UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA

JOHN J. BLUM, **Plaintiff,** **v.** **DEFENDANT "1" a/k/a "MIA TARA" and JOHN DOES 1-20, as yet unidentified Individuals, Business Entities and/or Unincorporated Associates,** **Defendants.**	**Case No.** 3:23-cv-24734

COMPLAINT FOR
CONVERSION OF STOLEN CRYPTOCURRENCIES

Plaintiff, JOHN J. BLUM, by and through undersigned counsel, sues DEFENDANT "1" a/k/a "MIA TARA" and JOHN DOES 1-20, as follows:

PRELIMINARY STATEMENT

1. Defendants stole 30.8298 Bitcoin (BTC) from Plaintiff pursuant to a sophisticated global internet cryptocurrency fraud and conversion scheme, the current market value of which is one-million one-hundred sixty thousand six hundred fifteen and fifty-eight cents ($1,160,615.58).

2. Defendant "1" played a material role in the theft of Plaintiff's assets,

and upon information and belief, she and her cohorts currently possess all or a significant portion of Plaintiff's stolen property.

3. Plaintiff brings this lawsuit to recover his stolen assets.

SUBJECT MATTER JURISDICTION AND VENUE

4. This is an action for damages related to the theft of Plaintiff's cryptocurrency assets as detailed below. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 (diversity jurisdiction).

5. Venue is proper in this District pursuant to 18 U.S.C. § 1965(a) and (b), and 28 U.S.C. § 1391(b) and (c).

6. Defendants are subject to personal jurisdiction in this district, because they direct business activities toward and conduct business with consumers throughout the United States, including within the State of Florida and this district through at least a fraudulent website and mobile application (Bitnukes) which can be accessed on the internet and on smartphones and are accessible from Florida.

7. Moreover, every website has at least one associated IP address that it uses to communicate with devices on a network. The IP address for Bitnukes is 108.156.83.15. Plaintiff has tracked the Bitnukes IP address to Miami, Florida.

8. Moreover, upon information and belief, Defendants are foreign nationals and are subject to personal jurisdiction in this district pursuant to Federal

Rule of Civil Procedure 4(k)(2) because (i) Defendants are not subject to jurisdiction in any state's court of general jurisdiction; and (ii) exercising jurisdiction is consistent with the United States Constitution and laws.

THE PARTIES AND PERSONAL JURISDICTION

9. Plaintiff, JOHN J. BLUM, an individual, is *sui juris*, and is a resident and citizen of Oregon.

10. Defendant "1" is an individual, is sui juris, and is subject to the personal jurisdiction of this Court. Defendant "1" represented to Plaintiff JOHN J. BLUM that her name was "Mia Tara." Defendant represented to Plaintiff that she was Ukrainian, and the parties' communications consistently demonstrated Defendant "1" was of Ukrainian descent who claimed that she was in Miami, Florida, as further evidence by the location of the IP address.

11. Defendants JOHN DOES 1-20 are as of yet unidentified Individuals, Business Entities, And/or Unincorporated Associations, cohorts of Defendant "1," are *sui juris*, and are subject to the personal jurisdiction of this Court.

12. At all times material hereto, Defendants have maintained and continue to maintain private cryptocurrency wallets and cryptocurrency exchange accounts in which all of or a portion of Plaintiff's stolen cryptocurrency currently sits.

ALLEGATIONS COMMON TO ALL COUNTS

A. Defendants Execute an International Cryptocurrency Theft Scheme

13. Plaintiff desired to invest money in cryptocurrency.

14. Plaintiff began searching online and on social media to learn how he could invest in cryptocurrency.

15. On or about March 9th, 2023, Plaintiff met Defendant "1" a/k/a "Mia Tara" who communicated with Plaintiff via WhatsApp, with a WhatsApp phone number of 845-999-7210 (VOIP), phone number 402-804-8336 (VOIP) and email address eloym6566@gmail.com.

16. Defendant "1" a/k/a "Mia Tara" used multiple fake identities on social media platforms.

17. Defendant "1" misrepresented that she would teach Plaintiff how to become a successful cryptocurrency trader.

18. Defendant "1" lured Plaintiff by showing him examples over WhatsApp of how she was successfully earning high returns on her cryptocurrency trading methods.

19. Defendant "1" represented to Plaintiff that she was using a trusted mobile application called Bitnukes that, according to Defendant "1", was owned and operated by her aunt, a cryptocurrency data analyst.

