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 **PLAINTIFF'S EX PARTE APPLICATION FOR TEMORARY RESTRAININNG ORDER AND OSC RE: PRELIMINARY INJUNCTION;** **MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT;** **DECLARATION OF BRIAN SAMUELS, MAYA VICK AND DIMITRI NICHOLS [FILED CONCURRENTLY HEREWITH];** **[PROPOSED] ORDER AND ORDER TO SHOW CAUSE [FILED CONCURRENTLY HEREWITH]** Date/Time: May 21, 2026 at 9:00 a.m. Dept.:14

PLEASE TAKE NOTICE that Plaintiff Brian Samuels, on behalf of himself and all others similarly situated, hereby applies *ex parte* for a Temporary Restraining Order ("TRO") as follows:

1. Asset Freeze of Identified Cryptocurrency Wallets

Restraining Defendants **JOHN DOE Nos. 1–25**, and non-party cryptocurrency exchanges

Binance, OKX, Gate.io, Kraken, and KuCoin, together with their respective agents, servants, employees, attorneys, affiliates, partners, successors, assigns, subsidiaries, and all persons acting in concert or participation with them who receive actual notice of the Court's Order, whether by personal service or otherwise (collectively, the "Enjoined Parties"), from withdrawing, transferring, selling, encumbering, or otherwise altering any cryptocurrency or other assets held in the wallet addresses identified below, whether such property is located inside or outside the United States.

Plaintiff further requests that the Court order the asset freeze to apply to assets within the custody or control of the exchanges regardless of where such assets are located, and that the exchanges preserve all account records, transaction histories, login records, IP logs, and related information associated with the identified wallet addresses pending further order of the Court.

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

The wallet addresses identified above were determined through forensic blockchain tracing to contain proceeds of Defendants' fraudulent scheme. Immediate relief is necessary because cryptocurrency transactions are irreversible and can be transferred across blockchain networks within seconds.

2. Notice to Account Holders

A. Alternative Service of Notice on Account Holders

Plaintiff requests the Court allow service of the proposed Temporary Restraining Order ("TRO") and Order to Show Cause ("OSC"), together with a copy of the papers upon which they are based, as well as the Verified Complaint and Summons and all other papers and orders in this action, to be served upon the person or persons controlling the wallets identified in Paragraph 1 above, as well as **Appendix A** of the proposed Order, via a special purpose token or similar device

delivered into each of the wallets identified in **Appendix A** of the Order, and each of these service tokens will contain a hyperlink to a website maintained by Plaintiff's counsel that will include both the Order and all papers upon which it is based. The hyperlink will include a mechanism to track when a person clicks on the hyperlink. This process shall constitute actual notice of this Order and sufficient service of process on Defendants and the person or persons controlling the corresponding wallet addresses identified in **Appendix A** of the Order.

B. Notice by Non-Party Exchanges

Binance, OKX, Gate.io, Kraken, and KuCoin, together with their respective agents, servants, employees, attorneys, partners, affiliates, successors, assigns, subsidiaries, and all persons acting in concert or participation with them who receive actual notice of this Order by personal service or otherwise, are hereby directed within twenty-four (24) hours of receiving actual notice of this Order to:

a. Provide notice of this Order to any of their customers associated with the wallet addresses identified in Paragraph 1, including Defendants John Doe Nos. 1–25; and

b. Provide counsel for Plaintiff with a copy of such notice.

3. Grounds for Relief

This application for provisional relief, as set forth in the [Proposed] Temporary Restraining Order, is made on the grounds that the conduct sought to be restrained, if allowed to occur, will cause immediate and irreparable injury to Plaintiff because the cryptocurrency assets identified above can be transferred within seconds and dissipated beyond the reach of this Court.

4. Order to Show Cause

Plaintiff requests that the Court issue an Order to Show Cause ("OSC") pursuant to California Rule of Court 3.1150, affording Defendants the opportunity to appear and show cause why a Preliminary Injunction should not issue restraining and enjoining the Enjoined Parties in the same manner for the remainder of this litigation.

///

///

5. Basis for Application

This Application is made pursuant to California Code of Civil Procedure §§ 413.30, 527, and 529. The Application is based upon the attached Memorandum of Points and Authorities, the supporting declarations filed herewith, including the Declarations of Brian Samuels, Maya Vick, and Dimitri Nichols, the Verified Complaint filed in this action, and upon such further evidence and argument as may be presented prior to or at the hearing on this Application.

6. Expedited Discovery

Plaintiff further requests the Court allow him to serve expedited discovery on the non-party cryptocurrency exchanges Binance, OKX, Gate.io, Kraken, and KuCoin for the limited purpose of identifying the account holders associated with the wallet addresses listed in Paragraph No. 1 and tracing the movement of the misappropriated cryptocurrency. Plaintiff seeks records sufficient to identify the account holders, including customer identification and know-your-customer ("KYC") documentation, associated accounts or wallet addresses controlled by the same user, transaction records reflecting transfers to or from the identified wallets, and related account access information such as IP logs and login history. Expedited discovery is necessary to identify Defendants and trace the stolen assets before they can be further transferred or dissipated.

7. Bond

Plaintiff respectfully requests that no bond be required, or that a nominal bond be set, because the requested TRO merely preserves the status quo and imposes no cognizable harm on Defendants. Code Civ. Proc. §§ 529, 995.240, 995.710.

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
(414) 383-1501 | Fax (424) 383-1504
Email: californiaservice@gorilaw.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This action arises from a cryptocurrency investment fraud commonly known as a "pig butchering" [1] scheme, in which fraudsters cultivate victims' trust and persuade them to invest increasing sums of money into what appear to be legitimate cryptocurrency trading platforms. The perpetrators fabricate account balances and trading profits to create the illusion of successful investment activity. Once the victim has transferred substantial assets, the perpetrators refuse withdrawal requests, impose fabricated payment demands, and ultimately disappear with the victim's funds.

That is precisely what occurred here. Through a series of fraudulent misrepresentations and a fictitious online trading platform, Defendants induced Plaintiff to transfer nearly $4.9 million in cryptocurrency to blockchain wallet addresses controlled by Defendants. No legitimate trading occurred. Instead, Plaintiff's cryptocurrency was misappropriated and routed through a network of blockchain wallets used to receive and move the stolen assets. Through the efforts of Plaintiff, his counsel, and forensic blockchain investigators, Plaintiff has identified specific wallet addresses and exchange-hosted accounts through which the stolen assets were transferred and which presently hold proceeds of Defendants' scheme.

Immediate relief is necessary. Cryptocurrency can be transferred across blockchain networks within seconds and moved beyond the reach of victims and courts almost instantly. Unless restrained, Defendants can rapidly dissipate or conceal the remaining traceable assets. Forensic blockchain tracing has already identified wallet addresses and exchange-hosted accounts presently holding traceable proceeds of Defendants' scheme. (Vick Decl. ¶¶ 11-12, 39, 40-42.) Without prompt intervention by this Court, those assets may be permanently lost.

