

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

AFFIRMATION OF
ADAM ZARAZINSKI IN SUPPORT OF
PLAINTIFF’S MOTION FOR A
TEMPORARY RESTRAINING ORDER

I, ADAM ZARAZINSKI, affirm the following under penalty of perjury, pursuant to
C.P.L.R. § 2106:

A. Introduction

1. I am employed as the Chief Executive Officer of Inca Digital (“Inca”), a company that specializes in financial risk intelligence and investigating cryptocurrency schemes, including “pig butchering.” As part of my employment at Inca, I have investigated matters related to Shameela Karmali-Rawji’s (“Class Plaintiff”) above-captioned action against Defendants Trustwave.Trade (“Trustwave”), Jane Doe 1, and John Does Nos. 1-10 (collectively “Defendants”). I am over 18 years of age, of sound mind, and am competent to make this Affirmation. The evidence set forth in this Affirmation is based on my personal knowledge unless expressly stated otherwise.

2. Inca is a leading digital asset intelligence firm providing data, analytics, and expertise to cryptocurrency exchanges, financial institutions, regulators, and government agencies. Inca Digital’s services are used to trace illicit financial activity and combat fraud, particularly in cases involving complex cryptocurrency schemes.

3. I hold a J.D. from the University of Michigan Law School, a Master’s Degree in International Relations from the University of Nottingham, and a Bachelor of Arts in Political Science from DePaul University. I have leveraged my specialized knowledge of blockchain technology, digital asset ecosystems, and regulatory frameworks to serve as an expert witness in cryptocurrency-related litigation and testified at the House Financial Services Subcommittee on National Security, Illicit Finance, and International Financial Institutions on terrorist financing. Prior to my work at Inca Digital, I worked as an intelligence analyst at INTERPOL and served in the United States Air Force as a judge advocate. I continue to serve as Major in the USAF JAG Corps Reserve.

4. Inca has been investigating “pig butchering” cases for over four years. “Pig butchering” is a fraudulent scheme in which victims are manipulated into investing in fake cryptocurrency platforms, often through social media or messaging applications. These scams have resulted in billions of dollars in losses and are under investigation by both state and federal authorities.¹ Based on my extensive experience in investigating such schemes, this case clearly involves a coordinated and large-scale “pig butchering” operation.

5. In this case, the fraudulent scheme revolves around a fake cryptocurrency trading and investment platform, Trustwave. Defendants used Trustwave to lure Class Plaintiff and other class members into transferring cryptocurrency to wallets that Defendants controlled. The goal of this class action is to freeze the wallets holding the converted funds and facilitate the return of these stolen assets to the defrauded Class Members.

¹ See FinCEN Alert of Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering,” U.S. Treasury Financial Crimes Enforcement Network Sep. 8, 2023, https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf

6. Based on Inca’s investigation to date, the Defendants’ conversion scheme involved fraudulent transactions from approximately October 14, 2024, to November 14, 2024. The scheme affected, on information and belief, approximately at least 115 wallets.

7. As detailed in Appendix A, Inca identified the specific cryptocurrency wallets in which a portion of the ill-gotten gains of Defendants’ scheme are presently held. These wallets are linked to the common “pig butchering” scheme that centers around the fraudulent platforms mentioned above.

B. Summary of Inca’s Investigation

8. Inca’s investigation was based upon the review of communications between Plaintiff and Defendants, notes of interviews with Plaintiff, records from Plaintiff’s financial institutions, and forensic analysis of transactions publicly available on various cryptocurrency blockchains.

9. Inca’s investigation confirmed that Defendants directed Plaintiff to transfer funds to a trading platform that was completely fictitious: Trustwave. Trustwave is fraudulent and designed to deceive Class Members into believing that their funds were being invested in legitimate cryptocurrency ventures. The purported profits and returns displayed to the victims were falsified to create the illusion of growing investments, while the Defendants had already misappropriated their cryptocurrency.

10. Inca’s investigation further revealed that Defendants utilized Trustwave to move and convert Plaintiff’s Class Members’ assets, transferring the stolen funds through a series of transactions designed to obscure their origins. In connection with Inca’s tracing of Plaintiff’s assets, Plaintiff’s assets were not traded. Rather, as described below, a short time after Plaintiff’s assets were transferred to Trustwave, the Defendants diverted her assets through a series of transfers involving Pivot addresses and Transport addresses (commonly used in pig butchering

scams). Inca's tracing analysis ultimately traced Plaintiff's assets to 9 crypto wallets, including 4 cryptocurrency wallets held on the Binance cryptocurrency exchange, among others. Those wallets are listed in Appendix A.

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

12. Through this analysis, Inca uncovered further wallet addresses involved in the diversion of Class Plaintiff's funds, thus revealing a broader network of wallets involved in the scam.

