Dimitri Nichols, Esq. (SBN 242098)
THE GORI LAW FIRM, P.C.
3848 W. Carson Street, Suite 350
Torrance, CA 90503
Telephone: (424) 383-1501
Facsimile: (424) 383-1504
E-mail: californiaservice@gorilaw.com

Samuel D. Elswick, Esq. (FL SBN 0105108)
(Pro Hac Vice Application Pending)
THE GORI LAW FIRM, P.C.
37 N. Orange Ave., Ste. 226
Orlando, FL 32801
Phone (321) 430-0864 | Fax (321) 234-0336
Email: selswick@gorilaw.com

Attorneys for: PLAINTIFF

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF YOLO

BRIAN M. SAMUELS, on behalf of himself and others similarly situated, PLAINTIFF, v. JOHN DOE NOS. 1-25, Defendants.	YOLO CASE NO. CV2026-1200 **VERIFIED COMPLAINT** **(1) CONVERSION** **(2) MONEY HAD AND RECEIVED** **CLASS ACTION**

GENERAL ALLEGATIONS

COME NOW PLAINTIFF BRIAN M. SAMUELS ("Mr. Samuels" or "Plaintiff"), on behalf of himself and all others similarly situated alleges as follows:

1. Plaintiff Brian M. Samuels is an individual residing in this jurisdiction.

2. This Court is the proper forum for trial of the within action, in that the dispute concerns exchange of currency and contractual obligations in this jurisdiction.

3. The true names and capacities, whether individual, corporate, associate or otherwise of the Defendants sued herein as DOES 1 through 25, inclusive, are unknown to Plaintiff, who therefore

sue said Defendants by such fictitious names. Plaintiff is informed and believes, and thereon alleges, that each of the Defendants designated herein as a fictitiously-named Defendant is in some manner responsible for the events and happenings herein referenced, either contractually or tortiously, and caused the damaged to Plaintiff as herein alleged. When Plaintiff ascertains the true names and capacities of DOES 1 through 100, inclusive, it will seek leave of this Court to amend this Complaint by setting forth the same.

4. At all times herein mentioned, each of the Defendants mentioned in the caption of this Complaint, which is incorporated herein by this reference, was and is the agent, servant and employee of each of the other Defendants and all the things alleged to have been done by said Defendants were done in the capacity of agent of the other Defendants.

5. Defendants Does 1–25 (collectively, "Defendants") operated or controlled a fraudulent online cryptocurrency investment platform accessible through the website Okdaxuda.com. Through that platform and related communications, Defendants engaged in a scheme commonly referred to as "pig butchering," in which victims are induced to purchase cryptocurrency and transfer it to wallet addresses designated by Defendants under the false representation that the assets will be invested on their behalf.

6. Plaintiff Brian M. Samuels was one of many victims of a coordinated cryptocurrency investment scheme. Mr. Samuels was contacted via email by an individual falsely purporting to be a former colleague and was informed of an alleged "foolproof" opportunity and method to invest in cryptocurrency. The email advised that, if interested, Plaintiff should respond affirmatively to receive further instructions. After Plaintiff responded, he was provided with additional communications directing him to a website operating under the domain Okdaxuda.com and related domains.

7. Over the course of several months, individuals associated with that website induced Mr. Samuels to purchase cryptocurrency and transfer those digital assets to cryptocurrency wallet addresses designated by Defendants. These transfers were made in reliance on false representations that the funds would be invested and remain under Plaintiff's control. Instead, the cryptocurrency was wrongfully diverted and retained by Defendants.

8. Plaintiff Brian Samuels is a retired individual who currently and at all relevant times herein resided in the city of El Macero, Yolo County, California.

9. Plaintiff is informed and believes, and on that basis alleges, that one or more of the Defendants operated, controlled, maintained, or otherwise utilized the website located at the domain **Okdaxuda.com**, which functioned as a fraudulent online cryptocurrency investment platform. Through that website and related communications, Defendants solicited and induced Plaintiff to transfer cryptocurrency to digital wallet addresses designated and controlled by Defendants, after which Defendants wrongfully retained and converted those digital assets.

10. Plaintiff is informed and believes, and on that basis alleges, that Defendants Does 1 through 25, inclusive, are individuals and/or entities who participated in, directed, controlled, operated, or otherwise facilitated the fraudulent conduct alleged herein, including the operation of the website referenced above and the control of cryptocurrency wallet addresses used to receive and transfer Plaintiff's digital assets. The true names and capacities of Defendants Does 1 through 25 are presently unknown to Plaintiff, who therefore sues these Defendants by such fictitious names pursuant to California Code of Civil Procedure section 474. Plaintiff will amend this Complaint to allege their true names and capacities when they are ascertained.

JURISDICTION AND VENUE

11. Jurisdiction is proper pursuant to California Code of Civil Procedure section 410.10 and Article 4 of the California Constitution, as this Court may exercise jurisdiction on any basis consistent with the Constitution of this State and of the United States.

12. Venue is proper in this Court pursuant to California Code of Civil Procedure section 395 because the obligations and transactions giving rise to this action were incurred in the County of Yolo, and the injuries alleged herein were sustained in the County of Yolo. Plaintiff is informed and believes, and on that basis alleges, that Defendant Okdaxuda.com and Defendants Does 1 through 25, inclusive, are non-residents of the State of California. Their true identities, forms, and locations are presently unknown to Plaintiff.

13. Plaintiff is informed and believes, and on that basis alleges, that Defendants purposefully directed their conduct toward California by soliciting Plaintiff while he was located in California

and induced him to transfer cryptocurrency from California, thereby causing injury within this state. Plaintiff's claims arise directly from those forum-related activities. The exercise of personal jurisdiction over Defendants is therefore proper and consistent with due process.

FACTUAL ALLEGATIONS

A. The Fraudulent Scheme

14. This action arises from a coordinated cryptocurrency investment fraud scheme through which Defendants induced Plaintiff to transfer cryptocurrency valued at approximately **$4,868,861.23** to blockchain wallet addresses controlled by Defendants. Forensic blockchain tracing conducted to date has identified **at least $4,149,761.13** of Plaintiff's transfers as moving through specific blockchain wallet addresses associated with Defendants and ultimately deposited into exchange-hosted wallets identified in **Appendix A**, which is incorporated herein by reference. The traced funds represent the portion of Plaintiff's losses that can presently be followed through publicly available blockchain transaction data. Additional portions of Plaintiff's transferred cryptocurrency were dissipated through laundering techniques, cross-chain transfers, decentralized exchanges, or other obfuscation methods that currently limit further tracing.

