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(s),

-against-

TRUSTWAVE.TRADE, AVIV NAFTALI, JANDE DOE 1 and JOHN DOES NOS. 1-10

                                        Defendant(s).

Index No. 150162/2025

Summons

Date Index No. Purchased: January 7, 2025

To the above named Defendant(s)

TRUSTWAVE.TRADE, AVIV NAFTALI, JANE DOE 1 and JOHN DOES NOS. 1-10

You are hereby summoned to answer the complaint in this action and to serve a copy of your answer, or, if the complaint is not served with this summons, to serve a notice of appearance, on the Plaintiff's attorney within 20 days after 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.

The basis of venue is C.P.L.R. § 503(a) which is because a substantial part of the events giving rise to this action occurred in New York County.

Dated: January 7, 2025

                    Walden Macht Haran & Williams

                    by_____
                     John Curran
                    Attorneys for Plaintiff
                     Shameela Karmali-Rawji
                     250 Vesey St,Fl 27
                     New York, NY 10281

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 1and JOHN DOE NOS. 1-10,

Defendants.

Index No.

COMPLAINT

Plaintiff Shameela Karmali-Rawji ("Plaintiff"), by and through her attorneys at Walden Macht Haran & Williams LLP, brings this action against Trustwave.Trade ("Trustwave"), Jane Doe 1, Aviv Naftali ("Naftali"), and John Does 1-10 (collectively, "Defendants"), and alleges as follows:

INTRODUCTION

1.   This case arises from a sophisticated online theft scheme, commonly known as "pig butchering," in which Defendants used a fake cryptocurrency trading platform, Trustwave, as a front to steal over $1.5 million in cryptocurrency from Plaintiff and others similarly situated.

2.   Defendants posed as Trustwave investment advisors and/or representatives and falsely claimed that the Trustwave platform offered advanced Artificial Intelligence ("AI") trading technologies that would provide substantial returns. Defendants fostered trust with victims by following a uniform playbook: constant communication, fabricated reports of profits, and simulated trading activity on the Trustwave platform. Defendants' lies caused Plaintiff and other Class members to reasonably believe their money was secure and earning substantial profits, and to transfer additional cryptocurrency. Defendants then stole the funds.

3.   Between September 2024 and November 2024, Defendants directed Plaintiff to engage in purportedly profitable cryptocurrency trades on the Trustwave platform. These trades were fictitious. Based upon the Defendants' statements and actions, Plaintiff believed her funds

were secure and generating substantial returns and as a result she transferred over $1.5 million worth of cryptocurrency to Trustwave.

4.   Defendants deployed various tactics to conceal their theft. When Plaintiff and other similarly situated victims (the "Class") attempted to withdraw funds, Defendants created and returned counterfeit cryptocurrency assets called "Classic USDC" that were designed to resemble legitimate crypto assets. In reality, Classic USDC was valueless.

5.   Despite Plaintiff's exhaustive efforts to withdraw her investment at Trustwave, Defendants have failed to return her assets.

6.   Defendants' actions deprived Plaintiff and Class members of their assets, violated their ownership rights, and unjustly enriched Defendants at the victims' expense. After securing custody over victims' funds, Defendants stole these assets and routed them through a series of complex online transactions designed to obscure their trail and hinder recovery. Despite these efforts at concealment, Plaintiff and digital tracing experts identified cryptocurrency wallets that currently hold at least some of the stolen funds and are within the jurisdiction of this Court.

7.   This action seeks to recover the stolen cryptocurrency and freeze the cryptocurrency wallets currently holding the stolen assets and obtain damages for the harm caused.

THE PARTIES

8.   Plaintiff Shameela Karmali-Rawji ("Plaintiff") is a resident of Canada who was targeted by Defendants, including while she was present in New York County between October 18, 2024, and October 24, 2024—a critical period of the fraudulent scheme described herein. Plaintiff sustained financial harm in New York County, where she made significant financial transfers that were funneled into cryptocurrency wallets controlled by Defendants.

