

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF LOUISIANA**

JEYSEN ZIVAN YOGARATNAM,
Plaintiff,

v.

DEFENDANT “1” a/k/a “DARINA DUBOIS”
and JOHN DOES 1-20, as yet unidentified
Individuals, Business Entities and/or
Unincorporated Associations,
Defendants.

CASE NO. 2:24-cv-00393

**COMPLAINT FOR
CONVERSION OF STOLEN CRYPTOCURRENCIES**

Plaintiff, JEYSEN ZIVAN YOGARATNAM, by and through undersigned counsel, sues DEFENDANT “1” a/k/a “Darina Dubois” and JOHN DOES 1-20, as yet unidentified Individuals, Business Entities and/or Unincorporated Associations and alleges as follows:

PRELIMINARY STATEMENT

1. Defendants stole 9.0584 BTC (Bitcoin) and \$39,770.36609 USDT (Tether) from Plaintiff which at the time of the theft had an approximate value of two hundred ninety-four thousand two hundred and fifteen dollars (\$294,215.00)¹ pursuant to a sophisticated global internet cryptocurrency fraud and conversion scheme.

2. Defendant “1” played a material role in the theft of Plaintiff’s assets, and upon information and belief, currently possesses all or a significant portion of Plaintiff’s stolen property.

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

¹ The approximate value of the stolen cryptocurrency at time of filing this Complaint is \$509,470.14625.

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).

THE PARTIES AND PERSONAL JURISDICTION

6. Plaintiff, JEYSEN ZIVAN YOGARATNAM, an individual, is *sui juris*, and is a resident and citizen of Nevada.

7. Defendant “1” is an individual, is *sui juris*, and is subject to the personal jurisdiction of this Court. Defendant “1” represented to Plaintiff Jeysen Zivan Yogaratnam that her name was “Darina Dubois.” Defendant represented to Plaintiff that she was American citizen but originally from Lyon, France. However, the parties’ communications demonstrated Defendant “1” was of Chinese descent who is likely located in Hong Kong, as further evidenced by the location of the bank to which Defendant “1” instructed Plaintiff to wire fraudulent fees.

8. 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.

9. 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.

10. 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 “https://www.ctrl-fx.com” which can be accessed on the internet and on smartphones and are accessible from Louisiana.

11. CTRL-FX claims to be operated by CTRL-FX Global Limited headquartered in London.

12. Further, based upon Defendants’ Hong Kong bank accounts to which Defendants directed Plaintiff wire purported fees and taxes, Plaintiff believes Defendants are likely located in China.

13. Furthermore, Plaintiff also believes Defendants are located in China because the CTRL-FX application presently links only to the Chinese Apple Store and shows only in Chinese characters.

14. Thus, alternatively, Defendants 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.

ALLEGATIONS COMMON TO ALL COUNTS

A. Defendants Execute an International Cryptocurrency Theft Scheme

15. Plaintiff desired to invest money in cryptocurrency.

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

17. In March 2023, Plaintiff met Defendant “1” a/k/a “Darina Dubois” who communicated with Plaintiff via LinkedIn.

18. Defendant “1” misrepresented that she would teach Plaintiff how to become a

successful cryptocurrency trader.

19. Defendant “1” lured Plaintiff by showing him examples over the Telegram app of how she was successfully earning high returns on her cryptocurrency trading methods.

20. Defendant “1” represented to Plaintiff that she was using a trusted cryptocurrency trading exchange called <https://www.ctrl-fx.com> that, according to Defendant “1”, was a legitimate forex trading website.

21. According to the CTRL-FX website, CTRL-FX is registered by the Financial Conduct Authority, which regulates financial services firms and financial markets in the UK registered. According to CTRL-FX, “[t]he FCA's mandate includes protecting investor rights, protecting and strengthening the integrity of the UK financial system, and promoting healthy competition among financial service providers for the benefit of consumers. Its core work is to regulate the market behavior of financial companies, investigate misconduct, supervise financial products, and ensure that financial services meet basic requirements or standards.” Furthermore, CTRL-FX website provides, “CTRL-FX will not use your funds for its business interests, and you can withdraw your funds at any time. All your funds will be segregated and deposited in a secure financial institution. This way, in case CTRL-FX goes bankrupt, all your money will be returned to you, as it will never be merged with our funds.”