15. At all relevant times, Plaintiff, a resident of Yolo County, California, lawfully owned and maintained digital assets in custodial cryptocurrency accounts at Coinbase, Inc. The cryptocurrency transferred from this account constituted specific, identifiable digital property recorded on public blockchain ledgers and was at all times subject to Plaintiff's exclusive ownership and right to immediate possession.

16. Defendants, identified herein as John Doe Nos. 1–25, acted individually and in concert through a coordinated scheme designed to induce Plaintiff to transfer his cryptocurrency to blockchain wallet addresses designated by Defendants. Upon information and belief, Defendants operated through a fictitious online persona using fabricated images, biographical details, and electronic communications in order to cause Plaintiff to believe he was communicating with a legitimate and experienced cryptocurrency investor and former colleague identified as "Dan Vivoli" (hereinafter "Vivoli"). These representations were knowingly false and were made for the purpose of obtaining Plaintiff's cryptocurrency.

17. In or about November 2024, Plaintiff was contacted via email by an individual falsely purporting to be a former colleague identified as Vivoli and was invited to participate in a "fool proof" cryptocurrency investment opportunity. A subsequent communication provided instructions and a web address through which Plaintiff was directed to make investments in cryptocurrency.

18. Defendants represented that the individual identifying himself as Vivoli was a successful professional and experienced cryptocurrency investor capable of mentoring Plaintiff in cryptocurrency trading and wealth generation. Defendants further represented that Vivoli had discovered a "fool proof" method of online trading of cryptocurrency that allowed him to predict favorable trading opportunities in cryptocurrency markets.

19. In reliance on these representations, Plaintiff agreed to participate in cryptocurrency trading on the Okdaxuda.com platform under Defendants' direction. At Defendants' instruction, Plaintiff opened and funded a cryptocurrency exchange account at Coinbase, Inc. Plaintiff transferred U.S. dollars from his brokerage account at Charles Schwab to Coinbase, Inc., converted the funds into a cryptocurrency identified as USDC and then transferred the USDC cryptocurrency to the purported trading platform known as Okdaxuda.com for trading purposes.

20. Okdaxuda.com was not a legitimate trading platform but rather a fraudulent website operated and controlled by Defendants for the purpose of receiving, misappropriating, and converting victims' cryptocurrency. The representations described above were false and constituted part of a fraudulent scheme. The online trading platform identified as Okdaxuda.com was fake, and there was no actual investing done or profits made. The entire scheme was deliberately designed to entice victims like Mr. Samuels and other similarly situated individuals to deposit money into their accounts, as Plaintiff did, which was then misappropriated by Defendants.

B. The Fraudulent Trading Platform

21. Defendants operated and promoted a fraudulent cryptocurrency trading platform through the website Okdaxuda.com. Upon information and belief, the platform was designed to appear as a legitimate cryptocurrency exchange in order to deceive users and induce cryptocurrency deposits.

22. In online communications with Plaintiff, Defendants repeatedly represented that Okdaxuda.com had received Plaintiff's deposits and withdrawal requests, falsely suggesting that

Plaintiff's assets were being processed through a legitimate cryptocurrency exchange. Defendants reinforced this deception by using the domain name Okdaxuda.com, which mimics the name "okx.com," a legitimate cryptocurrency exchange. These representations created the false impression that the platform was affiliated with or connected to the legitimate exchange.

23. Defendants further represented that Plaintiff's cryptocurrency deposits had been received, converted, and credited through Okdaxuda.com. These representations were false and were made to induce Plaintiff to transfer additional cryptocurrency to wallet addresses designated by Defendants.

24. Defendants also imposed fabricated conditions on withdrawals from the platform, including demands that Plaintiff pay purported "taxes," to international bodies and state administrative agencies and additional "risk margins," or other deposits before withdrawals could be processed. Legitimate cryptocurrency exchanges do not collect taxes from customers or require advance payment of such taxes or "risk margins" in order to withdraw funds.

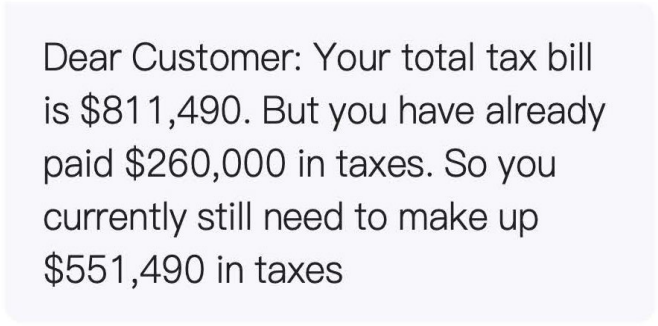
25. Through these misrepresentations, Defendants induced Plaintiff to transfer additional cryptocurrency while maintaining the false appearance of legitimate trading activity and preventing Plaintiff from withdrawing his assets.

26. Defendants represented that Plaintiff's cryptocurrency would remain credited to his account and be deployed in automated trading strategies designed to generate profits. The Okdaxuda.com interface displayed account balances and purported trading gains that Defendants represented were the result of successful trading activity. In reliance on these representations, Plaintiff initially transferred approximately $100,000 in cryptocurrency from his Coinbase.com account to Okdaxuda.com and engaged in trading activity that appeared to generate substantial profits, which increased Plaintiff's trust in the Okdaxuda.com platform.

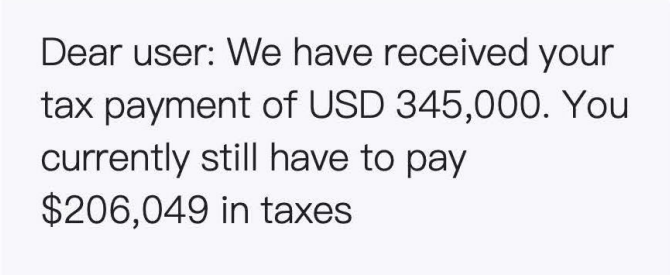
27. Before Plaintiff transferred larger sums, Defendants instructed him not to disclose to cryptocurrency exchanges or financial institutions that he was acting at another person's direction. Instead, Defendants instructed Plaintiff to represent that he was acting independently and purchasing cryptocurrency as a long-term investment. Upon information and belief, these instructions were given in order to conceal Defendants' involvement, avoid scrutiny from exchanges and financial institutions, and facilitate continued misappropriation of Plaintiff's assets.

