**IN THE CIRCUIT COURT OF THE THIRTEENTH JUDICIAL CIRCUIT IN AND FOR HILLSBOROUGH COUNTY, FLORIDA**

**NAVIN PASEM,**

**Plaintiff,** **Case No.: 25-CA-002901**

**v.**

**JOHN DOE 1, JOHN DOE 2, JOHN DOE 3, and DOES 4 through 200**

**Defendants.**

---

## SECOND AMENDED VERIFIED COMPLAINT

Navin Pasem, an individual ("Plaintiff"), sues Defendant John Doe 1, Defendant John Doe 2, Defendant John Doe 3, and Does 4 through 200 (collectively, "Defendants") and alleges as follows:

## GENERAL ALLEGATIONS

### Parties, Jurisdiction and Venue

1. Plaintiff is an individual residing in Hillsborough County, Florida.

2. Defendant John Doe 1 is an individual of unknown residence who, acting in concert with other Defendants, induced Plaintiff to transfer cryptocurrency assets into wallets controlled by Defendants and misappropriated those assets. The identity of Defendant John Doe 1 is unknown to Plaintiff at this time and is subject to ongoing investigation.

3. Defendant John Doe 2 is an individual of unknown residence who, acting in concert with other Defendants, induced Plaintiff to transfer cryptocurrency assets into wallets controlled by Defendants and misappropriated those assets. The identity of Defendant John Doe 2 is unknown to Plaintiff at this time and is subject to ongoing investigation.

4. Defendant John Doe 3 is an individual of unknown residence who, acting in concert with other Defendants, induced Plaintiff to transfer cryptocurrency assets into wallets controlled by Defendants and misappropriated those assets. The identity of Defendant John Doe 3 is unknown to Plaintiff at this time and is subject to ongoing investigation.

5. Defendants, Does 4 through 200, inclusive, are the individuals and/or entities who orchestrated and perpetrated the activities complained of herein. The true names and capacities of Defendants Does 4 through 200, inclusive, are unknown to Plaintiff at this time and are subject to ongoing investigation.

6. Jurisdiction is proper under Section 26.012(2)(a), Florida Statutes, because this Court has original jurisdiction over civil actions in which the matter in controversy exceeds $50,000.00.

7. Venue is proper in Hillsborough County, Florida, because Plaintiff resides in Hillsborough County and Plaintiff was the primary target of Defendants' scheme.

## INTRODUCTION

8. This case arises from a deliberate, calculated, and coordinated scheme in which Defendants fraudulently impersonated Coinbase personnel, fabricated a purported security breach, and manipulated Plaintiff into transferring digital assets to cryptocurrency wallet addresses under their control. Acting under the false and deceptive belief that he was protecting his Coinbase Exchange account from unauthorized access, Plaintiff followed Defendants' instructions to transfer his cryptocurrency to what he was told were secure wallet addresses linked to his account. In reality, these wallet addresses were controlled by Defendants for the sole purpose of misappropriating Plaintiff's cryptocurrency.

9. Plaintiff retained Applied Technology Solutions ("ATS"), a firm that specializes in financial intelligence, sanctions investigations, and blockchain-based asset tracing. ATS conducted a detailed investigation using forensic blockchain analysis and determined that after

Defendants received Plaintiff's cryptocurrency, they employed a range of tactics to obscure both the origins and ultimate destinations of these funds. Defendants dispersed Plaintiff's cryptocurrency across multiple networks and platforms, using fragmentation, asset swaps, blockchain bridges, and mixing — techniques specifically designed to hinder forensic tracing efforts. Despite these obfuscation strategies, ATS traced the movement of Plaintiff's stolen cryptocurrency to a series of deposit wallets at centralized exchanges. The identified wallet addresses, which continue to hold traceable proceeds of the theft, are listed in the attached Appendix A.