//

//

//

[1] See U.S. Dep't of the Treasury, Financial Crimes Enforcement Network (FinCEN), *Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* (Sept. 8, 2023), available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Pig%20Butchering%20FINAL%20508c.pdf

II. STATEMENT OF FACTS

A. Defendants' Cryptocurrency Fraud Scheme

Plaintiff Brian Samuels is a senior citizen who resides in El Macero, California. He is competent to testify to the facts set forth herein and submits his declaration based on personal knowledge. (Samuels Decl. ¶¶ 1–2.)

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. (Samuels Decl. ¶ 3.)

At all relevant times, Plaintiff lawfully owned digital assets maintained in custodial cryptocurrency accounts at Coinbase, Inc. Those assets constituted identifiable digital property recorded on public blockchain ledgers and were subject to Plaintiff's exclusive ownership and right to immediate possession. (Samuels Decl. ¶¶ 4–5.)

In or about November 2024, Plaintiff was contacted by an individual falsely claiming to be a former colleague identified as "Dan Vivoli." This individual represented that he was an experienced cryptocurrency investor and invited Plaintiff to participate in what was described as a "foolproof" cryptocurrency investment opportunity capable of generating substantial profits. (Samuels Decl. ¶ 6.)

Through subsequent communications, Defendants directed Plaintiff to invest cryptocurrency through a website operating under the domain **Okdaxuda.com**, which Defendants represented to be a legitimate cryptocurrency trading platform utilizing automated trading strategies designed to generate profits. (Samuels Decl. ¶¶ 7–8.)

Plaintiff later learned that the Okdaxuda.com platform was a fraudulent website designed to misappropriate cryptocurrency deposits from victims. (Samuels Decl. ¶ 9.)

The platform appeared highly legitimate and displayed account balances and purported trading profits that reinforced the appearance of profitable trading activity. Plaintiff later learned that the balances, trading activity, and transaction confirmations displayed on the platform were fabricated and controlled entirely by the operators of the website rather than reflecting genuine cryptocurrency trading activity recorded on the blockchain. (Samuels Decl. ¶ 10.)

B. Plaintiff's Cryptocurrency Transfers

Relying on Defendants' representations, Plaintiff transferred U.S. dollars from his brokerage account at Charles Schwab to a Coinbase cryptocurrency account that Defendants instructed him to establish. Plaintiff then converted those funds into USDC cryptocurrency and transferred the digital assets to wallet addresses associated with the Okdaxuda.com platform. (Samuels Decl. ¶ 11.)

Over the course of several months, Defendants induced Plaintiff to transfer increasingly larger amounts of cryptocurrency. In total, Plaintiff transferred approximately **$4,868,861.23** in cryptocurrency through multiple transactions to wallet addresses designated by Defendants. Plaintiff made these transfers in reliance on Defendants' representations that the platform was legitimate and that the deposits were being used for cryptocurrency trading. (Samuels Decl. ¶ 12.)

The Okdaxuda.com interface displayed account balances and purported trading gains that appeared to show profitable trading activity and reinforced Plaintiff's belief that the platform was legitimate. A screenshot reflecting the account balance displayed on the platform is attached as Exhibit A to the Declaration. (Samuels Decl. ¶ 13.)

C. Defendants' Fraudulent Withdrawal Demands

In February 2025, Plaintiff attempted to withdraw his principal and the purported trading profits displayed on the Okdaxuda.com platform. The withdrawal request was immediately denied. (Samuels Decl. ¶ 14.)

Instead, representatives of the platform informed Plaintiff that he was required to pay approximately $811,490 USDT in taxes to international tax authorities before his withdrawal could be processed. A screenshot of this communication is attached as Exhibit B to the Declaration. (Samuels Decl. ¶ 15.)

Believing that this payment was necessary to withdraw his funds, Plaintiff transferred cryptocurrency from his Coinbase account in two transactions totaling approximately $606,743.00 to the wallet address designated by Defendants to satisfy the purported tax obligation. Confirmation of these payments is attached as Exhibit C to the Declaration. (Samuels Decl. ¶ 16.)

Defendants subsequently presented a purported transaction confirmation referencing a blockchain transaction hash in order to falsely suggest that Plaintiff had transferred funds from an unauthorized or suspicious source. This representation was used as a pretext to freeze Plaintiff's account and demand additional payments. A screenshot of this communication is attached as Exhibit D to the Declaration. (Samuels Decl. ¶ 17.)

After Plaintiff made these payments, he again attempted to withdraw his principal and purported profits. Representatives of Okdaxuda.com refused the withdrawal and informed Plaintiff that his account had been frozen pending review by the platform's "risk control department." Defendants demanded an additional $800,000 "risk deposit" in order to release his funds and threatened Plaintiff with prosecution for suspected money laundering if the payment was not made. A screenshot of this communication is attached as Exhibit E to the Declaration. (Samuels Decl. ¶ 18.)

Relying on these representations and threats, Plaintiff transferred $150,000 USDC to Okdaxuda.com and requested a thirty-day extension to pay the remaining balance of the amount demanded. A screenshot reflecting this demand is attached as Exhibit F to the Declaration. (Samuels Decl. ¶ 19.)

Plaintiff subsequently received another message stating that he had until March 30, 2025 to pay the remaining $700,000 risk deposit or his account would be permanently frozen and he would be prosecuted. The message further threatened that his account would incur an additional $5,000 daily fine if the alleged risk margin was not paid by the due date. A screenshot of this communication is attached as Exhibit G to the Declaration. (Samuels Decl. ¶ 20.)

On March 18, 2025, Plaintiff complied with Defendants' demand and transferred an additional $800,000 USDC, valued at approximately $799,000 U.S. dollars, to the wallet address designated by Defendants. A screenshot confirming this transaction is attached as Exhibit H to the Declaration. (Samuels Decl. ¶ 21.)

Despite receiving this payment, Defendants again froze Plaintiff's account and claimed that his withdrawal application had been rejected by a "blockchain node." Defendants then demanded an additional $850,000 payment described as "risk money" allegedly required to verify

account security for large withdrawals. A screenshot of this communication is attached as Exhibit I to the Declaration. (Samuels Decl. ¶ 22.)

After this demand, Plaintiff informed Okdaxuda.com representatives that he was unable and unwilling to transfer any additional funds. By that time, Plaintiff had exhausted all of his available resources and remained unable to withdraw the assets displayed in his account. (Samuels Decl. ¶ 23.)