20. According to the Bitnukes website, Bitnuke is a Swiss Bitcoin

exchange and wallet, founded in April 2018. Bitnuke claims their goal is to "create an alternative to other crypto exchanges which are often untrustworthy and too complex to use, so we decided to make ours better - more intuitive, safer and completely transparent. We built Bitnuk as a convenient platform for those who want to buy Bitcoin for the first time and long-term investors. This is why we skipped overly-technical trading tools, went for user-friendly interface and created a system which does all the heavy-lifting in the background. We understand that the cryptocurrency world is still new and unfamiliar to most people so we made sure that our Bitnuke customer support is easy to reach, flexible and ready to help you with anything Bitnuke-related."

21. Defendant "1" assisted Plaintiff in downloading Bitnukes which she claimed was the trading mobile application. She stated that "Bitnukes" would be used as a trading platform with the purpose of making transactions; and when done, the assets would be transferred to Crypto.com for withdrawal.

22. However, the application Defendant "1" provided to Plaintiff was not a legitimate exchange application owned and operated by any exchange but was instead a fraudulent copycat mobile application created to deceive individuals, including Plaintiff, into believing they were investing on a legitimate cryptocurrency exchange owned and operated by Bitnukes.

23. To further entice Plaintiff into believing she was a legitimate investor

who only wanted to assist Plaintiff in becoming a successful cryptocurrency trader like her, on or about March 17th, 2023 Defendant "1" had Plaintiff run a test where he transferred approximately $919.79 worth of cryptocurrency from his Crypto.com account into the fraudulent Bitnukes mobile application. When Plaintiff was able to transfer this amount back to his digital wallet, he believed that Defendant "1" was a legitimate investor who wanted to help him learn how to invest cryptocurrency and, further, that the fraudulent mobile application he had downloaded was also legitimate.

24. After familiarizing himself with the process of trading on the fraudulent mobile application recommended by Defendant "1," and in reliance on the foregoing false and fraudulent misrepresentations, Plaintiff started to transfer cryptocurrency from his Crypto.com and Kraken accounts, legitimate third-party online platforms for buying, selling, transferring, and storing cryptocurrency, to the fraudulent platform (Bitnukes).

25. Defendants posted fraudulent returns on their fake mobile application which made it appear that Plaintiff was making money on his trades.

26. As a result, he continued to transfer cryptocurrency from his Crypto.com and Kraken accounts to the fraudulent exchange. Because of the fraudulent representations contained on the fake Bitnukes account, and misrepresentations made by Defendant "1", and additional individuals who claimed to be Bitnuke account

managers and/or customer service representatives, Plaintiff believed that he had made significant money from the investment.

27. Plaintiff was told by Defendant "1" that the value of his cryptocurrency had grown from approximately eight hundred eighty-one thousand and five dollars and eleven cents ($881,005.11) to approximately two million nine hundred thirty-two thousand one hundred fifty-one and seventy-three cents ($2,932,151.73), which was also reflected on the fraudulent Bitnukes statements.

28. On April 21st, 2023, Defendants advised Plaintiff to withdrawal his account balance from Bitnukes to his personal bank account. When Plaintiff attempted to withdrawal his cryptocurrency from the fraudulent application, Plaintiff experienced issues and was unable to make transfers.

29. However, Plaintiff was told by individuals claiming to be Bitnuke customer representatives that before he could withdrawal his cryptocurrency, he was required to transfer additional cryptocurrency to the fraudulent Bitnukes exchange to pay taxes on his earnings.

30. When Plaintiff questioned Defendant "1" about the transfer issues he was experiencing, Defendant "1" provided excuses and made additional false representations.

31. Plaintiff communicated with additional individuals who claimed to be Bitnukes customer service representatives and account managers and assured

Plaintiff that everything would be resolved once he deposited additional cryptocurrency to pay taxes on his earnings.

32. This is when Plaintiff realized he had been scammed. Plaintiff made numerous unsuccessful attempts to transfer the cryptocurrency from the fake copycat exchange back to his Crypto.com wallet.

B. Plaintiff's Forensic Tracing of Their Stolen Cryptocurrency

33. When a transaction is made on the blockchain it is assigned a "transaction hash" ("TXID"). A transaction hash is a unique string of characters that is given to every transaction that is verified and added to the blockchain. A TXID is used to uniquely identify a particular transaction. All on-chain transactions (the transactions from or to external addresses) have a unique TXID that can be seen in transaction details. All on-chain transactions (depositing and withdrawing of funds) have a unique TXID that can be found in transaction details.

34. Within the time frame of March 17th, 2023, and April 21st, 2023, Plaintiff JOHN J. BLUM transferred made 8 transactions from his Crypto.com and Kraken accounts to the fraudulent exchange. In total, Plaintiff transferred approximately 30.8298 (BTC) to the fraudulent exchange, which had a market value at the time of approximately $881,005.11 (USD).