9.   Defendant Trustwave.trade ("Trustwave"), a fictitious platform designed to mimic the appearance and functionality of a legitimate cryptocurrency trading platform. Trustwave's website states that Trustwave is registered in Switzerland under the name "Trustwave" with the company number CHE-476.213.688 and registered with the Swiss Financial Market Supervisory

2

Authority ("FINMA") under the number F01424921. However, on November 14, 2024, FINMA confirmed that (1) Trustwave.trade does not have a FINMA license; (2) the company number of the Swiss license listed on its website 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.

10. Additionally, Trustwave utilizes fabricated personas and false contact information to mislead victims and steal victims' funds under the guise of profitable cryptocurrency trades. 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 Neopulse, its AI trading product. Trustwave's website also lists "Aviv Naftali" as its chief trade strategist and displays a misappropriated photo of Rabbi Ari Shishler. Notably, Defendant Naftali sent Plaintiff a fake Israeli driver's license, bearing the same photo of Rabbi Ari Shishler with the name Aviv Naftali.

11. Defendant Jane Doe 1 falsely identified herself as a representative of Trustwave, located in Quebec, Canada. Jane Doe 1 provided Plaintiff with the email address catherinedubois@trustwave.trades. Defendant Jane Doe 1 facilitated the fraudulent scheme by connecting Plaintiff with Defendant Aviv Naftali, a purported financial advisor for Trustwave. Upon information and belief, Defendant Jane Doe 1's true identity and residence remain unknown and are subject to ongoing investigation.

12. Defendant Aviv Naftali ("Naftali") is an individual who falsely identified himself as "Aviv Naftali," claimed to be located in Ashdod, Israel and work as a crypto broker who was not directly affiliated with Trustwave. Defendant Naftali called and text messaged Plaintiff and provided her with contact information, including several phone numbers and the email address Avivnaftali@trustwave.trade. Defendant Naftali played a critical role in the fraudulent scheme by directing Plaintiff to transfer funds to wallets at Trustwave under Defendants' control. Defendant Naftali's true identity and residence remain unknown and are subject to ongoing investigation.

3

13.   Defendants John Does 1-10 are individuals or entities of unknown citizenship who perpetrated, aided, or abetted the alleged wrongdoing herein. Plaintiff intends to identify these Defendants through discovery.

JURISDICTION AND VENUE

14.   This Court has jurisdiction over this action pursuant to C.P.L.R. §§ 302(a)(1) and 302(a)(3). Defendants knowingly defrauded Plaintiff and induced her to transfer substantial funds to Trustwave while she was physically located in New York, thereby causing injury to Plaintiff and her property within New York.

15.   Venue is proper pursuant to C.P.L.R. § 503(a) because a substantial part of the events giving rise to this action occurred in New York County. In response to Defendants' misrepresentations and communications, which were knowingly directed at Plaintiff when she was located in New York County, Plaintiff initiated significant cryptocurrency transfers while located in the jurisdiction. Plaintiff also sustained harm while located in New York County. These substantial ties to the jurisdiction establish venue as proper in this Court.

16.   This Court also has the right to hear a class action pursuant to C.P.L.R. § 901 because (1) the class is so numerous that joinder of all members, whether otherwise required or permitted, is impracticable; (2) there are questions of law or fact common to the class which predominate over any questions affecting only individual members; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; (4) the representative parties will fairly and adequately protect the interests of the class; and (5) a class action is superior to other available methods for the fair and efficient adjudication of the controversy.[1]

DEFINITIONS AND BACKGROUND ON CRYPTOCURRENCY AND VIRTUAL CURRENCY EXCHANGES

---

[1] Digital tracing experts have identified Classic USDC sent to numerous wallet addresses in patterns matching the pattern in which Plaintiff received Classic USDC. As such, Plaintiff knows that there are other victims, but does not currently know their identities because there is no central database of names associated with those wallet addresses. Plaintiff seeks class certification. Thereafter, Plaintiff will subpoena the wallet providers for identification of the wallet holders, and then notify those wallet holders that they are a part of the Class.