D. Plaintiff's Efforts to Recover His Cryptocurrency

After realizing that the platform was fraudulent, Plaintiff immediately undertook efforts to recover his misappropriated cryptocurrency. Plaintiff filed a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), contacted the United States Secret Service, and retained cryptocurrency tracing firms ZeroShadow and Outrider Analytics to investigate the transactions. Despite months of effort, those firms advised Plaintiff that recovery through those channels was not possible. (Samuels Decl. ¶ 24.)

Plaintiff thereafter retained Inca Digital, a cryptocurrency investigation firm, which conducted a forensic blockchain analysis of his transactions. Inca advised Plaintiff that Defendants operated a common cryptocurrency fraud scheme known as "pig butchering" and traced Plaintiff's stolen cryptocurrency to specific wallet addresses associated with that scheme. Inca further determined that numerous similarly situated victims transferred cryptocurrency to the same or related wallet addresses as part of the same standardized operation. (Samuels Decl. ¶ 25.)

At all relevant times, Plaintiff retained the lawful right to immediate possession of the transferred cryptocurrency. The assets remain specifically identifiable on public blockchain ledgers and traceable to recipient wallet addresses controlled, directly or indirectly, by Defendants. (Samuels Decl. ¶ 26.)

Defendants exercised and continue to exercise unauthorized dominion and control over Plaintiff's digital assets and have converted those assets to their own use. (Samuels Decl. ¶ 27.)

Unless the cryptocurrency transferred to Defendants is promptly frozen and preserved, Plaintiff will suffer irreparable harm because cryptocurrency can be transferred instantly across

blockchain networks and rapidly dissipated beyond the reach of law enforcement or the courts. (Samuels Decl. ¶ 28.)

Cryptocurrency can be moved through multiple intermediary wallet addresses, exchanges, or cross-chain bridges within seconds, quickly obscuring the trail of stolen assets. Investigators who reviewed Plaintiff's transactions advised that if the cryptocurrency associated with this fraud is not promptly frozen, Defendants could rapidly dissipate the assets beyond the reach of victims, law enforcement, or the Court. (Samuels Decl. ¶ 29.)

Because the stolen cryptocurrency remains traceable to identifiable wallet addresses, prompt action by the Court directing cryptocurrency exchanges or custodians to freeze assets associated with those wallets is necessary to preserve the possibility of recovery. Without immediate injunctive relief, the assets may be permanently transferred or concealed beyond the jurisdiction of this Court. (Samuels Decl. ¶ 30.)

As a result of Defendants' conduct, Plaintiff lost his entire life savings and nearly lost his home. The financial harm caused by Defendants' actions has been devastating and has severely impacted Plaintiff's financial stability. (Samuels Decl. ¶ 31.)

E. Blockchain Tracing of Plaintiff's Cryptocurrency

Forensic blockchain analysis conducted by cryptocurrency investigation firm Inca Digital traced the movement of Plaintiff's stolen cryptocurrency across blockchain networks and identified the wallet infrastructure used by Defendants to receive and launder those assets. (Vick Decl. ¶¶ 1–4.)

Based on her education, training, and experience investigating cryptocurrency fraud schemes, Inca Digital investigator Maya Vick determined that the conduct described in the Verified Complaint is consistent with a transnational cryptocurrency investment fraud scheme commonly referred to as a "pig butchering" scheme. In such schemes, perpetrators induce victims to transfer cryptocurrency to fraudulent investment platforms controlled by the perpetrators and then impose fabricated withdrawal conditions—such as taxes, margin deposits, or other fees—in order to extract additional payments while preventing victims from recovering their assets. (Vick Decl. ¶¶ 5–9.)

Using forensic blockchain tracing tools, investigators analyzed blockchain transaction data associated with Plaintiff's cryptocurrency transfers in order to identify the wallet addresses that received Plaintiff's assets, trace the subsequent movement of those assets through intermediary wallets, and determine whether the assets were ultimately deposited into custodial cryptocurrency exchanges. (Vick Decl. ¶ 10.)

The forensic analysis confirmed that between **December 27, 2024 and March 18, 2025**, Plaintiff transferred cryptocurrency valued at approximately **$4,868,861.13** as part of the fraudulent scheme. Of those transfers, approximately **$4,149,761.13** has been successfully traced through identifiable blockchain transactions. (Vick Decl. ¶ 11.)

The traced funds were first directed to a scam-controlled intake wallet provided by the perpetrators, which served as the initial collection point for Plaintiff's cryptocurrency. (Vick Decl. ¶¶ 11, 13-14.)

From that intake wallet, the perpetrators systematically routed the stolen cryptocurrency through numerous intermediary wallet addresses and pivot wallets, splitting and recombining transactions in a manner designed to obscure the origin and ownership of the assets and hinder asset recovery. (Vick Decl. ¶¶ 16–18.)

Despite these laundering efforts, forensic tracing successfully followed substantial portions of Plaintiff's cryptocurrency through intermediary wallets and determined that the assets were ultimately deposited into exchange-hosted deposit wallets associated with centralized cryptocurrency exchanges. (Vick Decl. ¶¶ 12, 15, 39.)

Specifically, the traced cryptocurrency was deposited into exchange-hosted deposit wallets associated with cryptocurrency exchanges including **Binance, OKX, Gate.io, Kraken, KuCoin, Bybit, and Bitget.** (Vick Decl. ¶¶ 15, 34, 39.)

Exchange-hosted deposit wallets are custodial addresses controlled by the exchange operators. Cryptocurrency deposited into such wallets is held within accounts maintained by those exchanges, which possess the technical ability to restrict transfers or freeze assets associated with those accounts when directed by court order. (Vick Decl. ¶¶ 10, 40, 43.)

Based on the forensic tracing analysis conducted in this matter, the **wallet addresses identified in Paragraph 1 and Appendix A of Plaintiff's Proposed Temporary Restraining Order represent the last known locations where Plaintiff's misappropriated cryptocurrency has been traced on the blockchain.** (Vick Decl. ¶¶ 12, 15, 39, 40.)

The forensic analysis further confirms that the wallet infrastructure used in this case—including shared intake wallets, pivot wallets, and exchange-hosted deposit wallets—is consistent with a coordinated cryptocurrency fraud operation affecting multiple victims whose funds were aggregated and routed through the same laundering pathways. (Vick Decl. ¶¶ 30–33, 41.)

Ms. Vick concludes that Plaintiff's cryptocurrency was transferred from his Coinbase account to the perpetrators' intake wallet, routed through intermediary and pivot wallets designed to obscure the transaction trail, and ultimately deposited into exchange-hosted deposit wallets associated with accounts controlled by or accessible to Defendants. (Vick Decl. ¶ 40.)

Ms. Vick further concludes that, absent immediate injunctive relief, the remaining misappropriated cryptocurrency is at substantial risk of being transferred, concealed, or dissipated in a manner that would render recovery impracticable or impossible. (Vick Decl. ¶ 42.)