35. Plaintiff has retained forensic cryptocurrency tracing experts who have traced Plaintiffs stolen assets on the blockchain. Attached hereto as Exhibit A is the

tracing report completed by experts at CipherBlade. Plaintiff incorporates Exhibit A into his verified complaint.

COUNT 1
CONVERSION

36. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 39 above, as if fully and expressly set forth herein, and further alleges as follows.

37. As more fully alleged above, Defendants misappropriated Plaintiff's funds.

38. Defendants have converted Plaintiff's funds to their own use or to the use of others not entitled thereto and have exercised dominion and control over the funds to Plaintiff's exclusion and detriment.

39. Plaintiff has suffered damages as a direct and proximate result of Defendants' conversion.

WHEREFORE, Plaintiff JOHN J. BLUM demands that judgment be entered against Defendant "1" and JOHN DOES 1-20, jointly and severally, for damages, interest, costs, and such other and further relief as this Court deems just and proper.

COUNT II
UNJUST ENRICHMENT

40. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 42 above, as if fully and expressly set forth herein, and further alleges as

follows.

41. Plaintiff conferred a direct benefit upon Defendants by transferring the valuable cryptocurrency that Defendants converted from Plaintiff.

42. Defendants have knowledge of the benefit Plaintiff conferred upon them and have retained such benefit.

43. The circumstances under which Plaintiff conferred, and Defendants accepted, such benefit render Defendants' retention of the benefits inequitable.

44. Equity required that Defendants return to Plaintiff the benefits he conferred upon Defendants.

WHEREFORE, Plaintiff JOHN J. BLUM demands that judgment be entered against Defendant "1" and JOHN DOES 1-20, jointly and severally, for damages, interest, costs, and such other further relief as this Court deems just and proper.

COUNT III
IMPOSITION OF CONSTRUCTIVE TRUST AND DISGORGEMENT OF FUNDS

45. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 47 above, as if fully and expressly set forth herein, and further alleges as follows.

46. This is an action to impose a constructive trust upon the property taken from Plaintiff that is currently held by Defendants.

47. This action further calls for the restoration to Plaintiff of that

wrongfully obtained property.

48. As set forth above, Defendants – through actual fraud, misappropriation, conversion, theft, or other questionable means – obtained Plaintiff's cryptocurrency, which in equity and good conscience Defendants should not be permitted to hold.

49. The cryptocurrency assets at issue are specific identifiable property and have been traced to MEXC, OKX, AND HTX.

50. Any and all assets being held by Defendants at MEXC, OKX, AND HTX must be held in trust for Plaintiff's benefit, and Defendants are not entitled to the benefit of wrongfully misappropriated, converted and stolen cryptocurrency assets that were taken from Plaintiff.

51. The digital assets identified herein which are being held by Defendants at MEXC, OKX, AND HTX must be disgorged to Plaintiff's benefit, as Defendants are not entitled to the benefit of wrongfully misappropriated, converted, and stolen cryptocurrency assets that were taken from Plaintiff.

WHEREFORE, Plaintiff JOHN J. BLUM demands the equitable imposition of a constructive trust over the property taken from Plaintiff that is currently under the control of Defendant "1" and/or JOHN DOES 1-20, in the identified cryptocurrency wallet addresses held at MEXC, OKX, AND HTX and further

demands that the wrongfully obtained property be returned to Plaintiff.

COUNT IV
CONSPIRACY

52. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 43 above as if fully and expressly set forth herein and further alleges as follows.

53. The Defendants conspired and confederated with each other to commit, and committed, Conversion (Count I); and Unjust Enrichment (Count II).

54. Plaintiff has suffered damages as a direct and proximate result of Defendants' conspiracy.

WHEREFORE, Plaintiff JOHN J. BLUM demands that judgment be entered against Defendant "1" and JOHN DOES 1-20, jointly and severally, for damages, interest, costs, and such other and further relief as this Court deems just and proper.

DEMAND FOR A JURY TRIAL

Plaintiff demands trial by jury on all issues so triable.

VERIFICATION

I, JOHN J. BLUM, hereby declare under penalty of perjury that I have read the foregoing COMPLAINT FOR CONVERSION OF STOLEN CRYPTOCURRENCY and verify that all statements herein are true and correct to the best of my knowledge, understanding, and belief.

Dated: December 01, 2023

DocuSigned by:
John Blum
971B3DF376BD468...

JOHN J. BLUM, Plaintiff

Dated: December 01, 2023

Respectfully Submitted,

/s/ Daniel J. Thornburgh

Daniel J. Thornburgh, Esq.
Fla. Bar No. 0042661
AYLSTOCK, WITKIN,
KREIS & OVERHOLTZ, PLLC
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449
dthornburgh@awkolaw.com

Attorney for Plaintiff