10. Plaintiff brings this action to recover the cryptocurrency stolen by Defendants and seeks full restitution of the misappropriated assets, along with damages resulting from Defendants' fraudulent conduct. Plaintiff also seeks emergency injunctive relief to immediately freeze the identified deposit wallets at centralized exchanges, as listed in Appendix A, to prevent further dissipation, transfer, or concealment of the stolen cryptocurrency.

## FACTUAL ALLEGATIONS

11. On or about February 25, 2025, Plaintiff received a text message from the phone number (351) 215-1378, Defendant John Doe 1. The message claimed to be from Coinbase Support and warned that someone had requested a "withdrawal code" to authorize a transaction from Plaintiff's Coinbase Exchange account. The message stated that if Plaintiff had not initiated the request, urgent action was required, and he should immediately call (770) 258-6200 to prevent unauthorized access.

12. Believing this was a legitimate security alert, Plaintiff called the phone number Defendant John Doe 1 provided, (770) 258-6200 — belonging to Defendant John Doe 2. On that phone call, Defendant John Doe 2 claimed to be a Coinbase support agent. He warned that overseas hackers were actively attempting to access Plaintiff's Coinbase Exchange account and

that immediate action was necessary to secure his assets. Defendant John Doe 2 claimed the matter would be escalated to Coinbase's fraud prevention department.

13. Shortly thereafter, Defendant John Doe 2 escalated the call to Defendant John Doe 3, who claimed to be part of Coinbase's fraud prevention team. Defendant John Doe 3 called back Plaintiff using the number (202) 750-1446 and directed Plaintiff to download the "Coinbase Wallet" mobile app, falsely claiming that downloading the app was a necessary security measure to protect his funds. Defendant John Doe 3 stated that the Coinbase Wallet app was a secure extension of Plaintiff's existing Coinbase account and that transferring funds to wallet addresses within the app would safeguard them from unauthorized access.

14. Coinbase Wallet is a legitimate mobile application offered by Coinbase. Defendant John Doe 3 misrepresented it as a security tool linked to Plaintiff's existing account, leading Plaintiff to reasonably believe that using the app was necessary to protect his assets.

15. Relying on repeated false assurances, Plaintiff transferred his cryptocurrency holdings — including 76.099 Ethereum (ETH) and 4.909 Bitcoin (BTC), valued at $607,492.38 at the time of the theft — to the wallet addresses provided by Defendant John Doe 3. After completing the transfers, Plaintiff was unable to reestablish contact with any of the individuals who had contacted him, and the assets were immediately moved out of reach.

16. Following the theft, Plaintiff retained Applied Technology Solutions ("ATS"), a blockchain forensic tracing firm, to conduct a detailed analysis of Plaintiff's stolen cryptocurrency assets. Using blockchain analytics tools and open-source intelligence, ATS traced the movement of Plaintiff's assets and identified the wallets used to receive, consolidate, and disperse the misappropriated funds. Multiple subsequent transactions by Defendants were structured to frustrate attribution, hinder tracing, and make recovery more difficult.

17. ATS's investigation revealed that Defendants first directed Plaintiff's Ethereum ("ETH") to wallet address 0xaC500C1B6f8b197afd48fbc8576712D80c088ab0 (the "0xaC500

wallet"), which is controlled by Defendants. From that address, Defendants then routed the ETH through two separate paths to obscure its origin.

18. Approximately $80,000 in ETH was transferred from the 0xaC500 wallet to an intermediary wallet and then deposited into a cryptocurrency wallet hosted at TradeOgre, a centralized cryptocurrency exchange.

19. The other approximately $75,000 in ETH was transferred to a wallet under Defendant's control with the address 0x5aF944437b46A68194D5d0Ad1D48Bcd603a51eFA (the "0x5aF944 wallet"), fragmented into smaller transactions, and partially bridged using Across.to. During that bridge transaction, Wrapped Ether (WETH) was swapped for ETH before the assets continued on the Ethereum blockchain. The fragmented ETH was ultimately deposited into more than twenty deposit addresses of wallets hosted by various exchanges—all under Defendants' control.

