

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

RACHEL POUYAFAR,)	
)	Index No. 654820/2023
Plaintiff,)	
)	
-against-)	AFFIRMATION
)	<u>OF CHARLES ZACH</u>
JOHN DOE NOS. 1-25,)	
)	
Defendants.)	
)	

I, Charles Zach, affirm under penalty of perjury as follows:

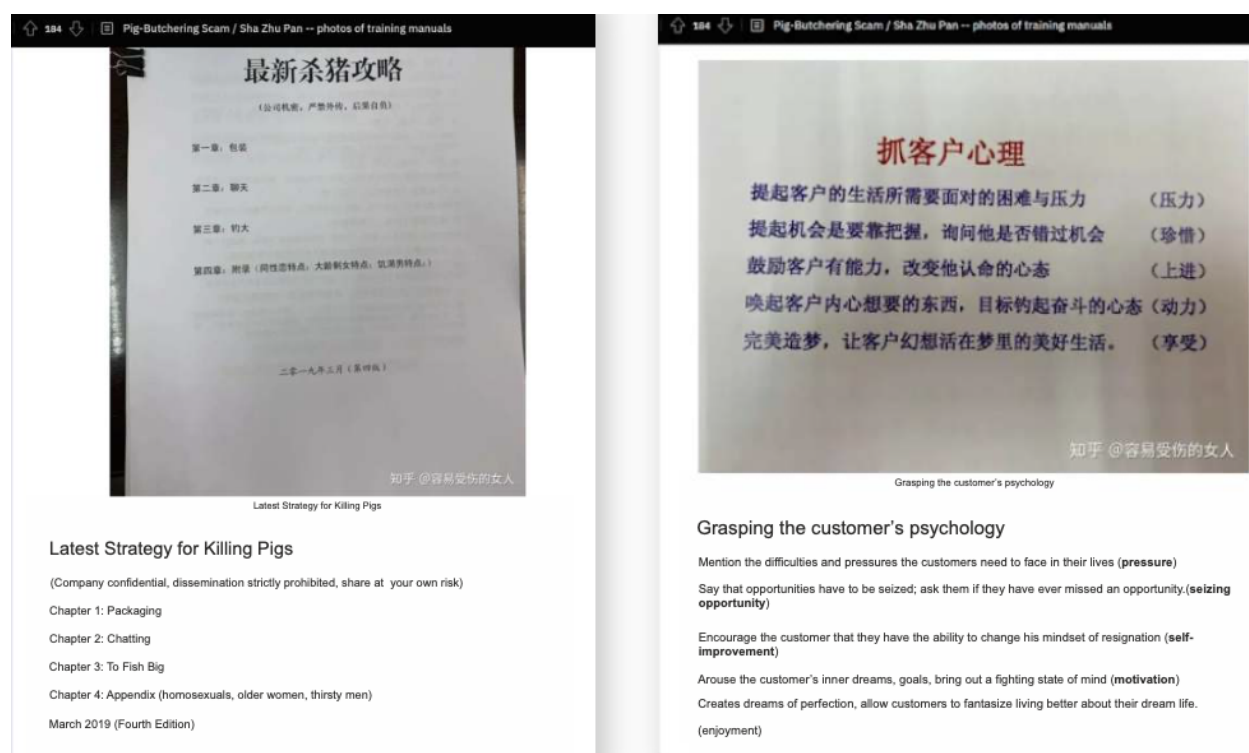
INTRODUCTION

1. I am an employee at Inca Digital, a company that investigates cryptocurrency schemes, including “pig butchering.” As part of my employment at Inca Digital, I have investigated matters related to Rachel Pouyafar’s (“Plaintiff”) above-captioned action against Defendant John Does Nos. 1-25 (collectively “Defendants”). I am over 18 years of age, of sound mind, and am competent to make this Affirmation. The evidence set forth in the foregoing Affirmation is based on my personal knowledge unless expressly stated otherwise.