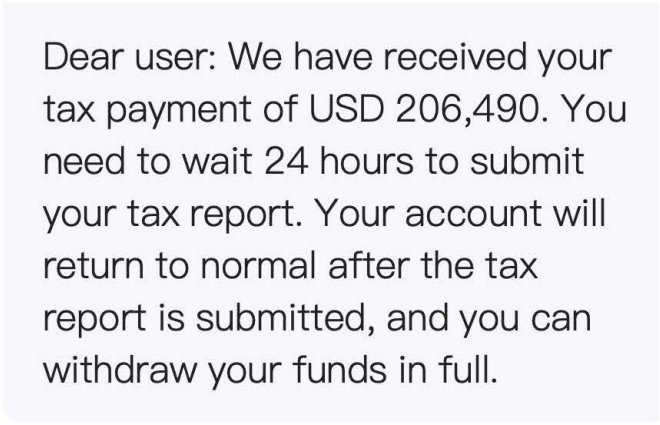
28. At Defendants' direction, Plaintiff began transferring increasingly larger amounts of U.S. dollars from his Charles Schwab brokerage account to his cryptocurrency exchange account at Coinbase.com, converting those funds into cryptocurrency, and then transferring the cryptocurrency to the Okdaxuda.com platform for purported trading in cryptocurrency.

29. In February 2025, Plaintiff attempted to withdraw his principal and purported profits from his Okdaxuda.com account. The withdrawal request was immediately denied. Okdaxuda.com representatives instead informed Plaintiff that his balance totaled approximately $8,722,849.59 USDT, and that he had generated substantial profits. Okdaxuda.com then represented that Plaintiff was required to pay purported taxes to the "International Tax Center" and "State Administration of Taxation," which appeared equal to around 15 percent of Plaintiff's alleged profits, approximately $811,490 USDT, before any withdrawal could be processed. A screenshot of Okdaxuda.com's communication imposing this requirement is shown below.

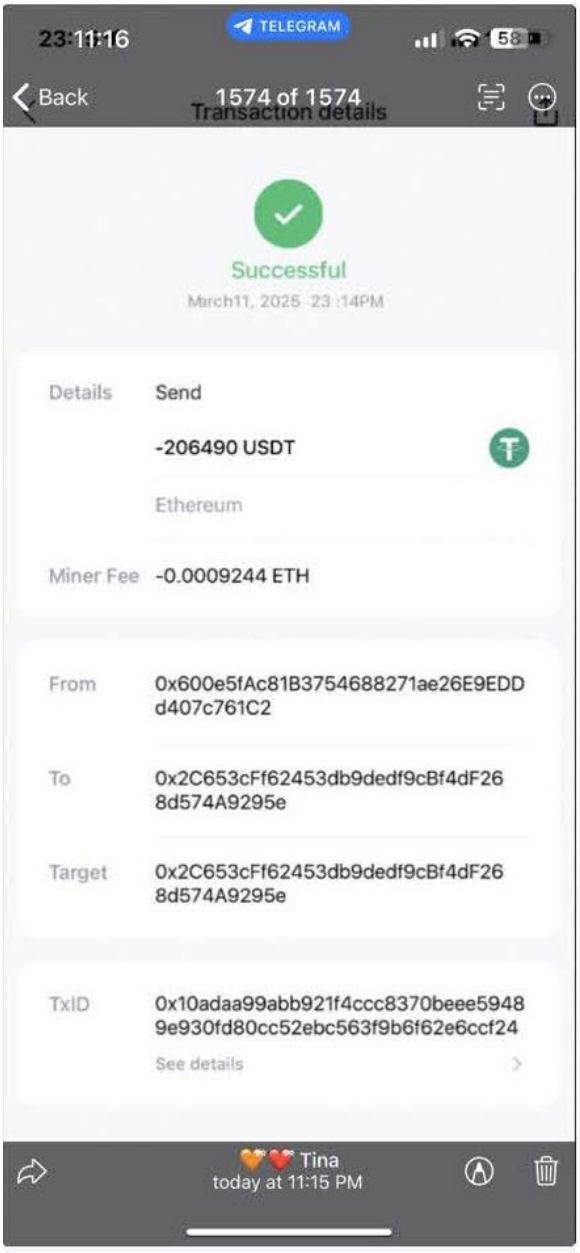


30. Believing that the payment was necessary to withdraw his funds, Plaintiff transferred approximately $260,000 USDT, and $346,743 USDT, valued at approximately $606,743.00 U.S. dollars, to Okdaxuda.com to satisfy the purported tax bill. Okdaxuda.com representatives then confirmed receipt of the two transfers and represented that they had used the cryptocurrency to satisfy Plaintiff's tax debt. A screenshot of this communication is shown below.