Because cryptocurrency transactions can be executed within seconds and assets can be moved across blockchain networks and exchanges with minimal delay, the assets identified through forensic tracing remain at imminent risk of further dissipation unless the exchanges hosting the identified deposit wallets are promptly directed to freeze those assets. Immediate injunctive relief directing the relevant cryptocurrency exchanges to freeze the identified wallets is therefore necessary to preserve the possibility of recovery and prevent further laundering or dissipation of Plaintiff's stolen assets.

F. Exchanges Possess the Ability to Freeze Identified Assets

Cryptocurrency exchanges maintain custody and control over deposit wallets associated with user accounts maintained on their platforms. Based on her experience investigating cryptocurrency exchanges and digital asset platforms, Ms. Vick explains that centralized exchanges—including Binance, OKX, Kraken, KuCoin, Gate.io, and similar platforms—possess

the technical ability to freeze or restrict withdrawals from accounts associated with deposit wallet addresses when directed by court order. (Vick Decl. ¶ 43.)

The forensic blockchain tracing conducted in this matter confirms that substantial portions of Plaintiff's misappropriated cryptocurrency were ultimately deposited into exchange-hosted wallets associated with centralized cryptocurrency exchanges. (Vick Decl. ¶¶ 12, 15, 34, 39, 40.)

The wallet addresses identified in **Paragraph 1 and Appendix A of Plaintiff's Proposed Temporary Restraining Order** represent the last known locations where Plaintiff's stolen cryptocurrency has been traced through blockchain analysis. (Vick Decl. ¶¶ 12, 15, 39, 40.)

Because the identified wallets are hosted by custodial cryptocurrency exchanges that control the associated user accounts, those exchanges possess the ability to freeze the assets associated with those wallets and prevent further transfers or withdrawals.

Accordingly, a temporary restraining order directing the exchanges identified in **Appendix A** to freeze assets associated with the identified wallet addresses will preserve the status quo and prevent further dissipation of Plaintiff's stolen cryptocurrency.

Absent immediate court intervention directing the exchanges to freeze these assets, Defendants can transfer the cryptocurrency through additional intermediary wallets or exchanges within seconds, placing the assets beyond the reach of the Court and effectively preventing recovery.

III. LEGAL STANDARD

California Code of Civil Procedure § 527 permits the issuance of preliminary injunctions and temporary restraining orders. Section 527(b) expressly provides:

> A temporary restraining order, or preliminary injunction, or both, may be granted in a class action, in which one or more parties sues or defends for the benefit of numerous parties upon the same grounds as in other actions, whether or not the class has been certified.

Code Civ. Proc. § 527(b).

When ruling on a request for a temporary restraining order and/or a preliminary injunction, courts evaluate two factors: "(1) the likelihood that the plaintiff will prevail on the merits at trial and (2) the interim harm that the plaintiff would be likely to sustain if the injunction were denied as compared to the harm the defendant would likely suffer if the preliminary injunction were

issued." *Smith v. Adventist Health System/West* (2010) 182 Cal.App.4th 729, 749. These two factors are interrelated, and "the greater plaintiff's showing on one, the less must be shown on the other to support an injunction." *Butt v. State of California* (1992) 4 Cal.4th 668, 678.

In deciding whether to issue provisional relief, a court must exercise its discretion "in favor of the party most likely to be injured." *Robbins v. Superior Court (County of Sacramento)* (1985) 38 Cal.3d 199, 205. If denial of an injunction would result in great harm to the plaintiff and the defendants would suffer little harm if it were granted, it is an abuse of discretion to deny relief. *Id.*

Temporary restraining orders are issued to preserve the status quo pending a hearing on a preliminary injunction and terminate automatically once the preliminary injunction request is heard. *Lenard v. Edmonds* (1957) 151 Cal.App.2d 764, 769-770; Code Civ. Proc. § 527(d). The issuance of a TRO requires evidence from the moving party, but a verified complaint may itself be sufficient to support provisional relief. *Bank of America National Trust & Savings Assn v. Williams* (1948) 89 Cal.App.2d 21, 23; Code Civ. Proc. § 527(a).

IV. ARGUMENT

A. This Court Should Grant a Temporary Restraining Order Without Notice and Order Defendants to Show Cause Why a Preliminary Injunction Should Not Issue.

1. TRO without notice is appropriate.

The verified complaint and supporting declarations establish that notice should not be required prior to the issuance of a temporary restraining order. Code Civ. Proc. § 527(c) expressly authorizes issuance of TROs without notice.

If Plaintiff were required to provide advance notice, Defendants could immediately transfer the cryptocurrency at issue beyond the reach of discovery or recovery. Cryptocurrency transactions can occur within seconds and may be transferred across blockchain networks to anonymous recipients, creating a substantial risk of rapid dissipation. (Vick Decl. ¶ 42.)

Providing notice under these circumstances would undermine the very purpose of provisional relief—preserving the status quo pending determination of the merits. *Lenard v. Edmonds* (1957) 151 Cal.App.2d 764, 769-770.

Courts have routinely granted temporary restraining orders without notice in cryptocurrency fraud schemes because cryptocurrency "poses a heightened risk of asset dissipation." *Jacobo v. Doe*, 2022 U.S. Dist. LEXIS 101504, *9 (E.D. Cal. June 7, 2022); accord *Heissenberg v. Doe*, 2021 U.S. Dist. LEXIS 257218, at *7-9 (S.D. Fla. Apr. 22, 2021); accord *Bullock v. Doe*, 2023 U.S. Dist. LEXIS 234778 at *20-23 (N.D. Iowa Nov. 3, 2023).

As the court observed in *Jacobo*, providing notice would allow a defendant to transfer cryptocurrency "to unidentified recipients outside the traditional banking system… and effectively put it beyond the reach of this court." *Id.* at *9. Courts therefore routinely grant ex parte relief in cryptocurrency theft cases because such assets may rapidly become lost and untraceable. *Gaponyuk v. Alferov*, 2023 U.S. Dist. LEXIS 125262, at *4-10 (E.D. Cal. July 20, 2023).

For these reasons, issuance of a temporary restraining order without notice is necessary to preserve the status quo.

2. Plaintiff is likely to succeed on the merits.

Plaintiff is likely to prevail on the merits of his claims. To establish likelihood of success, a party need only demonstrate that it is "reasonably probable that the moving party will prevail on the merits." *San Francisco Newspaper Printing Co. v. Superior Court (Miller)* (1985) 170 Cal.App.3d 438, 442.

To establish conversion, Plaintiff must show (1) ownership or a right to possession of the property, (2) wrongful interference with that property without consent, and (3) resulting damages. *Lee v. Hanley* (2015) 61 Cal.4th 1225, 1240; CACI No. 2100 (2024). A claim for money had and received requires proof that defendant received money intended for Plaintiff's benefit and failed to return it. *Mains v. City Title Ins. Co.* (1949) 34 Cal.2d 580, 586; CACI No. 370 (2024).