13. Further, based upon Inca and my expertise, the interactions between the wallets in the identified network are highly indicative of fraudulent activity. Specifically, the network contains wallets engaging in two types of behavior that is associated with cryptocurrency fraud schemes and is rarely, if ever, associated with legitimate cryptocurrency transactions. First, the network contains "Pivot Addresses," which are known for mixing funds and serve as hubs for numerous transport channels. They accumulate funds from a large number of transport nodes and forward larger amounts to 3-4 other transport nodes. 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. Additionally, sources of funds for these addresses often include wallets already flagged for scam activity, gambling, darknet

involvement, or inclusion in sanction lists. Overall, these interactions between the different wallets in the network gives me a high degree of confidence that the entire network exists as part of the scam and is controlled by Defendants.

14. Second, Inca analysis confirmed that “Transport Addresses” are present in the scam. “Transport Addresses” are designed to simply forward everything they receive, moving funds as far and as quickly as possible from the victim to frustrate tracing. Funds are rarely held in these wallets for more than a few days, with the sum of inputs equaling the sum of outputs. Additionally, the splitting of Plaintiff’s funds into nine separate deposit accounts is similarly indicative of fraudulent activity.

15. Inca uses a common tool called Etherscan to track transactions on the Ethereum blockchain.² Genuine USDC and its counterfeit version “Classic USDC” are transmitted on the Ethereum blockchain.

C. Inca’s Tracing Analysis

16. To determine the movement and ultimate location of Plaintiff’s stolen cryptocurrency, Plaintiff engaged Inca. Inca conducted a detailed analysis of blockchain transactions involving Plaintiff’s transfers, revealing that Defendants orchestrated a systematic scheme to divert Class Plaintiff’s genuine USDC and replace it with counterfeit Classic USDC tokens.

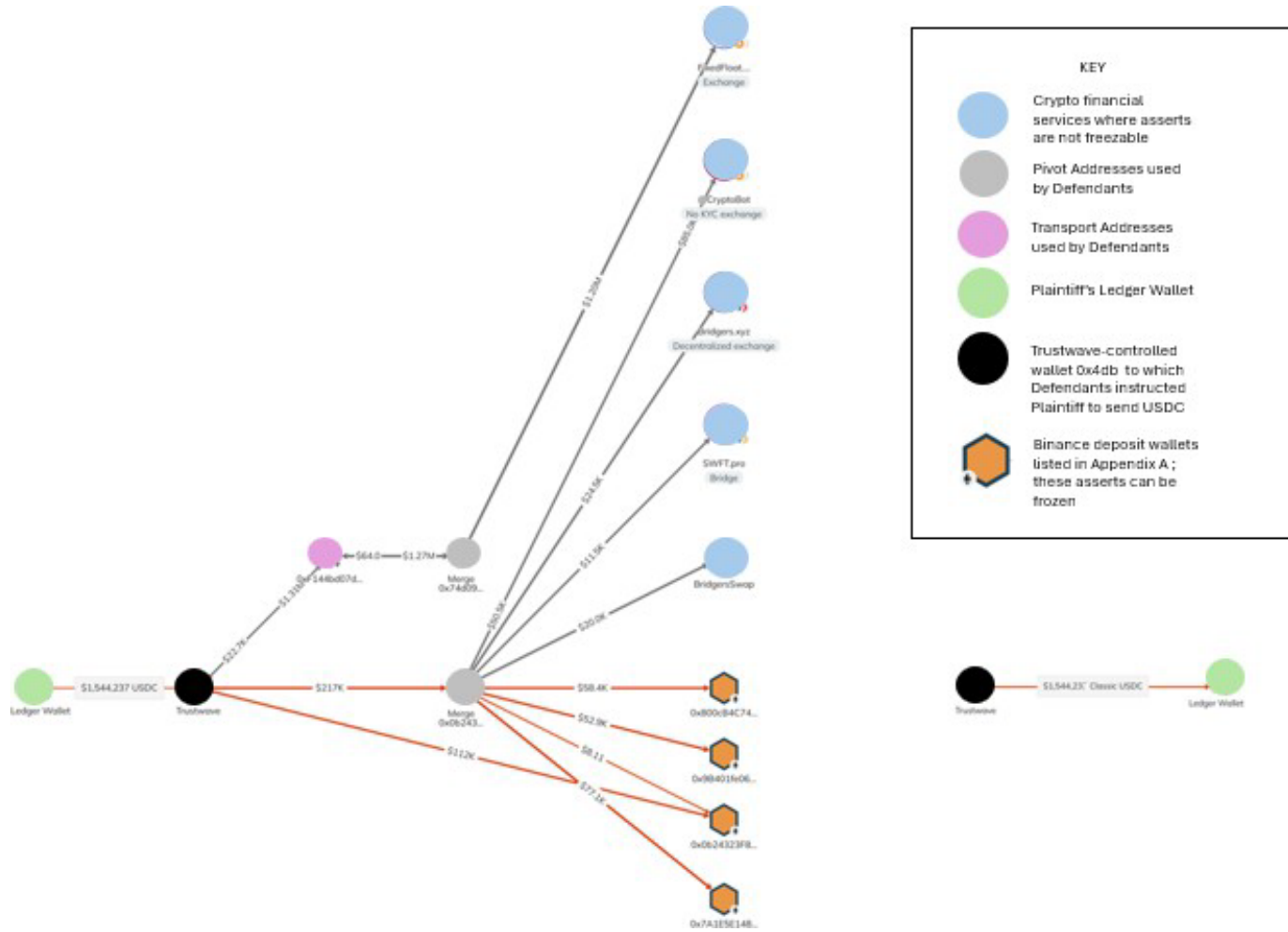
17. Inca’s investigation employed a forward-tracing analysis of Plaintiff’s USDC transfers, tracking the initial destinations and subsequent movement of her funds. Class Plaintiff