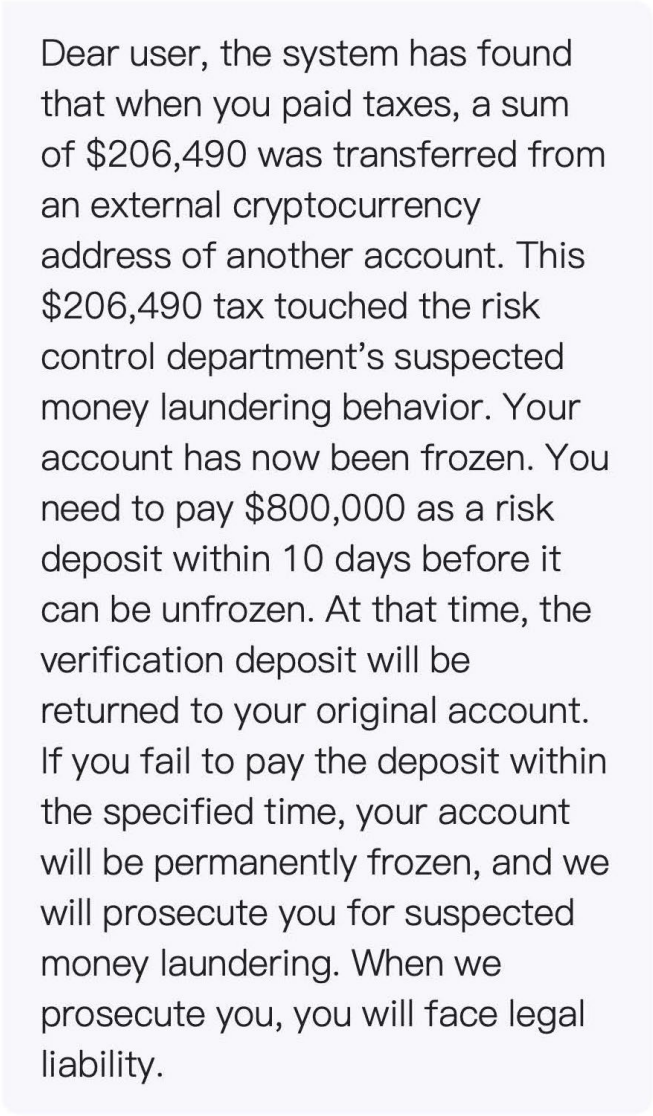


31. Upon information and belief, Defendants displayed within Plaintiff's account interface a purported transaction confirmation showing a transfer of 206,490 USDT and referencing a blockchain transaction hash. Subsequent review revealed that the referenced transaction corresponds to a different transaction involving a different amount and date, indicating that the transaction record shown by Defendants was inaccurate or misleading. Upon information and belief, Defendants presented the purported transaction confirmation to falsely suggest that Plaintiff's account involved suspicious funds and to mislead and confuse Plaintiff regarding the source of the transaction, which Defendants then used as a pretext to further freeze Plaintiff's account and demand additional payments from Plaintiff. A screenshot of this alleged transaction is shown below.



32. After the purported tax was allegedly paid, Plaintiff again attempted to withdraw his assets. However, Okdaxuda.com's representatives again refused to process the withdrawal. Instead, they informed Plaintiff that his withdrawal request had been placed on hold pending review by the Okdaxuda.com's "risk control department" because Plaintiff's payment of the alleged $206,490 tax was "transferred from an external cryptocurrency address of another account," and therefore, Plaintiff's account was frozen until he paid an $800,000 "risk deposit" within ten days. Okdaxuda.com's representatives further threatened to permanently freeze Plaintiff's account and

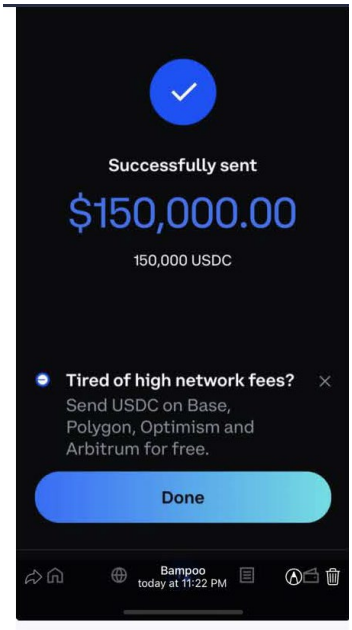
prosecute him for suspected money laundering and other "legal liability" if he did not pay the alleged risk deposit. A screenshot of this communication is shown below.



33. At this point, Plaintiff's finances were nearly drained but faced with the threat of prosecution for money laundering and freezing of his account, Plaintiff agreed to pay Okdaxuda.com the last $150,000 that he had to his name and desperately pleaded with them to give him a thirty-day extension to pay the remaining $700,000 that Okdaxuda.com alleged he owed. A screenshot of this communication is shown below.

I only have $150,000 that I can pay towards the $850,000 verification deposit that you told me I owe. I will deposit that later today (California time). How long after I make the $150,000 deposit will you be able to tell me the length of my extension? I desperately need at least 30 days extension. Thank you.

34. Relying on Okdaxuda.com's representation that a risk margin payment was required to release his funds, and halt prosecution on the alleged money laundering charges, Plaintiff transferred $150,000 USDC to Okdaxuda.com, valued at about $150,000 U.S. dollars. Plaintiff also requested a 30-day extension to pay the remaining balance of $700,000 that Okdaxuda.com alleged he owed. Screenshots of this communication are shown below.



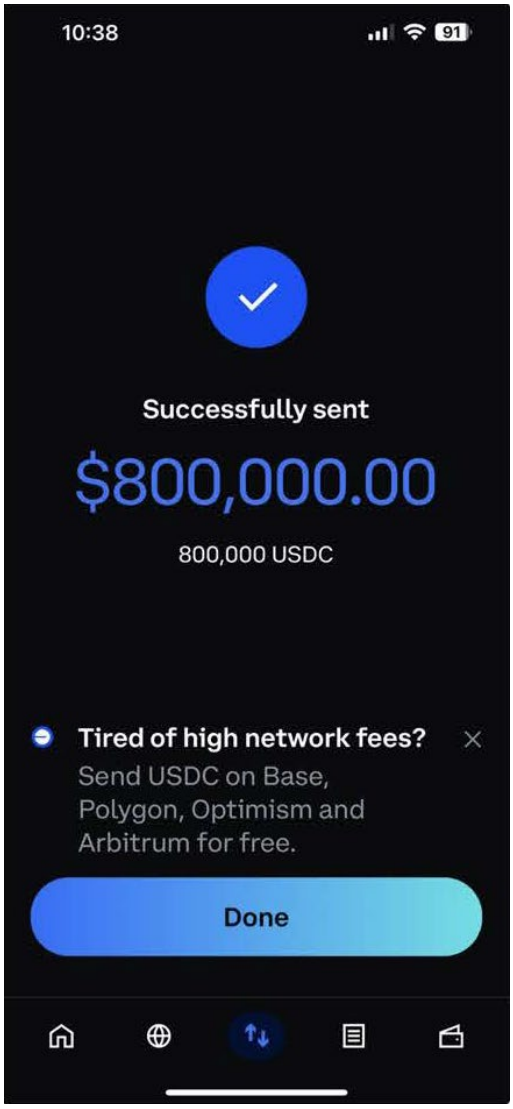
I just deposited $150,000 large withdrawal risk deposit. Please tell me how much extension you can give me. I request 30 days. Thank you

///

///

35. After Plaintiff complied with the risk margin demand and made his initial payment of $150,000, he received another threatening message from Okdaxuda.com that he had until March 30, 2025, to pay the balance of the alleged $700,000 large withdrawal risk deposit or his account would be permanently frozen and he would be prosecuted. Okdaxuda.com additionally threatened Plaintiff that if the $700,000 alleged risk margin was not paid by the due date, his account would be fined an additional $5,000 per day. A screenshot of this communication is shown below.