Although money ordinarily cannot be the subject of conversion, an exception exists where the funds are specific and identifiable. *Haigler v. Donnelly* (1941) 18 Cal.2d 674, 681. Courts likewise recognize that conversion may apply to intangible or electronic property interests capable of precise identification. *Welco Electronics, Inc. v. Mora* (2014) 223 Cal.App.4th 202, 208–209. Because blockchain ledgers record cryptocurrency transfers and allow those transfers to be traced to specific wallet addresses, the assets at issue constitute specific and identifiable property capable

of supporting a conversion claim. Here, forensic blockchain tracing identified the wallet addresses through which Plaintiff's cryptocurrency was transferred and the exchange-hosted wallets where those assets were ultimately deposited. (Vick Decl. ¶¶ 11–12, 39, 40.)

The Samuels Declaration and the Verified Complaint establish each of these elements. Plaintiff owned and controlled approximately $4,868,861.23 in cryptocurrency prior to transferring it in reliance on Defendants' fraudulent representations regarding a purported investment platform, Okdaxuda.com. (Samuels Decl. ¶¶11–12.) Defendants induced Plaintiff to transfer those assets to wallets under Defendants' control and thereafter diverted and transferred the cryptocurrency through blockchain transactions without Plaintiff's consent. (Samuels Decl. ¶¶ 11–12; Vick Decl. ¶¶ 11, 16–18.)

Blockchain tracing confirms that the assets were routed through a series of transactions designed to conceal their origin and current ownership. (Samuels Decl. ¶¶ 11–12; Vick Decl. ¶¶ 11, 16–18.) These acts constitute wrongful interference with Plaintiff's property and deprived him of possession of his cryptocurrency. Plaintiff has demanded the return of the funds, but Defendants have refused to return them and continue to maintain control over the assets. (Samuels Decl. ¶¶ 14–23.)

Cryptocurrency constitutes specific and identifiable property that can be traced through blockchain ledgers. Forensic blockchain tracing has identified at least $4,149,761.13 of Plaintiff's cryptocurrency moving through identifiable blockchain addresses and into exchange-hosted wallets associated with exchanges including Binance, OKX, Gate.io, Kraken, and KuCoin. (Vick Decl. ¶¶ 11–12, 15, 39.)

Because Plaintiff's cryptocurrency can be traced through blockchain analysis to specific wallet addresses now holding the assets, the funds constitute identifiable property subject to conversion and are properly treated as property held in constructive trust for Plaintiff. *See Heckmann v. Ahmanson* (1985) 168 Cal.App.3d 119, 135 (constructive trust appropriate where defendant wrongfully acquires property belonging to another).

Courts have recognized that cryptocurrency assets are specific and identifiable property capable of supporting a claim for conversion. As one court explained, "[t]he cryptocurrency assets

at issue are specific, identifiable property and can be traced in JOHN DOE's assets in the Destination Addresses or elsewhere." *Astrove v. Doe*, 2022 U.S. Dist. LEXIS 129286, at *6–7 (S.D. Fla. Apr. 22, 2022); accord *Blum v. Defendant*, 2023 U.S. Dist. LEXIS 235592, at *4–5 (N.D. Fla. Dec. 13, 2023).

For these reasons, Plaintiff has demonstrated a strong likelihood of success on the merits.

3. Irreparable harm will occur absent relief.

Courts repeatedly recognize that cryptocurrency theft schemes present a substantial risk of irreparable harm absent injunctive relief. "[C]ourts have found that the risk of irreparable harm to be likely in matters concerning fraudulent transfers of cryptocurrency due to the risk of anonymous and speedy asset dissipation." *Jacobo*, supra at *15–16, citing *Heissenberg v. Doe*, 2021 U.S. Dist. LEXIS 257218, at *2.

Cryptocurrency may be transferred instantly to anonymous recipients outside the traditional banking system, placing assets beyond the reach of courts and law enforcement. *Jacobo*, supra.

Courts have recognized that when stolen cryptocurrency can be traced to identifiable wallet addresses or exchange-hosted accounts, immediate injunctive relief is often the only effective means of preserving the property pending adjudication of the parties' rights. Because blockchain transactions occur rapidly and irreversibly, delay in issuing provisional relief can allow stolen assets to be transferred through additional intermediary wallets, exchanges, or cross-chain bridges, making recovery significantly more difficult or impossible. Here, forensic tracing has already identified wallet addresses associated with Defendants' scheme and exchange-hosted accounts capable of being frozen through court order. (Vick Decl. ¶¶ 40–42.) Immediate relief will therefore preserve traceable assets while imposing only a temporary restriction on transfers until the Court can conduct a hearing on Plaintiff's request for a preliminary injunction.

Courts have also held that money damages alone are often inadequate in cryptocurrency fraud cases because perpetrators are frequently anonymous and assets can quickly become untraceable. As the court explained in *Bullock v. Doe*, "defendants will likely convert the crypto to a place where plaintiff can no longer find it or find defendants themselves." *Bullock*, 2023 U.S.

Dist. LEXIS 234778 *16. Thus, "a money damages judgment would be essentially meaningless." *Id.*

The same risk exists here. Defendants' identities are unknown, and Plaintiff's cryptocurrency remains vulnerable to immediate transfer or liquidation. (Vick Decl. ¶¶ 40–42.) Absent injunctive relief, Defendants can readily move the assets beyond the reach of discovery and this Court.

The relief sought here is narrowly tailored to preserve the status quo pending a hearing on Plaintiff's request for a preliminary injunction. Plaintiff does not seek the transfer or seizure of any assets at this stage. Rather, Plaintiff seeks only a temporary restraint preventing the further movement of cryptocurrency that forensic blockchain tracing has identified as traceable to Plaintiff's transfers and currently located in identifiable wallet addresses associated with cryptocurrency exchanges. Absent such relief, Defendants can transfer the assets in seconds to anonymous blockchain addresses beyond the reach of this Court, effectively defeating any judgment that may ultimately be entered in this action. (Vick Decl. ¶¶ 11–12, 40–42.)

Accordingly, Plaintiff will suffer irreparable harm unless the requested temporary restraining order is issued.

B. Balance of harms favors Plaintiff.

The TRO sought by Plaintiff is temporary and will remain in effect only until the preliminary injunction hearing, which must occur within 15 days, or within 22 days for good cause shown, pursuant to Code of Civil Procedure § 527(d).

Even if Defendants claimed a legal interest in the cryptocurrency, the requested asset freeze would impose only a temporary restriction on transferring those assets. In contrast, denial of injunctive relief would permit Defendants to dissipate the stolen cryptocurrency, leaving Plaintiff without any remedy.