20. ATS's investigation further confirmed that Defendants instructed Plaintiff to transfer 4.909 Bitcoin ("BTC") initially to the below two Defendant-controlled wallet addresses: bc1qr5d2cycuze9x78axjl0v2989g9nn7xmsups23q

bc1qwp7hhd7pc5qr40ymzh2400lgfegy9tr5pnv4xw (the "bc1qwp wallet").

21. All BTC sent to the first address was quickly consolidated into the bc1qwp wallet, which served as the central hub for laundering the stolen Bitcoin. The ATS tracing analysis also confirmed that the bc1qwp wallet also received cryptocurrency linked to unrelated fraudulent schemes, indicating intentional commingling designed to obscure the source of misappropriated assets.

22. From the bc1qwp wallet, approximately 2.809 BTC (valued at $243,276) was deposited into a TradeOgre wallet. An additional 1.975 BTC (valued at approximately $171,000) was transferred to another intermediary wallet, fragmented into smaller amounts, and ultimately

routed into deposit addresses hosted by both identified exchanges and other custodial platforms whose hosting entities have not yet been determined through blockchain attribution.

23. The overall laundering process used by Defendants reflects deliberate obfuscation techniques. Defendants deployed asset fragmentation, swap protocols, cross-chain transfers, and commingling across multiple schemes to conceal the origin and movement of Plaintiff's cryptocurrency. Despite these efforts, Plaintiff's stolen assets were successfully traced to deposit addresses that are hosted by known centralized exchanges. These deposit addresses represent the final known locations of the stolen cryptocurrency and are listed in Appendix A.

**FIRST CAUSE OF ACTION**

**(For Conversion)**

24. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

25. Defendants wrongfully withheld and converted to themselves the assets and property of Plaintiff in a manner inconsistent with their property rights in those assets.

26. As a result of the foregoing, Plaintiff has been deprived of the use of his assets and damaged in an amount to be established at trial.

27. The above-described conduct of Defendants was made with oppression, fraud, and malice, and with actual and constructive knowledge that the assets were wrongfully converted by Defendants for their own personal use and without the knowledge of or approval by Plaintiff.

**SECOND CAUSE OF ACTION**

**(For Fraudulent Inducement)**

28. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

29. Defendants made a misrepresentation concerning a material fact, namely that they were representatives of Coinbase tech support.

30. Defendants knew such misrepresentation was a false statement.

31. Defendants intended for such false statement to induce Plaintiff to act on it, namely that Plaintiff would transfer funds to cryptocurrency wallets controlled by Defendants.

32. Pursuant to Plaintiff's reliance on Defendants' material misrepresentation, Plaintiff has been materially damaged.

**THIRD CAUSE OF ACTION**

**(Request for Injunctive Relief & Imposition of a Constructive Trust)**

33. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

34. Plaintiff believed there was a relationship of trust and confidence between the parties and Defendants were in a position to influence or advise Plaintiff.

35. Defendants promised Plaintiff his assets would be safe in transferring the same and Plaintiff transferred the assets in reliance on Defendants' promises.

36. Defendants would be unjustly enriched by Plaintiff's reliance on Defendants' promise.

37. Plaintiff requests an injunction to freeze of all accounts listed in Appendix A.

38. Such a freeze is necessary to preserve the possibility of restitution for the Plaintiff.

39. There is no adequate remedy at law.

40. Plaintiff will suffer irreparable harm if an injunction is not issued by this Court.

41. Plaintiff has a clear legal right to the property contained in the wallets he seeks to enjoin.

42. It is in the public interest for the Plaintiff's property to be preserved through injunctive relief.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff respectfully requests that this Court:

1. Enter a preliminary injunction to freeze the cryptocurrency addresses set forth in Appendix A;

2. Award a judgement against Defendants for compensatory damages of $607,492;
3. Award a judgement against Defendants for punitive damages of $250,000 to punish Defendants for their malicious conduct and to deter similar conduct in the future;
4. Award a judgement against Defendants for attorney's fees and costs of suit;
5. Award a judgement against Defendants for pre- and post-judgment interest; and
6. Grant any other equitable relief this Court deems just and proper, including the imposition of a constructive trust over any assets traceable to the theft.
7. Award a judgement against Defendants for such other and further relief as this Court deems just and proper.