36. On March 18, 2025, Plaintiff complied with Okdaxuda's demand and paid them an additional $800,000 USDC valued at $799,000 U.S. dollars. A screenshot of this communication is shown below.



37. After Plaintiff had paid the $800,000 risk margin Okdaxuda.com alleged was due, they again froze his account alleging that his withdrawal application had been rejected by the "blockchain node" due to the large amount of his withdrawal and that in order to "protect the safety of your funds" his account would be frozen until he paid an additional $850,000 as "risk money" to verify the account security for large withdrawals. A screenshot of this communication is shown below.

> Dear user: Your account is at risk of triggering an alert due to large withdrawals. Your account has not experienced any large withdrawals before. Therefore, in order to verify the security of your account and funds, you need to pay a deposit of $850,000 to verify the security of your large withdrawal account. After you pay the $850,000 deposit, your account will return to normal, and the $850,000 deposit will also be returned to your options trading account. Please pay the deposit within the specified time.

38. After Okdaxuda.com imposed this additional payment demand, Plaintiff informed the Okdaxuda.com representatives that he was unable and unwilling to transfer further funds. Plaintiff had by that time exhausted his available resources and remained unable to withdraw the assets displayed in his Okdaxuda.com account.

39. Upon realizing that the platform was fraudulent, Plaintiff acted diligently and immediately undertook efforts to recover his converted property. Plaintiff filed a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) and contacted the United States Secret Service. Plaintiff also retained two cryptocurrency tracing firms, ZeroShadow and Outrider Analytics, to investigate the transactions. Despite months of effort, Plaintiff was advised that recovery through those channels was not possible.

40. Plaintiff thereafter retained Inca Digital ("Inca"), a cryptocurrency investigation firm, which conducted a forensic blockchain analysis of Plaintiff's transactions. Inca confirmed that Defendants operated a common scheme through the online platform described above and traced Plaintiff's cryptocurrency to specific wallet addresses associated with that scheme. On information and belief, and based upon Inca's investigation, numerous similarly situated victims transferred cryptocurrency to the same or related wallet addresses as part of the same standardized operation.

41. At all relevant times, Plaintiff retained the lawful right to immediate possession of the transferred cryptocurrency. The assets are specifically identifiable on public blockchain ledgers and traceable to recipient wallet addresses controlled, directly or indirectly, by Defendants. Defendants exercised unauthorized dominion and control over Plaintiff's digital assets and converted those assets to their own use.

C. Plaintiff's Cryptocurrency Transfers to Scam-Controlled Intake Wallets

42. Between **December 27, 2024 and March 18, 2025,** Plaintiff transferred cryptocurrency valued at approximately **$868,861.13** across **14 cryptocurrency transactions** to **Intake Wallets**—the first known scam-controlled addresses to which perpetrators directed the Plaintiff to send assets. From those wallets, the Defendants systematically moved funds through a series of additional transactions—sending the funds through a maze of other intermediate addresses until they ultimately reached **Exchange-Hosted Deposit Wallets**. Forensic blockchain tracing conducted to date has identified at least **$4,149,761.13** of Plaintiff's transfers as flowing through blockchain wallets associated with Defendants and ultimately deposited into exchange-hosted accounts identified in **Appendix A**.

43. In total, the Victim sent funds to one Intake Wallet:

Intake Wallet #1: 0x525ccc3e1631657d2bc00ff1684c7109d3d27336.

Cryptocurrency received in these intake wallets was subsequently transferred through intermediary blockchain addresses and ultimately deposited into exchange-hosted deposit wallets at Binance, OKX, Bybit, HTX, Gate.io, MEXC, Bitget, Kraken, FixedFloat, and KuCoin.

44. After receiving Plaintiff's cryptocurrency in the intake wallets, the funds were transferred through intermediary blockchain addresses designed to obscure the origin, ownership, and control

of the cryptocurrency before ultimately being deposited into exchange-hosted deposit wallets.

D. Tracing Summary and Exchange Deposit Wallets

45. Forensic blockchain analysis traced Plaintiff's cryptocurrency from the Intake Wallets through subsequent transactions to exchange-hosted deposit wallets associated with cryptocurrency exchanges **Binance, OKX, Bybit, HTX, Gate.io, MEXC, Bitget, Kraken, FixedFloat**, and **KuCoin** and others.

46. These exchange-hosted deposit wallets represent the last known locations where cryptocurrency traceable to Plaintiff's transfers was deposited and therefore remain at risk of transfer, liquidation, or dissipation absent court intervention.

47. Additional tracing details, including wallet identifiers, transaction hashes, and transaction flow diagrams, are set forth in the supporting materials filed in connection with Plaintiff's Motion for Temporary Restraining Order.

48. Forensic blockchain tracing has identified exchange-hosted deposit wallet addresses that received cryptocurrency traceable to Plaintiff's transfers and, upon information and belief, transfers made by similarly situated victims. The wallet identifiers are set forth in Appendix A, which is incorporated herein by reference.

E. Broader Fraud Network Allegations

49. Forensic blockchain analysis indicates that the same intermediary wallets and recipient addresses involved in Plaintiff's cryptocurrency transfers are also associated with deposits from additional victims exhibiting similar transaction patterns. Upon information and belief, these patterns reflect a broader coordinated cryptocurrency fraud scheme rather than an isolated incident.

50. Upon information and belief and based on forensic blockchain analysis, Defendants operated a centralized and standardized fraudulent scheme designed to defraud victims through a uniform pattern of misrepresentations and cryptocurrency transfers to wallets under Defendants' control. The scheme was carried out through common methods, common wallet infrastructure, and uniform misrepresentations directed to numerous victims, resulting in similar financial harm to members of the proposed Class.