4

17.   "**Blockchain**" is used by many virtual currencies to publicly record all of their transactions. The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

18.   "**Fiat currency**" is a type of government issued currency that is not backed by a physical commodity, like gold or silver, or other tangible asset or commodity. Its value is derived from the issuing government.

19.   "**Virtual currencies**," also known as cryptocurrency, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin ("BTC") and Ethereum ("ETH") are the most well-known virtual currencies in use.

20.   Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

21.   The identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), but analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

5

22.   "**Virtual currency wallet**" is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

23.   "**Ledger wallet**" is a cryptocurrency wallet designed to securely store cryptocurrency private keys offline to protect them from hackers.

24.   "**Stablecoin**" is a digital asset that is designed to maintain a stable price over time. They are often pegged to a fiat currency, like the U.S. dollar, and maintain a 1:1 ratio with it, and backed by collateral. Stablecoins can be used to hold money within the crypto ecosystem.

25.   **USD Coin ("USDC")** is a type of fiat-backed stablecoin. It is tied to the value of the U.S. dollar; therefore, one unit of USDC is equivalent to approximately one U.S. dollar, making it what is known as a "stablecoin." USDC is issued by Circle Internet Financial Limited ("Circle), a company headquartered in the United States and is supported on over a dozen blockchain networks.

26.   "**Classic USDC**" is a counterfeit cryptocurrency token created by Defendants. Classic USDC is designed to resemble genuine USDC, which is a legitimate stablecoin, but Classic USDC is neither backed by a fiat currency nor had monetary value.

27.   "**Fantom USDC**" is a cryptocurrency token that is designed to resemble genuine USDC, which is a legitimate stablecoin, but is worth a fraction of the value of genuine USDC.

28.   "**Pivot address**" is a platform that allows users to manage a variety of cryptocurrencies and swap cryptocurrencies. Pivot addresses are known for mixing funds and serve as hubs for numerous transport channels.

29.   "**Transport address**" is a platform designed to forward cryptocurrency assets received as far and quickly as possible.

30.   "**Pig butchering**" is a sophisticated and evolving form of online fraud in which perpetrators gain the trust of their victims—sometimes over a period of weeks or months—and eventually introduce the idea of trading in cryptocurrency. Scammers entice their victims to make

6

investments in fraudulent cryptocurrency trading platforms, directing them to cryptocurrency investment platforms or to co-conspirators posing as investment advisors or customer service representatives. Scammers attempt to create the appearance of legitimacy by fabricating websites or mobile apps to display a bogus investment portfolio with large returns. These schemes, which rely on social engineering, fake websites, and promises of high returns, are designed to induce victims to transfer significant funds to wallets controlled by the scammers. Once victims make an initial "investment," the platforms purport to show substantial gains. Sometimes, victims are even allowed to withdraw some of these initial gains to further engender trust in the scheme. It is not until a large investment is made that victims find that they are unable to withdraw their funds. Even when a victim is denied access to their funds, the theft is often not yet over. Scammers request additional investments, taxes or fees, promising that these payments will allow victims access to their accounts. These scam operations often continue to steal from their victims and do not stop until they have deprived victims of any remaining savings. In recent years, these scams have proliferated across the United States, causing billions of dollars in financial losses and prompting numerous state and federal investigations and prosecutions.

<div align="center">**FACTUAL ALLEGATIONS**</div>

A.   Defendants Target the Plaintiff

19.   On September 3, 2024, Plaintiff enrolled in an online cryptocurrency trading course offered by an online education company named "Coursados" for $149 Canadian Dollars ("CAD"). Shortly after signing up, she received a telephone call from an individual falsely identifying herself as Jane Doe 1, who claimed to represent both Coursados and Trustwave. Defendant Dubois described Trustwave as a legitimate cryptocurrency trading platform leveraging advanced AI technology and suggested that Plaintiff apply her course fee toward Trustwave's services. Defendant Dubois then offered to introduce 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.