As the court held in *Jacobo*, balancing the harms favors the victim of cryptocurrency theft: "A delay in defendant's ability to transfer the assets only minimally prejudices defendant, whereas

withholding injunctive relief would severely prejudice plaintiff by providing defendant time to transfer the allegedly purloined assets into other accounts beyond the reach of this court." *Jacobo*, 2022 U.S. Dist. LEXIS 101504 at *17.

C. Public interest favors relief.

The provisional relief sought here also serves the public interest. As the court explained in *Jacobo*, "the public interest is properly served by promoting the objectives of … FinCEN and providing assurance to the public that courts will take action to promote protection of assets and recovery of stolen assets when they can be readily located and traced to specific locations." *Jacobo*, supra at *18, quoting *Heissenberg*, supra. at *2.

Courts have similarly recognized that freezing cryptocurrency accounts promotes confidence that fraud and theft can be addressed within the cryptocurrency marketplace. *Blum*, 2023 U.S. Dist. LEXIS 235592 at *5, quoting *Hikmatullaev v. Marco Alessandro Villa*, 2023 U.S. Dist. LEXIS 111619, at *8. Freezing the wallet addresses identified through forensic tracing serves the public interest by preserving assets pending adjudication of Plaintiff's claims.

D. No Bond Should Be Required.

Posting of a bond is ordinarily not required for issuance of a TRO that lasts only until the preliminary injunction hearing. *Venice Canal Resident HOA v. Superior Court* (1977) 72 Cal.App.3d 675, 681; Code Civ. Proc. § 527. Even at the preliminary injunction stage, courts may require only a minimal undertaking. Code Civ. Proc. §§ 529, 995.710, 995.240.

Courts in cryptocurrency theft cases frequently set the bond at zero where there is no evidence the restrained party will suffer damages from the injunction. *Gaponyuk v. Alferov*, 2023 U.S. Dist. LEXIS 125262, at *8; accord *Jacobo*, supra at *18.

Because the requested relief merely freezes cryptocurrency that was wrongfully obtained from Plaintiff, Defendants will suffer no cognizable harm from the temporary restraint.

E. Service by Blockchain Notice Is Reasonably Calculated to Provide Actual Notice

California law authorizes service of process "in a manner which is reasonably calculated to give actual notice" where traditional service methods are impracticable. Code Civ. Proc. § 413.30.

Courts regularly authorize alternative service where defendants intentionally conceal their identities or cannot be located despite diligent investigation.

Here, Defendants' identities and locations remain unknown despite substantial investigation by Plaintiff and his counsel. Defendants operated the fraudulent cryptocurrency scheme using fictitious identities and blockchain wallet infrastructure designed to conceal their identities and locations. As a result, Plaintiff cannot effectuate service through conventional means such as personal service, service by mail, or service on known counsel. (Nichols Decl. ¶¶ 3–4.)

Courts addressing cryptocurrency theft schemes have recognized that perpetrators frequently operate anonymously through blockchain wallet infrastructure and intentionally conceal their identities. In such circumstances, courts have authorized alternative service methods designed to provide notice through the digital infrastructure used to perpetrate the fraud. See, e.g., *Jacobo v. Doe,* 2022 U.S. Dist. LEXIS 101504, at *9 (E.D. Cal. June 7, 2022) (authorizing seizure of cryptocurrency assets and permitting notice to defendants through blockchain notification); *Younes v. Taylor,* Case No. 24STCV12520 (Los Angeles Sup. Ct. June 27, 2024); *Mann v. Moore*, Case No. 24STCV17012 (Los Angeles Sup. Ct. July 17, 2024). (Nichols Decl. ¶¶ 8–9.)

The service method proposed here is reasonably calculated to provide actual notice to Defendants. Plaintiff proposes to deliver an electronic "token" or similar blockchain notification directly into each of the wallet addresses identified in **Paragraph 1 above and Appendix** A of the proposed Order. Each notification token will contain a hyperlink to a website maintained by Plaintiff's counsel where Defendants may access this Order and all papers upon which it is based. The hyperlink will include a mechanism that records when the link is accessed.

Because the individuals controlling these wallets must necessarily retain access to the private keys controlling those wallets in order to transfer or dissipate the cryptocurrency assets, delivery of the notification token to those wallets provides a direct mechanism to notify the persons controlling the assets.

Providing advance notice through conventional means would also defeat the purpose of the requested relief. Cryptocurrency can be transferred across blockchain networks within seconds, and perpetrators of cryptocurrency fraud commonly move stolen assets immediately when alerted

to enforcement action. (Nichols Decl. ¶ 6.) If Defendants were notified before the wallets were frozen, they could rapidly transfer the assets to additional wallets or offshore exchanges and render recovery impossible.

Absent *ex parte* relief and alternative service through the identified wallets, Defendants could transfer the assets through additional intermediary wallets or exchanges before a noticed motion could be heard. (Nichols Decl. ¶ 7.)

Accordingly, the proposed method of service: delivery of a blockchain notification token containing a hyperlink to the relevant filings, is reasonably calculated to provide actual notice to Defendants and is authorized under Code Civ. Proc. § 413.30.

F. Exchanges Should Be Directed to Provide Notice to Associated Account Holders

The forensic blockchain tracing conducted in this matter confirms that substantial portions of Plaintiff's stolen cryptocurrency were ultimately deposited into exchange-hosted deposit wallets associated with centralized cryptocurrency exchanges including **Binance, OKX, Gate.io, Kraken, and KuCoin**. (Vick Decl. ¶¶ 12, 15, 34, 40.)

Cryptocurrency exchanges maintain custodial control over deposit wallets associated with user accounts maintained on their platforms and possess the technical ability to freeze or restrict withdrawals from those accounts when directed by court order. (Vick Decl. ¶ 43.)

Based on the forensic tracing analysis conducted in this matter, the wallet addresses identified in **Paragraph 1 above and Appendix A** of Plaintiff's Proposed Temporary Restraining Order represent the last known locations where Plaintiff's misappropriated cryptocurrency has been traced on the blockchain. (Vick Decl. ¶¶ 12, 15, 40.)

Because these exchanges maintain custody of the accounts associated with those deposit wallets, they are uniquely positioned to provide notice to the account holders associated with those wallets. Accordingly, Plaintiff respectfully requests that the Court direct the identified exchanges,

upon receiving notice of this Order, to provide notice of the proposed Order to any customer accounts associated with the wallet addresses identified in Appendix A of the Order and to provide confirmation of such notice to Plaintiff's counsel.

This additional notice mechanism further ensures that Defendants receive actual notice of this action and of the Court's Order while preserving the Court's ability to prevent further dissipation of Plaintiff's stolen cryptocurrency.

V. CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court grant the requested temporary restraining order restraining Defendants and the identified cryptocurrency exchanges from transferring or dissipating the cryptocurrency held in the wallet addresses identified herein and preserving associated account records. The requested relief is narrowly tailored to preserve the status quo and prevent the further movement of traceable assets pending a hearing on Plaintiff's request for a preliminary injunction. Absent immediate relief, Defendants may rapidly transfer or conceal the remaining proceeds of their fraudulent scheme beyond the reach of this Court. Plaintiff therefore respectfully requests that the Court issue the temporary restraining order and set an order to show cause hearing regarding a preliminary injunction.

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
(414) 383-1501 | Fax (424) 383-1504
Email: califonriaservice@gorilaw.com

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

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

Attorneys for Plaintiff
Brian M. Samuels

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF YOLO

BRIAN M. SAMUELS, on behalf of himself and others similarly situated, Plaintiffs, vs. JOHN DOE NOS. 1-25 Defendants.	Case No.: Number **DECLARATION OF MAYA VICK IN SUPPORT OF PLAINTIFF'S EX PARTE APPLICATION FOR TEMPORARY RESTRAINING ORDER AND OSC RE: PRELIMINARY INJUNCTION**

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

I. INTRODUCTION

1. I am over eighteen years of age, of sound mind, and competent to make this declaration. The statements contained herein are based on my personal knowledge, my professional training and experience, and information derived from forensic blockchain analysis conducted by Inca Digital, which is of the type reasonably relied upon by experts in the field of cryptocurrency investigations.

2. I am employed by Inca Digital, a digital asset intelligence company that provides data analytics, blockchain forensic analysis, and investigative support to cryptocurrency exchanges, financial institutions, regulators, and government agencies. Inca Digital conducts investigations into digital asset markets and cryptocurrency-related criminal activity, including fraud, market manipulation, and illicit financial flows. Additional information about Inca Digital and its work is available at https://inca.digital.

3. In my role at Inca Digital, I have conducted numerous investigations involving cryptocurrency fraud schemes, including schemes commonly referred to as "pig-butchering." These investigations typically involve tracing cryptocurrency transactions across blockchain networks in order to identify wallet infrastructure, intermediary routing wallets, and custodial exchange deposit addresses associated with fraudulent activity.

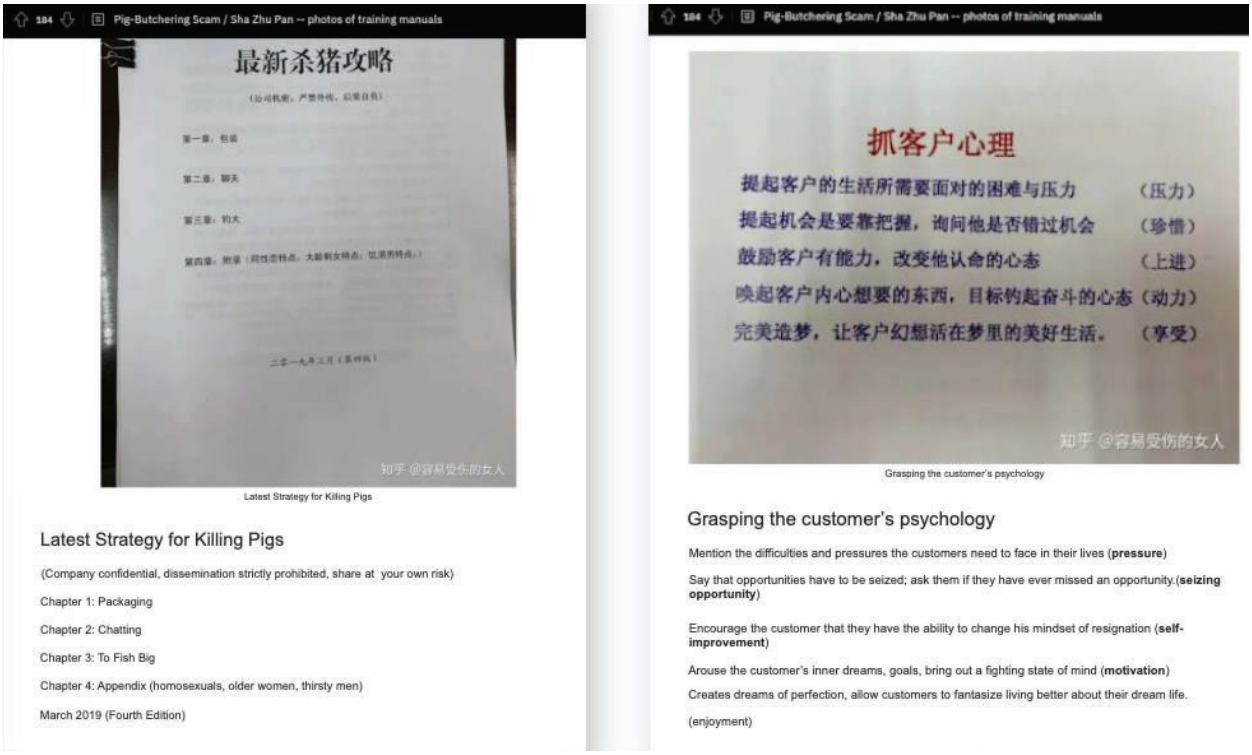
4. In connection with this matter, I have reviewed Plaintiff Brian Samuels' Verified Complaint and supporting materials and am familiar with the facts alleged therein. I have also reviewed blockchain transaction data and conducted forensic blockchain analysis relating to cryptocurrency transfers made by Plaintiff.

5. Based on my education, training, and experience investigating cryptocurrency fraud schemes, the conduct described in the Verified Complaint is consistent with a type of transnational cryptocurrency investment fraud commonly referred to as a "pig-butchering"[1]

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

scheme, sometimes referred to by the Chinese term *Sha Zhu Pan*. In such schemes, perpetrators typically establish fictitious online identities and communicate with victims through messaging platforms or social media in order to gain trust and induce victims to transfer cryptocurrency to fraudulent investment platforms controlled by the perpetrators.

6. Based on my experience investigating these schemes, many pig-butchering operations are conducted by organized transnational groups operating in East and Southeast Asia. Among other evidence, Inca Digital has obtained an operations manual of one such transnational criminal group as displayed below. The manual provides guidance in setting up and operating a pig butchering scheme.



Screenshots from Pig Butchering Operations Manual

7. Fraudulent cryptocurrency trading platforms used in pig-butchering schemes frequently attempt to mimic legitimate exchanges in order to create the appearance of credibility. Based on my experience investigating similar schemes, such platforms often use domain names,

branding, or other design elements that resemble established cryptocurrency exchanges. The website referenced in the Verified Complaint, Okdaxuda.com, appears consistent with this pattern in that it closely resembles the name of the legitimate cryptocurrency exchange OKX.com and was presented to Plaintiff as a trading platform associated with cryptocurrency investment activity.

