets); id. at NYSCEF Doc. No. 47 (N.Y. Sup. Ct. Feb. 15, 2024) (Latin, J.) (issuing preliminary injunction order freezing an additional 24 crypto wallets); LCX AG v. John Doe Nos. 1-25, Index No. 154644/2022, NYSCEF Doc. No 15 (N.Y. Sup. Ct. June 2, 2022) (Masley, J.) (issuing temporary restraining order freezing stolen crypto assets). Courts in other jurisdictions have followed suit. See, e.g., Jacobo v. Doe, 2022 WL 2052637, at *6; Fitzgerald v. Defendant 1, 2024 WL 3537916, at *3; Heissenberg v. Doe, 2021 WL 8154531, at *1; Gaponyuk v. Alferov, 2023 WL 4670043, at *1–2; Hikmatullaev v. Villa, 2023 WL 4373225, at *4–5, report and recommendation adopted, 2023 WL 4363566; Astrove v. Doe, 2022 WL 2805315, at *3; Bullock v. Doe, 2023 WL 9503380, at *4, *7; Chow v. Defendant 1, 2024 WL 1639029, at *3; Yogaratnam v. Dubois, 2024 WL 758387, at *4.

As in those cases, Plaintiff is entitled to a TRO to prevent Defendants from transferring assets in the Deposit Wallets and thereby forever depriving Plaintiff of the stolen assets.

II. THE UNDERTAKING, IF ANY, SHOULD BE MINIMAL

The purpose of an undertaking upon granting a preliminary injunction is to "cover the damages and costs which may be sustained by reason of the injunction" if it is later determined the movant is not entitled to the injunction. CPLR § 6312(b). In this case, the risk of harm to Defendants from a TRO is minimal, as the wallets will be frozen only for a short time before Defendants have an opportunity to be heard. As the risk of harm to Defendants is so low and the equities so clearly favor Plaintiff, the Court should not require an undertaking at this point.

New York courts have granted TROs restraining movement of crypto assets in similar situations without requiring any undertaking. See Chait v. Lee, Index No. 159881/2024, NYSCEF Doc. No. 16 (N.Y. Sup. Ct. Oct. 25, 2024) (Kingo, J.); Pouyafar v. John Doe Nos. 1-25, Index

No.654820/2023, NYSCEF Doc. No. 8 (N.Y. Sup. Ct. Sept. 29, 2023) (Silvera, J.); LCX AG v. John Doe Nos. 1-25, Index No. 154644/2022, NYSCEF Doc. No 15 (N.Y. Sup. Ct. June 2, 2022) (Masley, J.). Courts in other jurisdictions have granted TROs and preliminary injunctions in similar cases involving stolen cryptocurrency with minimal or no undertaking. See Jacobo v. Doe, 2022 WL 2052637, at *6 (E.D. Cal. June 7, 2022) (granting TRO with no bond); Hikmatullaev v. Villa, 2023 WL 4373225, at *4, report and recommendation adopted (same); Gaponyuk v. Alferov, 2023 WL 4670043, at *3 (same); Chow v. Defendant 1, 2024 WL 1639029, at *2 (granting TRO with $100 bond); Yogaratnam v. Dubois, 2024 WL 758387, at *4 (same); Astrove v. Doe, 2022 WL 2805345, at *5 (granting PI with no bond); Bullock v. Doe, 2023 WL 9503377, at *1 (granting PI with $100 bond); Blum v. Defendant 1, No. 3:23-cv-24734-MCR-HTC, 2023 WL 8880351, at *1(N.D. Fla. Dec. 23, 2023) (granting PI with $100 bond).

III. PLAINTIFF SHOULD BE PERMITTED TO SERVE DEFENDANTS USING APPROPRIATE ELECTRONIC MEANS

Plaintiff and investigators have identified the details of Defendants' transactions, and the current location of Plaintiff's and putative class members' property, and traced Plaintiff's stolen funds to the Deposit Wallets. However, Jane Doe 1 and John Doe Nos. 1–10 remain unidentified and therefore cannot be served by traditional means. Therefore, the Proposed Order to Show Cause and Temporary Restraining Order propose providing notice via the Input Data Message process, whereby a message with a link to a website containing documents is sent using the Input Data field on a transaction on the Ethereum blockchain. (ZA ¶ 30). This method, which has been approved by other courts in this jurisdiction, is reasonably calculated to result in actual notice of those documents to the individuals or entities controlling those wallets, and the existence and contents of those service tokens would be readily apparent to the owners. Id.