<div align="center">7</div>

20.   Thereafter, an individual falsely identifying himself as Aviv Naftali ("Defendant Naftali"), contacted Plaintiff via WhatsApp audio on September 4, 2024, and presented himself as a seasoned financial advisor and crypto strategist. Later that day, Plaintiff received an email from "support@trustwave.trade" asking for feedback on her initial conversation with "Aviv Naftali, your broker at Trustwave."

21.   Over the following months, Defendant Naftali cultivated Plaintiff's trust through frequent WhatsApp messages and hours-long phone calls. Defendant Naftali provided Plaintiff with advice on investing, including investing in cryptocurrencies. Defendant Naftali provided Plaintiff with step-by-step instructions 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"). Defendant Naftali also instructed Plaintiff to create and transfer assets into a Ledger wallet, claiming it was critical for securing her investments.

22.   As will be described below, these were necessary steps to the success of Defendants' fraudulent scheme so Plaintiff could transfer fiat currency to these legitimate platforms and convert the fiat currency into various cryptocurrencies, including stablecoins like USDC, and ultimately, at the behest of the Defendants, transfer the cryptocurrencies to the fraudulent exchange they controlled named Trustwave.

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

24.   On October 16, 2024, Defendant Naftali spent over two hours on a call with Plaintiff, guiding her through the purchase of $35,966.98 worth of USDC on the Newton exchange ("Newton Wallet") and then directing her to transfer the full amount to Trustwave. Later that evening, during an additional one-hour call, Defendant Naftali walked Plaintiff through

8

executing trades on Trustwave, reinforcing the appearance of the Trustwave platform's legitimacy.

25.   Between October 17, 2024, and October 23, 2024, Plaintiff traveled from Canada to New York, where she stayed in New York County. During this period, Plaintiff conducted frequent trades on Trustwave under Defendant Naftali's guidance and direction. During this period, Plaintiff was able to withdraw genuine USDC from a Trustwave wallet and transfer it back to her Ledger Wallet ("Ledger Wallet"). This reinforced Plaintiff's confidence in Defendants.

26.   On October 20, 2024, while located in New York, Plaintiff transferred $36,377.1 USDC from Ledger Wallet to a Trustwave wallet, during a two-hour phone call with Defendant Naftali, who assured her of increasing profits.   Later that day, at Defendant Naftali's direction, Plaintiff withdrew $36,914.85 USDC from a Trustwave wallet and sent it to Ledger Wallet; the amount reflected a trading profit of $537.75 USDC.

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

28.   Over the course of two days (October 31, 2024, and November 1, 2024), Defendants directed Plaintiff to transfer a total of $1,500,277 in USDC from Ledger Wallet to Trustwave. Immediately thereafter, during multiple calls spanning four hours, Defendant Naftali directed Plaintiff's trading activity with those funds.

29.   Plaintiff advised Defendant Naftali that she intended to transfer USDC from her Trustwave accounts back to her Ledger Wallet. 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.

9

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

31.   On November 16, 2024, after Plaintiff transferred the withdrawal fee of approximately $10,000 USD in crypto assets to Trustwave, Plaintiff then attempted to withdraw the entire amount of investment held at Trustwave, namely, $1,544,237 USDC.

32.   At the time, Plaintiff believed she had successfully withdrawn $1,544,237 USDC from her Trustwave account and transferred it to Ledger Wallet. 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. 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.

33.   Since November 16, 2024, Plaintiff has made repeated demands of Defendant Naftali and attempts to recover her funds, all to no avail.

34.   Blockchain analysis subsequently confirmed that the counterfeit Classic USDC tokens originated from a single wallet at Trustwave, which also sent Classic USDC to approximately 115 other wallets.