2. Inca Digital is a digital asset intelligence company that provides data, analytics, and expertise to many of the world’s leading exchanges, financial institutions, regulators, and government agencies. Inca Digital’s clients use its unique and comprehensive intelligence to surveil digital asset markets, fight crime, generate alpha, and more. For more information about Inca Digital and our work, please visit: <https://inca.digital/>

3. Inca Digital has been investigating ‘pig butchering’ cases for over two years. Based on my expertise and experience, this is a clear case of “pig butchering.” This unfortunate name is the one given by the scammers themselves: “Sha Zhu Pan” (殺豬

盤) or “Pig Butchering.” This name is unfortunately accurate: it describes the practice of using fake cryptocurrency accounts to “fatten” victims before slaughter. The perpetrators target people, frequently in New York, by promising—and then pretending to deliver—large, but fake, returns. These fake returns lure victims to deposit substantial amounts of their savings. Once victims have been “fattened” enough with reports of false profits, and have transferred large amounts of money, the perpetrators steal their property, and disappear. The perpetrators are a transnational criminal group operating out of China and its border countries. Among other evidence, Inca Digital has obtained their operations manual.



Screenshots from Pig Butchering Operations Manual

4. Defendants' actions here followed the "pig butchering" roadmap.¹ First, they created a fake identity, a person representing himself as "Yunhai Quan" ("Quan"). Quan posed as a former investment banker living a lavish lifestyle in California while running an investment firm. Quan initiated contact with Plaintiff via WhatsApp and won her trust by convincing her that he wanted to buy real estate through her, and was willing to help her invest in return for her help finding a New York residence. Then Quan persuaded Plaintiff to "invest" using a fake investment account she believed was associated with the QuedEx exchange. Quan convinced her to deposit a small amount of funds, sent her false evidence of investment "profits," and manipulated her to deposit increasing amounts.

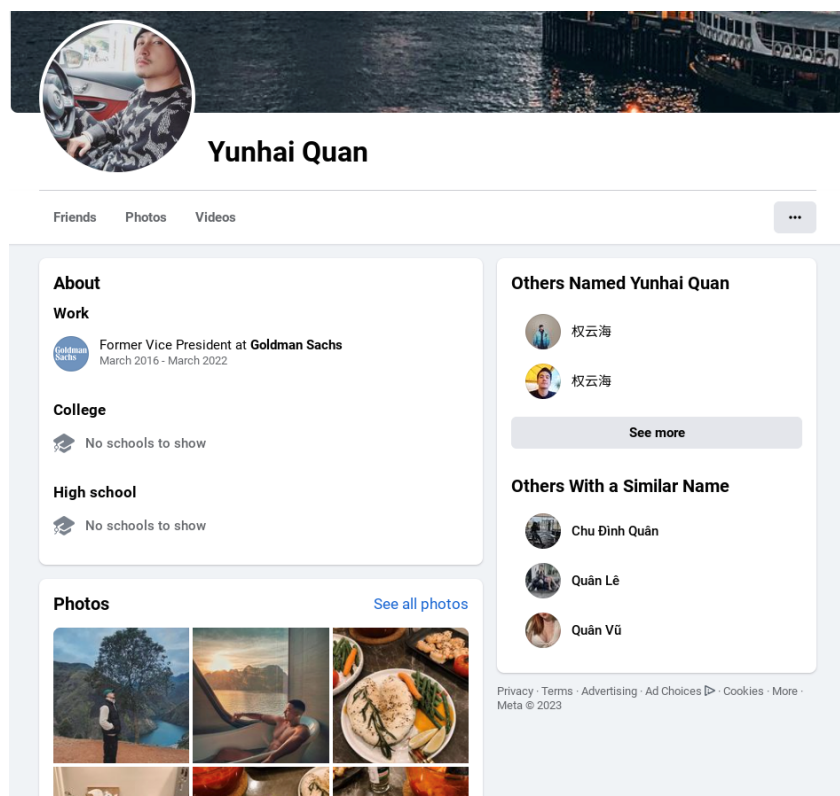
5. Defendants utilized a fake persona, Quan, to interact with Plaintiff. This fake persona was the combination of two individuals' stolen online information. The first individual's information used to create the Quan persona was Zhe Quan, a Vice President at Goldman Sachs living in Brooklyn, New York. The second individual's information used to create the Quan persona was Zind Lee, a Vietnamese Instagram model.