22. Defendant “1” assisted Plaintiff in downloading and registering for an account at <https://www.ctrl-fx.com> which Defendant claimed was a legitimate trading mobile application. However, the application she provided to Plaintiff was not a legitimate exchange application. It was instead a fraudulent application created to deceive individuals, including Plaintiff, into believing they were investing funds with a legitimate cryptocurrency exchange.

23. Unbeknownst to Plaintiff, CTRL-FX was not a legitimate cryptocurrency

exchange, but was rather a simulated exchange – expertly engineered and designed to trick and deceive unsuspecting users into transferring their cryptocurrency assets into the fraudulent platform.

24. The CTRL-FX site mimics real time market movements. Users, including and specifically Plaintiff, can see real time market data and place trades; they believe they are trading in an authentic exchange platform, but are in fact placing simulated trades while the scammer Defendants convert the funds for their own use and transfer the funds to genuine exchanges for Defendants own use.

25. Upon registering for his CTRL-FX registering, Plaintiff was instructed by the CTRL-FX site to download the FX-6 app from the Apple Store.

26. Plaintiff used this FX-6 app, which also appeared to be a bona fide exchange application, to transfer his own cryptocurrency funds into the CTRL-FX exchange and place trades thereafter.

27. Presently, the FX-6 has been replaced by a nearly identical app in the App Store; however, it is now named in Chinese characters. Further, the app linked via the CTRL-FX website links to a Chinese Apple Store page.

28. 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 23rd, 2023, Defendant “1” had Plaintiff run a test where he transferred approximately \$5,735.00 worth of cryptocurrency from his Coinbase account into the fraudulent <https://www.ctrl-fx.com> exchange. When Plaintiff was able to transfer the cryptocurrency from the fraudulent exchange back to his Coinbase account, 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.

29. 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 Coinbase and Kraken accounts, legitimate third-party online platforms for buying, selling, transferring, and storing cryptocurrency, to the fraudulent platform.

30. Defendants posted fraudulent returns on their fake mobile application which made it appear that Plaintiff was making money on his trades. As a result, he continued to transfer cryptocurrency from his Coinbase and Kraken account to the fraudulent exchange.

31. When Plaintiff attempted to transfer even a small portion of his cryptocurrency from the fraudulent application back to his Coinbase and Kraken, Plaintiff experienced issues and was unable to make transfers.

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

33. Plaintiff was eventually convinced not to withdrawal his cryptocurrency but to instead invest more of it in the fraudulent CTRL-FX platform.

34. Because of the fraudulent representations contained on the fake CTRL-FX account, and misrepresentations made by Defendant “1”, Plaintiff Jeysen Zivan Yogaratnam believed that he had made significant money from the investment.

35. By the end of July 2023, Plaintiff believed he had made a considerable amount of money. In fact, Plaintiff was told by Defendant “1” that the value of his cryptocurrency had grown from approximately two hundred ninety-four thousand two hundred and fifteen dollars (\$294,215.00) to approximately two million two hundred eighty-eight thousand three hundred

seventy-eight and eighty-nine cents (\$2,288,378.89), which was also reflected on the fraudulent CTRL-FX application.

36. Plaintiff was happy with what he believed was a significant return on Plaintiff's investment. However, Plaintiff decided it was time to transfer all the cryptocurrency from CTRL-FX back to Plaintiff's own Coinbase and Kraken accounts.

37. However, Plaintiff was told that before Plaintiff could withdrawal Plaintiff's cryptocurrency, Plaintiff was required to transfer additional cryptocurrency to the fraudulent CTRL-FX exchange to pay additional fees and taxes.