B.   Inca Digital Traces Plaintiff's Funds and Identifies Other Victims

35.   To determine the movement and ultimate location of Plaintiff's stolen cryptocurrency, Plaintiff engaged Inca Digital ("Inca"), a blockchain tracing firm with extensive expertise in tracing stolen digital assets. Inca conducted a detailed analysis of blockchain transactions involving Plaintiff's transfers, revealing that Defendants orchestrated a systematic
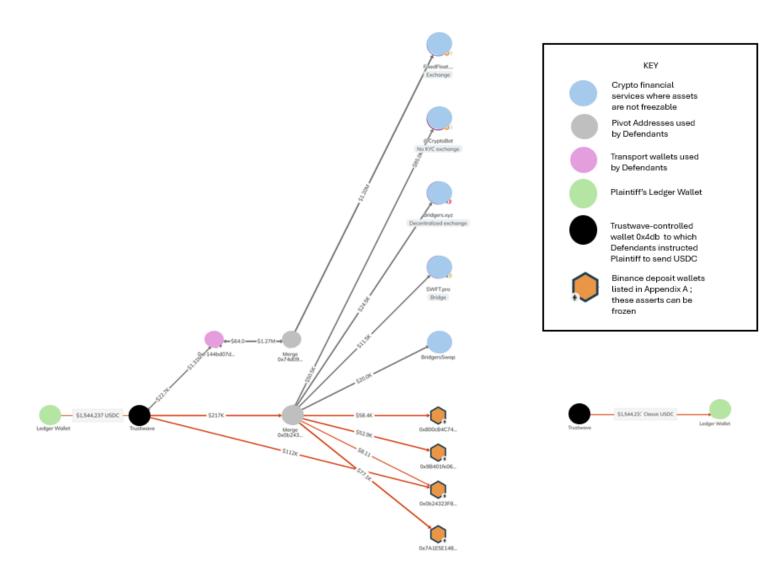
10

scheme to divert Plaintiff's genuine USDC to wallets controlled by the defendants and replace it with counterfeit Classic USDC tokens.

36.   Inca's investigation began with a blockchain analysis by tracing Plaintiff's USDC transfers, tracking the initial destinations and subsequent movement of her funds. Based on the representations made by Aviv Naftali, Plaintiff believed these transfers were directed to Trustwave for legitimate trading and saw them reflected as available in her Trustwave account. However, the analysis revealed that Trustwave was not a legitimate platform—and that Plaintiff's genuine USDC was never traded.

37.   As demonstrated in the below diagram, once Plaintiff's genuine USDC were transferred to Trustwave ("Wallet 0x4db"), the defendants without authorization or disclosure routed Plaintiff's USDC through intermediary addresses controlled by Defendants, including several pivot and transport addresses controlled by Defendants, and deposited into endpoint cryptocurrency wallets controlled by the defendants, including the Binance wallets listed in Appendix A.[2]

38.   Inca also examined the November 16, 2024 transaction in which Trustwave purportedly initiated a transfer of $1,544,237 USDC to Plaintiff. Plaintiff believed she was "withdrawing" her funds from her Trustwave account to the Ledger Wallet. However, blockchain analysis revealed that Wallet 0x4db sent counterfeit Classic USDC mimicking genuine USDC— to the Ledger Wallet, creating the illusion of a legitimate withdrawal while concealing the theft of her genuine USDC.

---

[2] In addition to the Binance wallets denoted in Appendix A, as detailed in the diagram, some of Plaintiff's stolen funds were ultimately deposited into endpoint cryptocurrency wallets through intermediary addresses controlled by Defendants, including several pivot and transport addresses controlled by Defendants, that Plaintiff is unable to freeze. These pivot addresses are identified in the diagram as grey circles labeled as "Merge" and transport addresses are identified in the diagram as pink circles.