6. Defendants based the work history of the fake persona Quan on the individual Zhe Quan, a real life employee of Goldman Sachs based in Brooklyn, New York. Quan represented himself to Plaintiff as a "former Senior Associate of Goldman Sachs". On a facebook profile page²

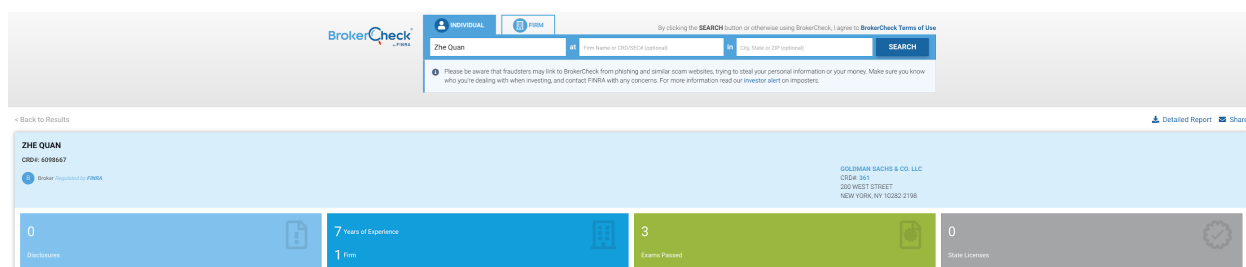
¹ ProPublica recently published an in-depth investigation of pig butchering, describing how criminal syndicates operate, often by forcing human trafficking victims to perpetrate the schemes against their will, including the following process: "1) Create a fake identity. 2) Initiate contact. 3) Win the trust of the target. 4) Sign them up. 5) Get them to put real money into the fake account. 6) "Prove" that it's legitimate. 7) Manipulate them into investing more. 8) Cut them off. 9) Use their desperation to your advantage. 10) Taunt and depart." See Cezary Podkul, *What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One*, PROPUBLICA, Sept. 19, 2022, <https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one>. As described below, Defendants likewise followed these steps.

² <http://facebook.com/amy.hampton.716195>

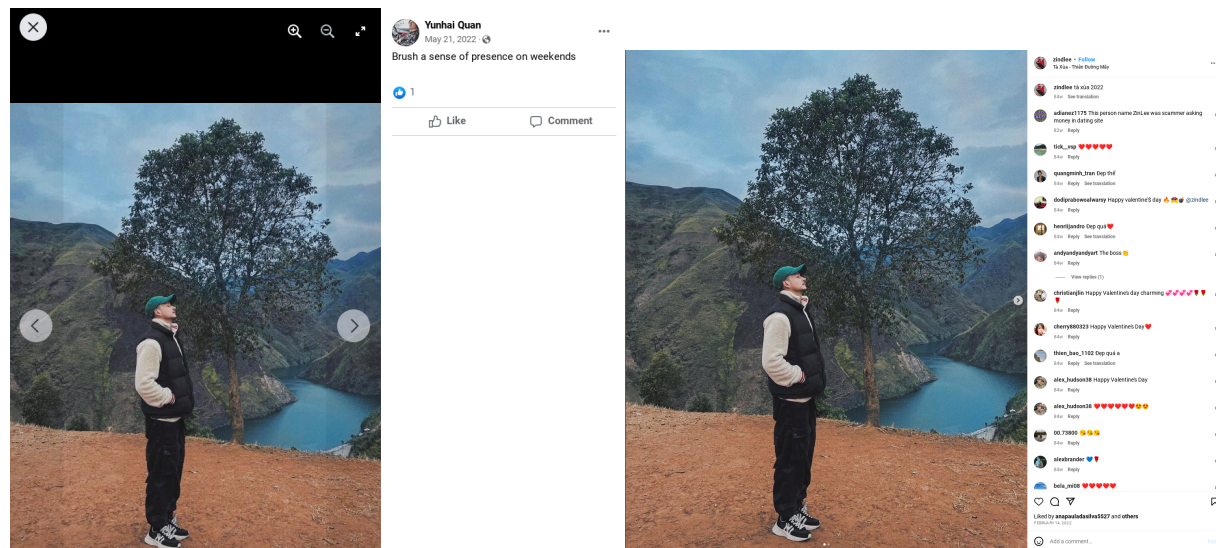
associated with the fake persona Quan, “Former Vice President at Goldman Sachs” is listed under work experience.