51. The scheme involved facts common to members of the Class, including, but not limited to, the following: (i) the use of standardized written communications designed to persuade victims to enroll in a fraudulent online investment platform, including communications through social media and messaging applications, the use of fictitious identities, and uniform misrepresentations concerning cryptocurrency investments and the purported need for victims to deposit cryptocurrency into the platform in order to participate in investments and receive purported profits; (ii) the common use of cryptocurrency exchanges and wallet applications by Class members to transfer funds to cryptocurrency wallets controlled by Defendants; (iii) the unlawful conversion and misappropriation of cryptocurrency belonging to Class members for Defendants' own use and benefit; (iv) the use of common cryptocurrency wallet addresses controlled by Defendants, including the transfer of cryptocurrency to the deposit addresses identified in **Appendix A** to this Verified Complaint; and (v) substantial and similar financial harm suffered by Class members as a result of Defendants' conversion of their cryptocurrency assets.

52. Because cryptocurrency transactions are permanently recorded on public blockchains, Defendants' scheme—including the transfer of victim funds to common wallet clusters and deposit addresses—can be traced and proven through common evidence applicable to all Class members.

53. Much of the evidence necessary to prove Defendants' scheme—including blockchain transaction records, exchange account records, wallet tracing analysis, and the communications used to recruit victims—will be common to the Class and will not require individualized proof. Accordingly, Defendants' conduct presents questions of law and fact common to the Class that predominate over any questions affecting only individual members.

54. Plaintiff and other similarly situated individuals lawfully owned and possessed the cryptocurrency transferred from their exchange accounts. These assets constituted specific, identifiable digital property recorded on public blockchain ledgers and traceable to wallet addresses designated by Defendants and under their control.

55. Defendants knowingly and intentionally exercised unauthorized dominion and control over Plaintiff's and other similarly situated individuals cryptocurrency by inducing them to transfer the assets to wallet addresses under Defendants' control and thereafter routing the cryptocurrency

through intermediary blockchain addresses to conceal its origin and ownership. Plaintiff was permanently deprived of possession and control of his property.

56. Defendants acted in concert, including the individual communicating with Plaintiff as "Vivoli," operators of the Okdaxuda.com platform, and persons controlling the recipient wallet addresses used to receive and transfer Plaintiff's cryptocurrency. Their coordinated conduct was undertaken to obtain and convert Plaintiff's and other similarly situated individuals' cryptocurrency for their own benefit, thereby depriving them of their property.

57. Defendants have been unjustly enriched by receiving and retaining Plaintiff's and other similarly situated individuals' cryptocurrency, which in equity and good conscience belongs to them.

58. Plaintiff retains the immediate right to possession of the cryptocurrency transferred from his accounts, and those assets remain traceable to exchange-hosted deposit wallets identified through forensic blockchain analysis. Defendants' continued retention of these assets is unlawful.

F. International Cryptocurrency Fraud Context

59. Upon information and belief, the scheme described herein is part of a coordinated cryptocurrency fraud operation in which victims are induced through fraudulent communications and fabricated trading platforms to transfer digital assets to blockchain wallets controlled by the perpetrators.

60. Such schemes commonly involve the rapid movement of cryptocurrency through multiple blockchain addresses before deposit into exchange-hosted wallets, after which the assets may be converted to fiat currency or transferred to additional wallets in order to conceal their origin.

61. Forensic blockchain tracing of the Plaintiff's transactions revealed that the misappropriated cryptocurrency was routed through a series of intermediary cryptocurrency wallets (the "Pivot Wallets") before being transferred onward through additional laundering layers. By tracing inflows into these known Pivot Wallets, forensic analysts identified numerous additional wallets that followed the same structured fund-movement patterns observed in the Plaintiff's transactions.

62. The identified wallets exhibited the same laundering behaviors as the Plaintiff's funds, including matching structured transaction pathways across multiple similarly situated individuals,

the aggregation of funds from different individuals into the same intermediary Pivot Wallets before onward transfers, and consistent transaction patterns reflecting the same laundering techniques used to move and conceal the misappropriated cryptocurrency.

63. The use of common Pivot Wallets and uniform transaction pathways demonstrates that Defendants processed cryptocurrency through a centralized laundering infrastructure designed to receive, pool, and transfer funds misappropriated from Plaintiff and other similarly situated individuals through the same fraudulent investment scheme.

64. Based on this forensic tracing analysis and upon information and belief, the proposed Class presently includes potentially hundreds of similarly situated individuals who collectively lost approximately **$21.1 million in cryptocurrency** as a result of Defendants' fraudulent scheme. The identities of additional Class members and the full extent of damages will be confirmed through discovery and continued blockchain tracing analysis. Blockchain tracing indicates that the same wallet cluster processed cryptocurrency from numerous victims following the same laundering pathways.

65. Once cryptocurrency is transferred out of exchange custody and off-ramped into fiat currency or privacy-enhancing wallet infrastructure, recovery becomes significantly more difficult or impracticable.

66. Because Plaintiff's and other similarly situated individuals' cryptocurrency remains traceable to exchange-hosted deposit wallets identified through forensic blockchain analysis, a limited window exists in which injunctive relief may prevent further dissipation. Delay in freezing the assets materially increases the risk that the cryptocurrency will be transferred, liquidated, or otherwise placed beyond the reach of this Court. Cryptocurrency can be transferred across jurisdictions within minutes, making judicial intervention necessary to preserve the Court's ability to grant effective relief.

CLASS ALLEGATIONS

67. This action may be properly maintained as a class action pursuant to California Code of Civil Procedure section 382.

68. The proposed class definition is proposed as follows:

> All persons or entities who, during the applicable limitations period, transferred cryptocurrency to blockchain wallet addresses associated with the Okdaxuda.com scheme described herein, and whose cryptocurrency was misappropriated as part of that scheme.

69. Excluded from this Class are individual Defendants and their families, corporate Defendants and their officers, directors and affiliates, if any, at all relevant times. Defendants' legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

70. Plaintiff reserves the right to amend or modify the Class in connection with a motion for class certification or as the result of discovery.

71. Plaintiff is informed and believes that the members of the proposed class are so numerous that joinder of all members is impracticable. Based on the investigation to date, the number of affected persons is substantial and geographically dispersed. Upon information and belief, the Class includes at least 100 members.

72. The identities of class members are ascertainable through blockchain tracing analysis, wallet records, exchange records, and discovery directed to entities that processed or facilitated the cryptocurrency transfers described herein.