11

39.   Inca's blockchain analysis revealed that Defendants utilized a Trustwave wallet, Wallet 0x4db, to transfer counterfeit tokens to Plaintiff's Ledger Wallet. In addition to identifying Wallet 0x4db as sending Plaintiff the counterfeit Classic USDC tokens, the analysis of the transactional activity of this wallet demonstrated that Defendants utilized this same wallet to distribute counterfeit Classic USDC to at least 115 other wallets. Defendants thus used Classic USDC to deceive all Class Members in the same way, replacing their genuine USDC with counterfeit tokens.

40.   Trustwave served as the origin point for these counterfeit tokens, meaning that Plaintiff and Class members uniformly received fake Classic USDC tokens from the same source:

12

Wallet 0x4db. Thus, the use of Trustwave directly ties Defendants' activity to all Class Members.

Every Class member was similarly deceived into believing their assets retained value while their

legitimate cryptocurrency was stolen and replaced with valueless Classic USDC.

41.   Tracing evidence demonstrates that Plaintiff's stolen funds were routed through

intermediary wallets and deposited into the Binance wallets listed as follows and in Appendix A:

42.   Inca identified wallet 0x800cB4C746c3fe494A3Bbd192D0017B094FA9ea2 as a

Binance deposit address and confirmed this address both received Plaintiff's stolen funds and is

a Binance deposit address using open-source forensics tools.

43.   Inca identified wallet 0x9B401fe06EB03B878BDDe2465BcA88118af1fAE5 as a

Binance deposit address and confirmed this address both received Plaintiff's stolen funds and is

a Binance deposit address using open-source forensics tools.

44.   Inca identified wallet 0x0b24323F8424c9DDf445afB835c233d489B1Fc37 as a

Binance deposit address and confirmed this address both received Plaintiff's stolen funds and is

a Binance deposit address using open-source forensics tools.

45.   Inca identified wallet 0x7A1E5E148a47F3875624D72C27B0E35D1745a75F as a

Binance deposit address and confirmed this address both received Plaintiff's stolen funds and is

a Binance deposit address using open-source forensics tools.

46.   As repositories of ill-gotten gains under Defendants' control, these four wallets are

critical targets for freezing to safeguard assets for recovery by Plaintiff and the Class.

<u>**CLASS ALLEGATIONS**</u>

47.   This action may be properly maintained as a class action under Article 9 of the

C.P.L.R.

48.   The proposed Class is initially defined as follows: All individuals whose

cryptocurrency was unlawfully taken and converted by Defendants, and who in return received

Classic USDC from Trustwave, and whose funds ended up in the wallets set forth in Appendix A.

49.   Excluded from the Class are individual Defendants and their families; corporate

Defendants and their officers, directors and affiliates, if any, at all relevant times; Defendants'

13

legal representatives, heirs, successors or assigns; and any entity in which Defendants have or had a controlling interest.

50.   Plaintiff reserves the right to amend or modify the Class in connection with a motion for class certification or as the result of discovery.

51.   Plaintiff does not currently know the precise size of the proposed Class, but Plaintiff is aware that the Class is so numerous that joinder of all members is impracticable, if not impossible, because of the number of Class Members and the fact that Class Members are potentially in geographically disparate locations. Upon information and belief, the Class includes at least one hundred members.

52.   Although the number and identities of Class Members are currently unknown to Plaintiff, it is possible to attempt to ascertain Class Member identities through notice to the original owners of assets contained in the accounts listed in Appendix A of this Complaint, as well as through discovery, including into account records at relevant institutions.

53.   Nearly all factual and legal issues raised in this Complaint are common to each of the members of the Class and will apply uniformly to every member of the Class.

54.   The claims of the representative Plaintiff are typical of the claims of each member of the Class, and by pursuing his own interests Plaintiff will advance the interest of the absent class members.

55.   Plaintiff, like all other members of the Class, sustained damages arising from Defendants' schemes and subsequent digital transactions to convert stolen property and hide the locations of victims' cryptocurrency assets.