7. Based on an investigation by Plaintiff’s counsel, the persona “Yunhai Quan” has never been registered as a financial broker with the Financial Industry Regulatory Authority (“FINRA”). There is an active FINRA broker registration for the individual Zhe Quan as a current employee of Goldman Sachs.



8. Defendants based the affluent lifestyle and photos of the fake persona Quan on the individual Zind Lee, a model from Vietnam. There is a known history³ of scammers using photos of Zind Lee to portray a lavish lifestyle. Reverse image searches for the photos posted to the Yunhai Quan Facebook page reveal the photos were taken directly from Zind Lee's Instagram account⁴.



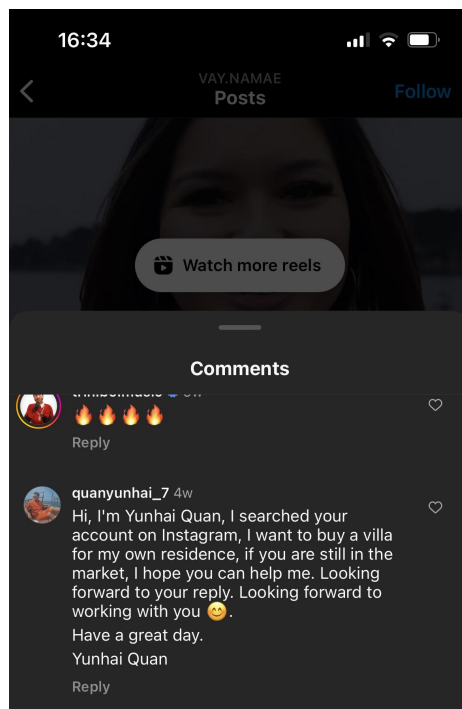
9. Defendants likely repurposed a stolen Facebook account to fit the persona of Quan. The URL link of the account is associated with an “Amy Hampton” facebook.com/amy.hampton.716195.

10. Defendants have used an Instagram account⁵ associated with Quan to spam template messages to real estate agents from across the United States since at least October of 2022. This activity is similar to the tactic used to initiate contact with Plaintiff.

³<https://www.scamsurvivors.com/forum/viewtopic.php?f=11&t=73904&sid=e2ff7f1e32c63bb645aa160b13711ba1>

⁴<https://www.instagram.com/zindlee/>

⁵https://www.instagram.com/quanyunhai_7/



11. Defendants enticed Plaintiff to invest through a fake website. Plaintiff was provided a link to her supposed investment account at QuedEx.⁶ Defendants manipulated the false link to show Plaintiff fake “returns” on her investment. In actuality, the funds Plaintiff sent to wallet address 0xf611bd67bb3ac6fc501a8fc990a950eea36bf903 were never associated with an investment account. Instead, Defendants presented Plaintiff with fraudulent data she believed to be her trading activity.

12. Based on an investigation by Plaintiff’s counsel, the transactions and transfers associated with the scheme involved the following cryptocurrencies: “USDC” refers to a cryptocurrency known as “USD Coin,” “ETH” refers to a cryptocurrency known as “Ethereum,” “USDT” refers to a cryptocurrency known as “Tether,” and “DAI” refers to a cryptocurrency maintained by a “decentralized autonomous organization” (“DAO”) on the Ethereum blockchain.

⁶ quedextrac.com/h5#/home.

13. Between August 1, 2023 and August 21, 2023, Plaintiff sent five transactions totaling 50,468.519489 USDC and 82.0994033 ETH from her Coinbase account to Ethereum address 0xf611bd67bb3ac6fc501a8fc990a950eea36bf903, which she believed was associated with QuedEx. In total, Plaintiff deposited a total of approximately \$240,500 in the above wallet address as follows:

July 31, 2023: \$500.00
 August 2, 2023: \$50,000
 August 7, 2023: \$50,000
 August 11, 2023: \$50,000
 August 21, 2023: \$50,000
 August 22, 2023: \$40,000

14. The conversions of these U.S. dollar deposits into cryptocurrencies (in these instances, USDC and ETH) are set forth in the chart below.