73. Common questions of law and fact predominate, including whether Defendants operated or controlled the online platform, whether Defendants controlled or utilized the wallet addresses described herein, whether the cryptocurrency transferred to those addresses was wrongfully retained or converted, and whether declaratory and injunctive relief is warranted to preserve and recover the digital assets at issue.

74. Plaintiff's claims are typical of the claims of the Class because they arise from the same course of conduct and involve the same alleged wrongful retention and conversion of identifiable cryptocurrency.

75. Plaintiff, like all other members of the Class, sustained damages arising from Defendants' scheme and subsequent transactions to convert stolen property and hide the locations of victims' cryptocurrency assets. The representative Plaintiff and the members of the Class were, and are,

similarly or identically harmed by the same unlawful, deceptive, unfair, systematic, and pervasive pattern of misconduct.

76. Plaintiff, like all other members of the Class, is entitled to the same declaratory, injunctive and other relief as the members of the Class.

77. Plaintiff will fairly and adequately represent and protect the interests of the Class. There are no material conflicts between the claims of the representative Plaintiff and the other members of the Class, including absent members of the Class, that would make class certification inappropriate.

78. Counsel selected to represent the Class will fairly and adequately protect the interests of the Class and have experience in complex and class litigation and are competent counsel for class action litigation. Counsel for the Class will vigorously assert the claims of all members of the Class.

79. This action is properly maintained as a class action in that common questions of law and fact exist as to the members of the Class and predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy, including consideration of: the interests of the members of the Class in individually controlling the prosecution or defense of separate actions and/or proceedings; the impracticability or inefficiency of prosecuting or defending separate actions and/or proceedings; the extent and nature of any litigation concerning the controversy already commenced by members of the Class; the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and the difficulties likely to be encountered in the management of a class action.

80. Among the numerous questions of law and fact common to the Class are as follows: whether Defendants have acted or refused to act on grounds generally applicable to the Plaintiff and the Class; whether Defendants have a pattern, practice, and scheme of "pig butchering" and subsequent digital transactions to convert stolen property and hide the locations of victims' cryptocurrency assets; to what extent Plaintiff and members of the Class are entitled to damages; and to what extent Plaintiff and members of the Class are entitled to declaratory and injunctive relief.

81. Defendants have consistently acted and refused to act in ways generally applicable to the Class. Thus, final declaratory and injunctive relief with respect to the entire Class is appropriate.

82. Plaintiff and the members of the Class have suffered or are at imminent, severe, and

unacceptably high risk of suffering irreparable harm because of Defendants' ability to move funds at any time, without notice. If Defendants withdraw funds, Plaintiff and the members of the Class will not be able to recover their funds and would lose their property forever.

83. Absent injunctive relief, Plaintiff and the proposed class face a substantial risk of irreparable harm, as Defendants may transfer or dissipate the digital assets at issue at any time through additional blockchain transactions.

FIRST CAUSE OF ACTION

(For Conversion)

(Against Each Defendant)

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

85. Plaintiff and the other members of the Class transferred assets owned by them to Defendants.

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

87. As a result of the foregoing, Plaintiff and the other members of the class have been deprived of the use of the above assets and damaged in an amount to be established at trial.

88. 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 or the other members of the Class.

89. Plaintiff, on behalf of himself and all others similarly situated, accordingly requests imposition of compensatory damages, in addition to exemplary and punitive damages, against Defendants, as well as appropriate equitable relief, including but not limited to entry of a preliminary and permanent injunction that seizes and returns to Plaintiff and the Class the cryptocurrency assets contained in the cryptocurrency wallets listed in **Appendix A** herein.

SECOND CAUSE OF ACTION

(For Money Had and Received)

(Against Each Defendant)

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

91. As described more fully above, Defendants received money and property from Plaintiff and the similarly-situated members of the class intended to be used for the exclusive benefit of Plaintiff and the class, respectively.

92. Defendants did not, in fact, use the money and property received from Plaintiff and the members of the class for their benefit, but instead used that money for themselves.

93. As a result of the foregoing, Plaintiff and the members of the class have been damaged in an amount to be established at trial and request compensatory damages in an amount to be established at trial in addition to appropriate equitable relief, including but not limited to entry of a preliminary and permanent injunction that seizes and returns to Plaintiff the class the cryptocurrency assets contained in the cryptocurrency wallets listed in **Appendix A** herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an award against Defendant as follows:

1. For compensatory damages in excess of $4,868,000, in an amount to be proved at trial;
2. For punitive damages in excess of $15,000,000 due to Defendant's wrongful conversion of funds;
3. For attorney's fees and costs of suit as allowed by law;
4. For pre- and post-judgment interest; and
5. For imposition of a constructive trust and/or equitable lien over all traceable proceeds of Plaintiff's funds, including cryptocurrency or fiat accounts holding such proceeds; and
6. For such other relief as the Court deems just and proper.

DATED: April 6, 2026

THE GORI LAW FIRM, P.C.

By: _____

Dimitri N. Nichols (CA SBN 242098)
Counsel for Plaintiffs

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

DATED: April 6, 2026

THE GORI LAW FIRM, P.C.

By: _____

Dimitri N. Nichols (CA SBN 242098)
3848 W. Carson St. Ste. 350
Torrance, CA 90503-6729
Phone (414) 383-1501 | Fax (424) 383-1504
californiaservice@gorilaw.com

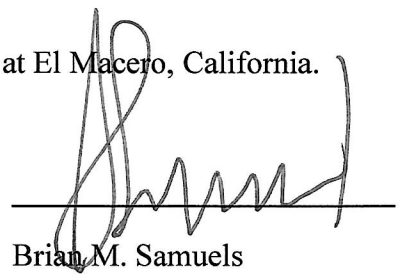
VERIFICATION

I, Brian M. Samuels, declare:

I am the plaintiff in this action and have read the foregoing Verified Complaint, know the contents thereof, and certify that the same is true to the best of my knowledge, except as to those matters stated on information and belief, and as to those matters, believe them to be true.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on Mar 26, 2026, at El Macero, California.