56.   The representative Plaintiff and the members of the Class were, and are, similarly or identically harmed by the same unlawful, deceptive, unfair, systematic, and pervasive pattern of misconduct.

57.   Plaintiff, like all other members of the Class, is entitled to the same declaratory, injunctive and other relief as the members of the Class.

58. Plaintiff will fairly and adequately represent and protect the interests of the Class. There are no material conflicts between the claims of the representative Plaintiff and the other members of the Class, including absent members of the Class, that would make class certification inappropriate.

59. Counsel selected to represent the Class will fairly and adequately protect the interest of the Class and have experience in complex and class litigation and are competent counsel for class action litigation.

60. Counsel for the Class will vigorously assert the claims of all members of the Class.

61. This action is properly maintained as a class action in that common questions of law and fact exist as to the members of the Class and predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy, including consideration of: the interests of the members of the Class in individually controlling the prosecution or defense of separate actions and/or proceedings; the impracticability or inefficiency of prosecuting or defending separate actions and/or proceedings; the extent and nature of any litigation concerning the controversy already commenced by members of the Class; the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and the difficulties likely to be encountered in the management of a class action.

62. Among the numerous questions of law and fact common to the Class are: whether Defendants have acted or refused to act on grounds generally applicable to the Plaintiff and the Class; whether Defendants have a pattern, practice and scheme of "pig butchering" and subsequent digital transactions to convert stolen property and hide the locations of victims' cryptocurrency assets; to what extent Plaintiff and members of the Class are entitled to damages; and to what extent Plaintiff and members of the Class are entitled to declaratory and injunctive relief.

15

63.   Defendants have consistently acted and refused to act in ways generally applicable to the Class. Thus, final declaratory and injunctive relief with respect to the entire Class is appropriate.

64.   Plaintiff and the members of the Class have suffered or are at imminent, severe, and unacceptably high risk of suffering irreparable harm because of Defendants' ability to move funds at any time, without notice. If Defendants withdraw funds from the wallets detailed in Appendix A, Plaintiff and the members of the Class will not be able to recover their funds and would lose their property forever.

FIRST CAUSE OF ACTION
DECLARATORY JUDGMENT

65.   Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

66.   Plaintiff and members of the Class seek a declaratory judgment to resolve questions concerning the respective rights, obligations and duties of the parties to the funds being held in the cryptocurrency wallets detailed in Appendix A.

67.   An actual case or judiciable controversy exists between Plaintiff and the Class and Defendants concerning the right to the funds being held in the cryptocurrency wallets detailed in Appendix A.

68.   The issuance of declaratory relief by this Court will terminate some or all of the existing controversy between the parties, and will provide certainty to the parties with respect to their rights and obligations concerning the cryptocurrency wallets detailed in Appendix A.

69.   By reason of the foregoing, Plaintiff and members of the Class are entitled to a declaratory judgment establishing the rights and obligations of the parties and determining the extent of Plaintiff's and the Class's entitlement to the funds in the cryptocurrency wallets detailed in Appendix A.

70.   Plaintiff therefore requests a declaration by this Court that the members of the Class are entitled to the return of the funds in the cryptocurrency wallets detailed in Appendix A.

16

SECOND CAUSE OF ACTION
FRAUD

71.   Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

72.   Defendants fraudulently and falsely represented that Trustwave was a legitimate cryptocurrency trading platform.

73.   Defendants fabricated personas and falsely represented individuals to be legitimate and knowledgeable crypto traders, brokers, and investment advisors on behalf of Trustwave.

74.   Defendants falsely represented that Classic USDC was a legitimate cryptocurrency.

75.   Defendants made these misrepresentations with the intent of inducing reliance by Plaintiff and others similarly situated.

76.   When these representations were made by Defendants, Defendants knew that Trustwave was a fraudulent cryptocurrency trading platform and that Classic USDC was not a legitimate cryptocurrency.