AUG 21, 2023 09:58:23 PM	ETH	29.37759565	0x2d8329deef12175f1696ef970028e9af25ca2c45aff1c1ad562a79dd009c1ab	0xe8044fa8f33cd2b12e52d6746f489a58fb4afcd0	
AUG 21, 2023 09:42:11 PM	ETH	29.37803080	0x585cd25e92e40fc8837f15342d4083fcd09d04d517d48a7b31bb00b6270c2c	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	Coinbase EXCHANGE
AUG 12, 2023 01:17:23 AM	USDC	49,988.51948900	0x925dfdd735b9d76b9a4fafeef794f37207f59aff667fec6769f9cb6d8ad86302	0xe8044fa8f33cd2b12e52d6746f489a58fb4afcd0	
AUG 12, 2023 01:17:23 AM	ETH	0.00000000	0x925dfdd735b9d76b9a4fafeef794f37207f59aff667fec6769f9cb6d8ad86302	0xa0b66991c6218b36c1d19d4a2e9eb0cc3606eb48	USD Coin SERVICES
AUG 12, 2023 01:06:47 AM	ETH	0.00160830	0x2b4f3255148fd76bb299e960521021ad49465887b44aa4cb678555d1d119901	0x9d8dd477b15fda345bda8111896b28136b5401bc	
AUG 12, 2023 12:55:11 AM	USDC	49,988.51948900	0xaf4e1eacd7d3ddf919ae14e185be7eb4fb5da8362ae920139d290e519c0cb9bc	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	Coinbase EXCHANGE
AUG 9, 2023 03:31:23 AM	ETH	26.24529619	0x2541b7eefa7692b2eb9ec9c7d538bcacd964efc76ceb2867d0b6151dd4d5c4	0xe8044fa8f33cd2b12e52d6746f489a58fb4afcd0	
AUG 9, 2023 03:16:11 AM	ETH	26.24552684	0x67214939b97bbf0bd9585e5a3f975a911e69207c35e4bd70c4f372f119e6b1b5	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	Coinbase EXCHANGE
AUG 2, 2023 09:52:23 PM	ETH	26.47719610	0x78ca936613c19e1dac17d8706c2a0874d8f048093f53698ae9b92699823cb4	0xe8044fa8f33cd2b12e52d6746f489a58fb4afcd0	
AUG 2, 2023 09:42:11 PM	ETH	26.47584575	0xe4576fd0e693aa95a103cd7bd712518653e83ee11a61e4cacc48d74183d76319	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	Coinbase EXCHANGE
AUG 1, 2023 04:53:59 AM	USDC	480.00000000	0x9a273ae51b6782c71af109978e96a883f2c5bf428c262a6d401d799046dbe518	0xe8044fa8f33cd2b12e52d6746f489a58fb4afcd0	
AUG 1, 2023 04:53:59 AM	ETH	0.00000000	0x9a273ae51b6782c71af109978e96a883f2c5bf428c262a6d401d799046dbe518	0xa0b66991c6218b36c1d19d4a2e9eb0cc3606eb48	USD Coin SERVICES
AUG 1, 2023 04:43:23 AM	ETH	0.00368063	0xdb5889fedbac76470ab96be7d30326ed92a882c3f11490bc719e8a9c72f3771	0x524e094d03a56bfcccf6581bc5c51338b875e344f	
AUG 1, 2023 04:09:11 AM	USDC	480.00000000	0x74c4fd0aac6d5db35ff0b3b42a6feae5ab196fb6d756b9231f1e5d9ab539c2ef	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	Coinbase EXCHANGE

15. We are aware of the following transactions as part of the scheme based on our investigation. On August 11, 2023, Defendants sent 49,988.519489 USDC from the initial wallet address 0xf611bd67bb3ac6fc501a8fc990a950eea36bf903, to wallet address 0xe8044fa8f33cd2b12e52d6746f489a58fb4afcd0 in transaction 0x925dfdd735b9d76b9a4fafeef794f37207f59aff667fec6769f9cb6d8ad86302.