38. Relying on these false statements, Plaintiffs transferred another \$484,460.83 worth of USD from his Bank of America account via wire to purported CTRL-FX bank accounts in Hong Kong in an effort to release the funds he believed to be held on the CTRL-FX exchange.

39. Unfortunately, even after paying what Plaintiff believed were the taxes and fees owed on his investments, Plaintiff made numerous unsuccessful attempts to transfer the cryptocurrency from the fake CTRL-FX account back to his Coinbase and Kraken accounts.

40. Plaintiff contacted CTRL-FX purported customer service demanding an explanation but was never responded to.

B. Plaintiff's Forensic Tracking of Their Stolen Cryptocurrency

41. 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.

42. Within the time frame of March 2023, and April 2023, Plaintiff made six (6)

transactions from his Coinbase and Kraken accounts to the fraudulent CTRL-FX exchange. In total, Plaintiff transferred approximately \$294,215.00 to the fraudulent exchange.

43. Plaintiff has retained forensic cryptocurrency tracing experts who have traced Plaintiff's stolen assets on the blockchain. Attached hereto as Exhibit "1" is the tracing report completed by experts at CNC Intelligence, Inc. Plaintiff incorporates Exhibit "1" into his verified complaint.

44. CNC Intelligence, Inc. traced Plaintiff's cryptocurrency on the blockchain and found that Defendants virtually absconded with Plaintiff's cryptocurrency and converted it for their own use. CNC Intelligence, Inc. found that Plaintiff's cryptocurrency was moved to four exchanges in wallets possessed and controlled by Defendants: Bitkub, Binance, Blofin, and Tokenlon.

COUNT 1
CONVERSION

45. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 41 above, as if fully and expressly set forth herein, and further alleges as follows.

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

47. 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.

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

WHEREFORE, Plaintiff Jeysen Zivan Yogaratnam 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

49. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 48 above, as if fully and expressly set forth herein, and further alleges as follows.

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

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

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

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

WHEREFORE, Plaintiff Jeysen Zivan Yogaratnam 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

54. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 53 above, as if fully and expressly set forth herein, and further alleges as follows.

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

56. This action further calls for the restoration to Plaintiff of that wrongfully obtained

property.

57. 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.

58. As set forth in Exhibit “1”, the cryptocurrency assets at issue are specific identifiable property and have been traced to Bitkub, Binance, Blofin, and Tokenlon.

59. Any and all assets being held by Defendants at Bitkub, Binance, Blofin, and Tokenlon 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.

60. The digital assets identified herein which are being held by Defendants at Bitkub, Binance, Blofin, and Tokenlon 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 Jeysen Zivan Yogaratnam 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 Bitkub, Binance, Blofin, and Tokenlon and further demands that the wrongfully obtained property be returned to Plaintiff.

COUNT IV
CONSPIRACY

61. Plaintiff adopts and realleges the allegations set forth in paragraphs 1 through 60 above as if fully and expressly set forth herein and further alleges as follows.

62. The Defendants conspired and confederated with each other to commit, and committed, Conversion (Count I); and Unjust Enrichment (Count II). Plaintiff has suffered damages as a direct and proximate result of Defendants' conspiracy.

WHEREFORE, Plaintiff Jeysen Zivan Yogaratnam 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, JEYSEN ZIVAN YOGARATNAM, 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: February, 15 _____, 2024

Jeysen Yogaratnam

JEYSEN ZIVAN YOGARATNAM, Plaintiff

Dated: February 15, 2024

Respectfully Submitted,

By: /s/ Reagan Charleston Thomas

Reagan Charleston Thomas

(LA Bar No. 38522)

**AYLSTOCK, WITKIN,
KREIS & OVERHOLTZ, PLLC**

17 East Main Street, Suite 200

Pensacola, FL 32502

Telephone: 850-202-1010

Fax: 850-916-7449

rthomas@awkolaw.com

Attorney for Plaintiff