77.   Plaintiff and other Class members reasonably relied on the legitimacy of Trustwave and Classic USDC.

78.   Relying on Defendants' misrepresentations, Plaintiff and other Class members invested in Trustwave, which resulted in actual damages to Plaintiff and Class members.

79.   Accordingly, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
CONVERSION

80.   Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

17

81.   Plaintiff's and members of the Class's stolen funds are identifiable intangible articles of property, traceable using identified techniques and associated with specific virtual asset addresses.

82.   Plaintiff and other Class members had an immediate possessory right to the stolen funds.

83.   Defendants intended to and did exercise absolute dominion over Plaintiff's and members of the Class's stolen funds when Defendants transferred the stolen funds to addresses over which Plaintiff and the Class have no control and moved those assets through multiple digital transactions in an attempt to hide the illicit transactions and current location of the stolen assets.

84.   Defendants' dominion over Plaintiff's and the Class's stolen assets was in derogation of their rights to the assets, completely depriving Plaintiff and the Class of the use of the stolen assets.

85.   Defendants' dominion over Plaintiff's and the Class's stolen assets damaged Plaintiff and the Class.

FOURTH CAUSE OF ACTION
MONEY HAD AND RECEIVED

86.   Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

87.   Defendants received Plaintiff's and the Class's stolen assets from them by way of the "pig butchering" scheme described above.

88.   Defendants benefited from receiving Plaintiff's and the Class's stolen assets by transferring them to digital wallets under Defendants' sole control.

89.   In principles of equity and good conscience, Defendants should not be allowed to retain Plaintiff's and the Class's stolen assets because Defendants had no authority to receive and transact Plaintiff's and the Class's stolen assets.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT

18

90.   Plaintiff repeats and realleges the allegations set forth in the paragraphs above as though fully set forth herein.

91.   Plaintiff and members of the Class each conferred a benefit on the Defendants when, as part of the "pig butchering" scheme described above, they sent assets to Defendants under the false pretense of participating in legitimate investments.

92.   Defendants did not use Plaintiffs' assets for legitimate investments, and instead, after gaining control of these assets under false pretenses, Defendants diverted Plaintiffs' assets into their own possession.

93.   Defendants' retention of Plaintiffs' assets is inequitable.

94.   It is against equity and good conscience to allow Defendants to retain these assets at the expense and detriment of Plaintiff and Class members.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. A declaratory judgment as set forth above;

B. A temporary restraining order and preliminary and permanent injunctive relief prohibiting Defendants from disposing of, processing, routing, facilitating, selling, transferring, encumbering, removing, paying over, conveying or otherwise interfering with debts, accounts, receivables, rights of payment, or tangible or intangible assets of any kind, whether such property is located inside or outside of the United States, including, but not limited to, cryptocurrency or other digital assets held in cryptocurrency wallets detailed in Appendix A, including property of Plaintiff and the Clas

C. Award Plaintiff damages in the amount of at least $ $1,500,000, that being the approximate value of Plaintiff's stolen assets at the time of the theft from Plaintiff;

19

D. Declare this action to be a class action properly maintained pursuant to C.P.L.R. §
    901, appoint Plaintiff as representative of the Class, and designate Plaintiff's
    counsel as Class Counsel;

E. Award compensatory damages, restitution, disgorgement, and any other relief
    permitted by law or equity;

F. Award Plaintiff reasonable attorneys' fees and costs pursuant to C.P.L.R. § 909,
    and any other applicable provision of law; and

G. Award Plaintiff and the Class such other relief as the Court may deem just and
    proper under the circumstances.

Dated: New York, NY
        January 7, 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 Shameela Karmali-
      Rawji on behalf of herself and all others
      similarly situated.

20

APPENDIX A

Binance
0x800cB4C746c3fe494A3Bbd192D0017B094FA9ea2
0x9B401fe06EB03B878BDDe2465BcA88118af1fAE5
0x0b24323F8424c9DDf445afB835c233d489B1Fc37
0x7A1E5E148a47F3875624D72C27B0E35D1745a75F

21