16. Defendants then utilized decentralized exchange Tokenlon smart contract 0x4a14347083b80e5216ca31350a2d21702ac3650d to swap the victim's 49,988.519489 USDC to

49,960.43400276 DAI in transaction 0x2e94ce936779cb6fb8fd8ba50e579465006edff5c46340b1438dd24851c53a71. This amount of DAI was then combined with other amounts of DAI already held in wallet 0xe8044fa8f33cd2b12e52d6746f489a58fb4afcd0 to total 76,974.0281 DAI which was then sent to wallet address 0xd1070a15381de901d90a8034f88fc30346dcda0e in transaction 0xc468cca6307631e888cd34d5467b85fd8a0b4151b381e6d977a27144be4662e0 on August 11, 2023.

17. Once in wallet address 0xd1070a15381de901d90a8034f88fc30346dcda0e, the DAI was then further combined with other funds to make an amount totaling 500,000.00 DAI which was then sent to wallet address 0x2829ada0f48dddc7352c12e2d686e172819b2dba in transaction 0xec028684ec560066060edcea8089948e10b5e4fa3fbf44034d0a108128feca52 on August 12, 2023.

18. On August 13, 2023, that 500,000 DAI was sent to wallet address 0x4c7822051e2395fafb9a2862863e3acbdb96171 in transaction 0x3b93621b78db98cd6c111ad59cb5c42681de15c6af05a6a97583721d24d941d7.

19. That 500,000 DAI was then combined with other amounts of DAI already held in wallet 0x4c7822051e2395fafb9a2862863e3acbdb96171 to total 1,000,000 DAI, which was then sent to wallet address 0x7f3c82e892616d4d5a325fa13e4f4d04a8d312ce in transaction 0x802292f8753af9b9aa44b7c682d29a98bdfa075f989bbdb1c49f7177083e1cc8 on August 21, 2023.

20. Once in wallet address 0x7f3c82e892616d4d5a325fa13e4f4d04a8d312ce, the 1,000,000 DAI was divided into three pieces of 500,000 DAI, 325,000 DAI, and 175,000 DAI. The 500,000 DAI was then swapped for 500,066.661335 USDT using Uniswap smart contract

0x48da0965ab2d2cbf1c17c09cfb5cbe67ad5b1406 in transaction 0xdf46c3ae75f128651bf294f595f622afd3ad8ccfc5ef744351787264d36a3945. This 500,000 USDT was then sent to wallet address 0xe85a08a79fc70e8d1aaa84a54404a22665aaac22 in transaction 0x73ba3fb0327efd367c217ed9a68fae711165cc005ccd41c2d23d344245e308a1 on August 21, 2023.

21. Once in wallet address 0xe85a08a79fc70e8d1aaa84a54404a22665aaac22, the 500,000 USDT was combined with other amounts of USDT already held in the wallet to total 989,017.00 USDT. On August 21, 2023, this 989,017.00 USDT was then swapped to 589.49992143 ETH utilizing Tokenlon smart contract 0x4a14347083b80e5216ca31350a2d21702ac3650d in transaction 0x5cfdce27f6236b6f772cb1b9f14d457dbd70e27c31cb2474fdd76af4027cd31. 588 of that ETH was then sent to wallet address 0x81aa37777aa5a00c02792bc08a5f1507e85ef8ad in transaction 0xdc20fd9db7ec45dfd0aaa7ba42bdcb972675d8f87e0b21b3fe1114966458bb1b.

22. On August 21, 2023, 480 of the 588 ETH was then swapped to 799,490.013651 USDT utilizing Tokenlon smart contract 0x4a14347083b80e5216ca31350a2d21702ac3650d in transaction 0xb022e8eff0d6264863d3c83afc02c89804957d850b8ec3d8a60233e2418c9d00. 620,600.00 USDT of that amount was then sent to wallet address 0x45d0093e066f8e942b78224554feb2ded73717a8 in transaction 0x6b2b037b5ab50571a976abee7e9ba39105bfd0e2efa18c96fe82361c5e1a7987. Those funds currently remain in wallet address 0x45d0093e066f8e942b78224554feb2ded73717a8.