Dated: April 3, 2025

/s/ Navin R. Pasem
Law Office of Navin R. Pasem, P.L.
Navin R. Pasem, Esq.
Florida Bar No. 18863
5401 W. Kennedy Blvd, Ste 100
Tampa, Florida 33609
Phone: (813) 444.3017
Fax: (813) 925.4317
navin@pasemlaw.com
*Plaintiff, appearing pro se*

**VERIFICATION OF NAVIN PASEM**

Pursuant to Section 92.525, Florida Statutes, and under penalty of perjury, I declare that I have read the foregoing Verified Complaint and that the facts stated therein are true and correct.

/s/ Navin R. Pasem

Navin R. Pasem

Dated: April 3, 2025

## Appendix A

Coinbase (3)
0x8495D0D64835bBbcA933501488483f83184AEE04
0x829f8Dc756f7bfe0fa93c4A4A349A248Abf3FBf9
0xD141b2a341B66Ba3FC98a83204bB3c13FA3979D0

OKX (2)
0x946A6903512eD5C758Ff29674CE2D80Ab3acf8D1
0xb96029D98301ebda17189dF57666A06019FC0f42

TradeOgre (4)
0x4648451b5F87FF8F0F7D622bD40574bb97E25980
bc1qnru0urp778ju4v3datvrhhwh7v772shpkajk89
bc1qmp6kgcmtzl944slcyp5dprx3vjggk20nuk2j43
bc1qhxmay86etyg9nzykgcsm2wjt7ccul4wmnhsyg8

Binance (5)
0x56957739BAe1b7C0725f4e517309eFC8EF6EB73e
0x615790F841d626688Bbc7C397a1dC15785487996
0x08E163449a1951c560c4c93E6638c346633aA56D
0x2c6E2140Fa5FD157fabc66263f241DdDb3b92946
15fJm7DahbW5vF71ns8UXdx74ZPCGPXv4N

KuCoin (1)
0x5021aF4f24c5Bd4Cb7c1CCF8eCc198664414A326

HTX (1)
1JaUhzMuXo3Xuvn5p67LNzmLhXnPu32FZn

WirexApp (1)
0x8b4A8493fDcD038e04E5fd6AE6A93b3a53c8967a

HitBTC (3)
0x52103366eB89a5f8c833c34B77892Ef90521C167
0x187fE1a8B76c60b85c00A2819152ff00Ff642386
0x32E2EeF43D74601a0eB52eA71c142A6f432F1924

ChangeNow (3)
0xfAaEf33462e2256cfeF3F96C7347Dd7e3C175F09
0xc9148Db23F4217fb320113724946D97bD373eCba
0xdA01f89Bce7E66BCe7a523E0F11A3a9a21Aa68f0

CoinEx (2)

0x7086ac523208cc53619Dc63dC7F47E8fb316D057
0x4C6324ebB5B438cfEcf0f878c776574FEeDE4F36

OxaPay (1)
0xC842355888f47C9E4F0eBEF7627A66724Be01295

Stake.com (1)
0x993Cd9D9eb1647eAD826C7F7bC8277E5227c2218

CoinPal (3)
0xAe2b3879ede4732FfD6942be25Ff796B31d67749
0x1472924b0325a37A71E71519ffaF765dc9D27cea
0x429d947cFDD87e4cb1ca3eBDa9075C6B4E801B9a

Uphold (1)
0x06a909c7ED913a8c3b613A4B2a5168Ca579b515c