² When tracing a cryptocurrency transaction, it is common to see slight discrepancies between the total value of funds sent and received. These discrepancies are caused by volatility of a cryptocurrency asset and the transaction fee (commonly known as “gas”), which is deducted from the amount received by the recipient. We do not believe such a discrepancy affects our analysis in this case.

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. Among other things, there is no evidence that Plaintiff’s genuine USDC was traded but instead diverted through a series of intermediary wallets before being deposited into endpoint cryptocurrency wallets at the cryptocurrency exchange Binance, as detailed in Appendix A. These findings align with the discovery by Plaintiff that Trustwave lacked proper registration or authority to conduct cryptocurrency transactions.

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

19. The following diagram depicts the sophisticated movement of victim funds described above.



20. Further analysis revealed that Wallet 0x4db not only sent counterfeit tokens to Class Plaintiff's Ledger wallet but also distributed counterfeit Classic USDC to at least 115 other wallets. Wallet 0x4db served as the origin point for these counterfeit tokens, establishing a direct link between Class Plaintiff's experience and Defendants' broader class-wide scheme. By issuing Classic USDC to multiple victims, including Class Plaintiff, Defendants created a unified pattern of deception designed to replace genuine USDC with counterfeit tokens.

21. Wallet 0x4db directly ties Class Plaintiff's experience to that of a broader class of victims, who were deceived into believing their assets retained value while their legitimate cryptocurrency was stolen and replaced with valueless Classic USDC.

22. Inca estimates that Defendants' scheme targeted at least 115 wallets. Tracing evidence demonstrates that Plaintiff's stolen funds were routed through intermediary wallets and deposited into the Binance wallets listed in Appendix A. Inca's analysis suggests that these wallets are likely to hold additional proceeds from Defendants' coordinated operation against the Class Members, all of whom traded on Trustwave and relied on the legitimacy of Classic USDC.

23. Inca identified wallet 0x800cB4C746c3fe494A3Bbd192D0017B094FA9ea2 as a Binance deposit address and confirmed this address both received Class Plaintiff's stolen funds and is a Binance deposit address using open-source forensics tools.

24. Inca identified wallet 0x9B401fe06EB03B878BDDe2465BcA88118af1fAE5 as a Binance deposit address and confirmed this address both received Class Plaintiff's stolen funds and is a Binance deposit address using open-source forensics tools.

25. Inca identified wallet 0x0b24323F8424c9DDf445afB835c233d489B1Fc37 as a Binance deposit address and confirmed this address both received Class Plaintiff's stolen funds and is a Binance deposit address using open-source forensics tools.

26. Inca identified wallet 0x7A1E5E148a47F3875624D72C27B0E35D1745a75F as a Binance deposit address and confirmed this address both received Class Plaintiff's stolen funds and is a Binance deposit address using open-source forensics tools.

27. As repositories of ill-gotten gains under Defendants' control, these four wallets are critical targets for freezing to safeguard assets for recovery by Class Plaintiff and the Class.

D. Conclusion


28. In summary, Inca's analysis demonstrates that the cryptocurrency assets belonging to Class Members, including Plaintiff Shameela Karmali-Rawji, were systematically misappropriated by the Defendants through the use of fraudulent platforms. The wallets that now hold the stolen funds are identified in Appendix A.

29. Based upon my expertise in blockchain forensics and my substantial experience investigating “pig butchering” schemes similar to this one, if Class Plaintiff is required to wait until after the Defendants receive notice of this action, it is highly likely that Defendants will transfer cryptocurrency at issue beyond the reach of discovery or recovery.

30. I am familiar with the process of 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. In my experience, the method of notice proposed in the Proposed Order to Show Cause and Temporary Restraining Order is reasonably calculated to and would likely result in actual notice of those documents to the individuals or entities that control those wallets, and the existence and contents of those service tokens would be readily apparent to the owners.

31. I affirm this 5th day of January, 2025, under the penalties of perjury under the laws of New York, which may include a fine or imprisonment, that the foregoing is true, and I understand that this document may be filed in an action or proceeding in a court of law.

Dated: New York, NY
January 5, 2025

DocuSigned by:

CAC32ADB9CDD4CE...

By: _____
Adam Zarazinski

Inca Digital
1100 15th St. NW
Washington, D.C. 20005
Phone: (908) 219-7750
Email: adam@inca.digital

Certification Pursuant to 22 NYCRR § 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 Affirmation contains 2,023 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, NY
January 6, 2025

By: */s/ John Curran*
John Curran, Esq.