In similar cases regarding stolen cryptocurrency, New York courts have approved of

service via the crypto wallets holding plaintiffs' stolen cryptocurrency. See e.g., Chait v. Lee, Index No. 159881/2024, NYSCEF Doc. No. 16 (N.Y. Sup. Ct. Oct. 25, 2024) (Kingo, J.) (permitting service by electronic means via Ethereum blockchain); Pouyafar v. John Doe Nos. 1-25, Index No. 654820/2023, NYSCEF Doc. No. 8 (N.Y. Sup. Ct. Sept. 29, 2023) (Silvera, J.) (service of temporary restraining order freezing stolen crypto assets); id. at NYSCEF Doc. No. 17 (N.Y. Sup. Ct. Oct. 19, 2023) (Latin, J.) (service of preliminary injunction order freezing crypto wallet); id. at NYSCEF Doc. No. 47 (N.Y. Sup. Ct. Feb. 15, 2024) (Latin, J.) (service of preliminary injunction order freezing an additional 24 crypto wallets); LCX AG v. John Doe Nos. 1-25, Index No. 154644/2022, NYSCEF Doc. No 15 (N.Y. Sup. Ct. June 2, 2022) (Masley, J.) (service of temporary restraining order freezing stolen crypto assets); id. at NYSCEF Doc. No. 112 (service via special-purpose Ethereum-based token delivered into crypto wallets satisfies CPLR 308(5)).

This form of service has also been approved in cases involving disputes with unknown defendants regarding cryptocurrency in other jurisdictions. E.g., Fitzgerald v. Defendant 1, No. 24-21925-CIV, 2024 WL 3538245, at *3 (S.D. Fla. June 28, 2024); Stil Well v. Defendant "1," No. 23-21920-CIV, 2023 WL 5670722, at *3 (S.D. Fla. Sept. 1, 2023); Bowen v. Li, No. 23-CV-20399, 2023 WL 2346292, at *3 (S.D. Fla. Mar. 3, 2023); Bandyopadhyay v. Defendant 1, No. 22-CV-22907, 2022 WL 17176849, at *3 (S.D. Fla. Nov. 23, 2022); Chow v. Defendant 1, No. 24-CV-480, 2024 WL 3225917, at *1 (E.D. La. Apr. 19, 2024); Blum v. Defendant 1, 2023 WL 8880351, at *2–3 (approving service via non-fungible token).

Plaintiff asks that the Court allow notice by similar electronic means here.

CONCLUSION

For the reasons set forth above, Plaintiff respectfully requests that this Court enter a TRO and freeze the cryptocurrency wallets listed in Appendix A of the Complaint, pending a hearing on

a preliminary injunction.

Plaintiff further respectfully requests that this Court permit Plaintiff to serve Defendants via the Input Data Message process, whereby a message with a link to a website containing documents is sent to a crypto wallet using the Input Data field on a transaction on the Ethereum blockchain, and that such service shall constitute good and sufficient service for purposes of jurisdiction under New York law on the person or persons controlling the Deposit Wallets.

Plaintiff further requests that the Court set no or minimal undertaking pursuant to CPLR § 6312(b).

Plaintiff further requests that the Court grant a preliminary injunction freezing the Deposit Wallets pending final disposition of this matter. Plaintiff further requests the Court grant all other relief that is just and proper.

Dated: New York, New York
January 5, 2025

WALDEN MACHT HARAN & WILLIAMS LLP

By: */s/ John Curran*

John Curran
Deanna M. Paul
Walden Macht Haran & Williams LLP
250 Vesey Street, 27th Floor
New York, New York 10281
(212) 335-2030
jcurran@wmhwlaw.com
dpaul@wmhlaw.com

BISHOP PARTNOY LLP

By: */s/ Frank Partnoy*

Frank Partnoy
Robert Bishop
1717 K Street, NW Suite 900
Washington, DC 20006
(202) 787-5769
frank@bishoppartnoy.com
bobby@bishoppartnoy.com

Attorneys for Plaintiff

CERTIFICATION PURSUANT TO 22 N.Y.C.R.R. 202.8-b

I, John Curran, an attorney duly admitted to practice law before the courts of the State of New York, hereby certify that this Memorandum of Law contains 6,998 words and therefore complies with the word count limit set forth in 22 N.Y.C.R.R. 202.8-b because it contains fewer than 7,000 words, excluding the parts of the memorandum exempted by 202.8-b. In preparing this certification, I have relied on the word count of the word processing system used to prepare this memorandum of law.

Dated: New York, NY
January 5, 2025

/s/ John Curran