23. On August 21, 2023, 150,000 USDT of the remaining amount in wallet address 0x81aa37777aa5a00c02792bc08a5f1507e85ef8ad was sent to wallet address 0xff1338533489d20ddcb191563ff0a102a03adb92 in transaction

0x2ad8780f71db4444896f70de8dbd844c3adb0c014985cdcfadd6009520725d63. The 150,000 USDT in wallet address 0xff1338533489d20ddcb191563ff0a102a03adb92 was then combined with an existed 350,000 USDT already in the wallet to total 500,000 USDT, which was then sent back to wallet address 0x81aa37777aa5a00c02792bc08a5f1507e85ef8ad in transaction 0xaa6644413492daf8bafcc91dc5cebbfa60b5cf804bd3de53a40e6209f7c2d87f on September 20, 2023.

24. Once back in wallet address 0x81aa37777aa5a00c02792bc08a5f1507e85ef8ad, the 500,000 USDT was split into two amounts of 150,000 USDT and 400,000 USDT, and sent to Binance hot wallet address 0x01d19c7dab1da4d2c9a7a8c54a9c1e9b7b5a7b9a on September 20, 2023, in transactions 0x092186f0dc5274bad9a55f031b735407d7dd74ba27d7ec44dac4980d138a48cd and 0x37d1272b48f24e43a02fccbbc047bf52691ec2d5b9631bf7b2c5b987188d853f, respectively.

25. The remaining 108 ETH of the 588 ETH which entered wallet address 0x81aa37777aa5a00c02792bc08a5f1507e85ef8ad was then part of transaction 0xeb8de862018d268965814a99418ecb34e271a7554c8fb8682b9b76a95f431bed, in which 198 ETH was swapped for 314,733.517521 USDT utilizing Tokenlon smart contract 0x8d90113a1e286a5ab3e496fbd1853f265e5913c6. This USDT was then combined with other USDT in the wallet to total 323,506.00 USDT, which was sent to Binance hot wallet address 0x01d19c7dab1da4d2c9a7a8c54a9c1e9b7b5a7b9a on September 21, 2023, in transaction 0x329bcb15b8604be3ff17f67b3199c6e34e74c1c4fd674c56611d000193cf26c3.

26. In total, three transactions worth 873,506 USDT connected to the cryptocurrency/tokens scammed from Plaintiff were deposited to Binance hot wallet

0x01d19c7dab1da4d2c9a7a8c54a9c1e9b7b5a7b9a between September 20, 2023 and September 22, 2023.

27. Plaintiff's counsel has access to proprietary technology that has allowed it to locate \$202,650 of Plaintiff's funds in the Binance Hot Wallet: 0x01d19c7dab1da4d2c9a7a8c54a9c1e9b7b5a7b9a. Defendants could move Plaintiff's funds from this account anytime, without notice. If this wallet is frozen before Defendants withdraw Plaintiff's funds, Plaintiff might be able to recover some or all of these funds. If not, she likely will lose her property forever.

28. Plaintiff's assets are commingled in this account with other funds that likely represent property that Defendants similarly have stolen and converted from other "pig butchering" victims. In all, the above commingled Binance Hot Wallet account has approximately \$2.1 million of assets, including funds deposited during September 18-24, 2023.

29. Plaintiff's counsel continues to track Defendants' actions in real time. Plaintiff seeks an immediate temporary restraining order, before Defendants transfer her assets elsewhere. Time is of the essence, given that Defendants could transfer funds from the Binance Hot Wallet at any time, without notice.

30. I affirm this 29th day of September, 2023, under the penalties of perjury under the laws of New York, which may include a fine or imprisonment, that I am physically located outside the geographic boundaries of the United States, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States, 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: Sinj, Croatia
September 29, 2023




By: _____
Charles Bo Zach

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

Certification Pursuant to 22 NYCRR § 202.8-b

I, Rishi Bhandari, at attorney duly admitted to practice law before the courts of the State of New York, hereby certifies that this Affirmation contains 1,992 words, excluding the parts exempted by § 202.8-b(b), and therefore complies with the word count limit set forth in 22 NYCRR § 202.8-b(a).

Dated: New York, New York
September 29, 2023

By: 
Rishi Bhandari, Esq.