Brian M. Samuels

APPENDIX A

Binance (42)

THNttSkLDWZ2vjJ7TC6JvuFRdwNaA3dP8F

TNsYvCGbmQaoF7PYkYpQbGEc4qaBN4JSrY

TJqr63cMVWRveDePA5Hufbdro9Gbua2rty

TKhpHGDRXrhnufCphzAHj37pd641wh3hyw

TF7wMYNphv8J6spRCnV9Y5zq6eSWdJngk9

TRLqkZKGEznV1J1ZYMmTJFTXie5uR74auR

TTg1u2hbKtgkZcfh8uHHG4qcCE892Vfn3C

TPa13azfzWevjTtqV6hQasSmygVk5gGbwd

TTH7TAt5iooLXSHAq9oX3V3TwB9P1uzPig

TBKYANtrr6AuncVbNNB7mz1D2XgYGa2Wpn

TC4gQS3iHQSxsxYCPAatNYt58CbZSFdXNA

TFUC1JFqeeEpW4NMcmbgEmE94HY1fdtUSp

TUpXKjk8P22DxCWFEnpyD4HCuqZJtvZFye

THjVQp8ySUJTtWGrMf9hpidnRQLmS8SBcR

TSuQjLyvcM2sPAtM9Xo87UCcukGMKUpGn3

TAwgMvibaKerEupQVhRiRGHvmYgfQ4us9sv

THNttSkLDWZ2vjJ7TC6JvuFRdwNaA3dP8F

TXLujcy8oURHZkoVhdkGWorB3cqZqSj9bb

TJzquiiNesTr7iUE9ToeEddccLB1tisT2P

TShRoVDD8nxTpMMB53XjC7SZU4Y3joGubc

TTTQnjdc9GG9EjuP4jYHzx7wtpGXaqN1ti

TQrBaHHmmLXmAgMjGKxt5MChVKFbeqw2CJ

TYfVaiGaV7tSYyHy1txeYomVyU1t7nsxTF

TQrBaHHmmLXmAgMjGKxt5MChVKFbeqw2CJ

TC3zMkEtSk4aedh385aCVG1XostumUsWoW

TUJBiR24MWGXnBcHEaBCLQzYUEUhxKY8PP

TBfTVVJUd834av9nHux4j3wAYMdjQ9NgRj

TJwvvuur77dxnaHB3uEwDzLY6CeuXUaRUC

TSVK6bcrM94uvXMF9ieQ6XbgLc6fGJq3Ca

TK6GJDBbDwvvb1JPp2Y1pX6A54R5bdkVuP

TUoqpzipR9ghYLwu3Qkazd3AXyUucU3Dq9

TATPwcimMZmJctvQPXAY9QCaPdfxXqEBXs

TFYDfwq4KwNdQDQEjeVcwu9EZkuRghaSAS

TEJLuKgWYdS9cyjFYQpCodC2TyRPHGn2Sz

TJRncdeGcJqtUidKU7F6NHC8Pc9cj1mbs1

TLmNyFS88swiMAskucJhndDGZpZDN3bpwc

TTjCyPXjLBox5nsx1v4XXmpUVxSc4Ti7JE

TYegccZnMMtpYcNFQMfh79hyxbB4HGzPu5

TU6Eun751wDs9BRGXrJYYCqxxZspkpUnkf

TKst1Uiy8uy9ud9t3FXxrsjLoWPkH9rzeA

TUSa7RW3a4toySugQjyJyRXjQYkJCqA8us

TJSumRVVzDXRp7mMrfbSaAjj9iwmySnyA4

OKX (24)

TTMJLdJR7BTBSgfHL3ENvn4hut552a364G

TFnihNhC2H2sEyn2Dw75dJBy7jykcKbZei

THVHyp4TxyWbFeSmjJT4DmCcGxzsMVw1MC

TBoU8qmj8LhuiKStN2JUDEYXWBz94e6G1P

TYyfkAw8HCUhiQMbiU5v4FEquNGf659kdF

TWn1zcLGck67VfweGVVyUtWQK8hTtghPSr

TGEasWGn2MoUXHuj4RNkNZeb8vK7SKkiCn

TGrrVrAyC1GaPpwEiStdfzrs7Wz6Pougiw

TGEasWGn2MoUXHuj4RNkNZeb8vK7SKkiCn

TRXPRc6bhiAW6n38BFYStKJqYX1EbCnLF2

TU6SvAziDNnDD6j8ZRK4fiHiN9xcZGXJ4b

TJ3HHjCW4G5sr9ec3iWmEd1Ct61WqAi8QA

TTcCKqhh3qmWkCh16WddkwMv8tRPEb1BKw

TXwAR9nVF36JUFHrxHvj42f69uCDhGaZF1

TTKkmbWQqBpcP7riBhBuoPug87aPw3gEAL

TWwaSWH4EVyUU7ab8zgR8MSnKGJwHiakS3

TEGimixjnuHzd2XoYBiAuxXPvKdd2A1ksA

TVkxpYbrZbZUmyYapspvxofhZC8XEm5gWi

TSFndv7vEm1ETECfZXStUSx5GrmPZr4UBx

TKJrFQFT7a5NwVERhfNqvfaEZAcNKPKzSD

TNc8j9NdXS5mcickNeMW9dxxCiwn9NWR7P

TY86SnUpBfghkYotPe8qHqKtrYCzcwRwnP

TEe9pPd8oFpeimJJYugwTQzjs5JDy7869G

TATAK8z5WJXSqeoNSj7iuNTyVgDiPKL1uy

Gate.io (11)

TWS4FhKA1wGZJvDfMavTqUsMutTRhSu4Ek

TH65psJRGgztAE42dNSrW7aMWxb652bZtE

TAZcARfKQug3Hx4ZfRqwyfsq5MKmQ8PH1e

TLmys3Frztnrg3Gjtw3zduQMKjH8xr8cVr

TD8B7MpeV97WCtwojTkCzcgCAmyc6HMZCZ

TUcxVJkqpV6bV4zi3uePMJbJ3QspdLmgvv

TLmys3Frztnrg3Gjtw3zduQMKjH8xr8cVr

TKw6T6rFTno7SbVjvdJCGKZfub5t83i2WS

TM3XbAxCqojR12xYQNUycDjXrCTi1rMWyk

TXoBA7cgrCGJxGUHUoSHbLYF8hkngtAaHE

TYf6oi8SAjerRSGs1nCTYhw4jGWjqkpBeX

Kraken (2)

TCcsLwUi7M12MQddQbyZ2XSqY1ZYhn49JY

TLsH1CGwKbe4WrrJ2T7BGyaWhxaeuFHqz4

KuCoin (1)

TSDYHbXRkYyMqsifvGSoUZXPF4A62AiqGA