8. Platforms used in these schemes commonly display fabricated account balances and fictitious trading profits to encourage victims to transfer additional cryptocurrency. Victims may initially be permitted to withdraw small amounts of cryptocurrency in order to increase their confidence in the platform before larger deposits are requested. Once victims have transferred substantial amounts of cryptocurrency, the perpetrators often impose fabricated withdrawal conditions—such as purported taxes, margin payments, or other fees, in order to extract additional funds while preventing any meaningful withdrawal of assets.

9. Based on my experience investigating cryptocurrency exchanges and digital asset platforms, legitimate exchanges do not require customers to pay capital gains taxes, margin payments, or other deposits as a condition of withdrawing funds from their accounts. Such representations are commonly used in fraudulent cryptocurrency investment schemes.

10. I conducted blockchain forensic analysis to trace cryptocurrency transfers associated with Plaintiff's transactions. The purpose of this analysis is to identify the blockchain wallet addresses that received Plaintiff's cryptocurrency, trace the subsequent movement of those assets across intermediary wallets, and determine whether those assets were ultimately deposited into custodial cryptocurrency exchanges where they may remain subject to restraint.

The results of my blockchain tracing analysis are described below.

II. TRACING THE MOVEMENT OF BRIAN SAMUELS' STOLDEN FUNDS

A. Brian Samuels Initial Transactions

11. Between December 27, 2024 and March 18, 2025, Mr. Samuels transferred cryptocurrency with a total value of approximately $4,868,861.13 as part of the fraudulent scheme described in the Verified Complaint. Based on forensic blockchain analysis conducted to date, approximately $4,149,761.13 of those transfers—across 14 identified cryptocurrency transactions—have been traced to one Intake Wallets that represent the first known scam-controlled addresses to which the perpetrators directed the Mr. Samuels to send his assets. The remaining portion of Mr. Samuel's losses reflects transfers that have not yet been fully traced to identifiable downstream wallets through currently available blockchain data, but those transfers are consistent with the same fraudulent scheme described herein.

12. From those wallets, the perpetrators systematically moved funds through a series of additional transactions—sending the funds through a maze of other addresses until they ultimately reached Exchange-Hosted Deposit Wallets.

13. The table below details all transactions where the Victim transferred funds to Intake Wallet addresses provided by the perpetrators, which are listed in the "To Address" column.

Transfer	Date/Time	From Exchange	From Address	To Address	Asset Type	Asset Amount	USD Equivalent
1	Dec 27, 2024 10:40:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	10,000	$10,010
2	Dec 28, 2024 12:03:11 pm	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	89,000	$89,089
3	Jan 04, 2025 11:10:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	200,000	$200,200
4	Jan 04, 2025 11:31:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	DAI	174,908.74543727	$175,083.65

5	Jan 18, 2025 09:57:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	315,000	$315,000
6	Jan 23, 2025 10:37:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	150,000	$150,150
7	Jan 28, 2025 09:33:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	210,000	$210,210
8	Feb 04, 2025 09:26:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	624,000	$623,376
9	Feb 06, 2025 08:45:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	850,000	$850,000
10	Feb 07, 2025 09:24:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	690,000	$690,000
11	Feb 12, 2025 10:04:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	260,000	$260,000
12	Mar 12, 2025 08:31:47 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	346,743.480216	$346,743.48
13	Mar 20, 2025 09:18:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	149,999	$149,999
14	Mar 18, 2025 08:34:11 am	Coinbase	0xA9D1e08C7793af67e9d92fe308d5697FB81d3E43	0x525ccc3e1631657d2bc00ff1684c7109d3d27336	USDC	799,000	$799,000

14. In total, Mr. Samuels sent funds to 1 Intake Wallet:

- **Intake Wallet #1:** 0x525ccc3e1631657d2bc00ff1684c7109d3d27336

15. Funds from the Intake Wallet were ultimately transferred to Exchange Deposit Wallets, hosted at Binance, OKX, Bybit, HTX, Gate.io, MEXC, Bitget, Kraken, FixedFloat, and KuCoin.

B. Flow of Funds Analysis.

Overview

16. Forensic blockchain analysis confirms that the Victim's funds were systematically routed through transaction pathways designed to obscure their origin.

17. Funds were routed through intermediary wallets, including Pivot Wallets, where they were combined, split, and transferred across multiple additional addresses. These structured movements demonstrate an intent to break direct transaction links, disrupt traceability, and hinder asset recovery. The assets were ultimately deposited into the Exchange-Hosted Deposit Wallets, the addresses of which are listed in section "V. Wallets to Freeze" herein.

Role of Pivot Wallets in Fund Movement

18. Bad actors use Pivot Wallets as central points in the laundering process to consolidate stolen funds from multiple victims. By aggregating and redistributing assets, these wallets obscure direct transactional links, making it harder to trace funds from their original sources to final destinations. Forensic blockchain analysis conducted in this case successfully traced the movement of funds through these wallets, revealing a coordinated scheme. Specifically identified Pivot Wallet addresses in this case include:

- **Pivot Wallet #1: TKfQUDkabrT9oQpChyJgKZbYkPsPM3Sv2N**
- **Pivot Wallet #2: TQ7CdS3cXZ6gxwYh2cdEHXgFAPxZEwEXWf**
- **Pivot Wallet #3: TU8EZ3pkpqvKEeAt53kojgreDoEfirVJ3s**
- **Pivot Wallet #4: TGjzAFEaTwDTPSvmwMPQVGtFAbMYdkjRif**
- **Pivot Wallet #5: TVULbjyahj7KyKfdtC4ZwbTeFCtc44E9Sm**
- **Pivot Wallet #6: TDQfJm9yPvQq5fNLK1ikMTPCGmnALRkX6v**

Traced Pathways of Victim Funds

19. Pathways describe how funds move from Victim Wallets to Exchange Deposit Wallets. The analysis in this case identified two pathway types, categorized as Pathway 5 and Pathway 6.

20. Pathway 5 involves the transfer of funds from Pivot Wallets through one or more Intermediary Wallets before reaching Exchange Deposit Wallets without additional intermediary steps. Pathway 6 shows a more complex route in which funds moved from Intake Wallet through one or more Intermediary Wallets before being deposited into a Pivot Wallet, which transferred portions of the funds either directly into an Exchange Hosted Deposit Wallet or through one or more Intermediary Wallets before being deposited into different Exchange Hosted Deposit Wallets.

21. Below is an analysis of Pathway 5.

Pathway 5: Transfer to Intake Wallet to Intermediary Wallets to Pivot Wallet to Additional Intermediary Wallets to Exchange-Hosted Deposit Wallets

• The Victim transferred funds from their personally controlled wallet to an Intake Wallet 0x525ccc3e1631657d2bc00ff1684c7109d3d27336.

• Funds first passed through 4 intermediary wallets and then swapped through Bridge.

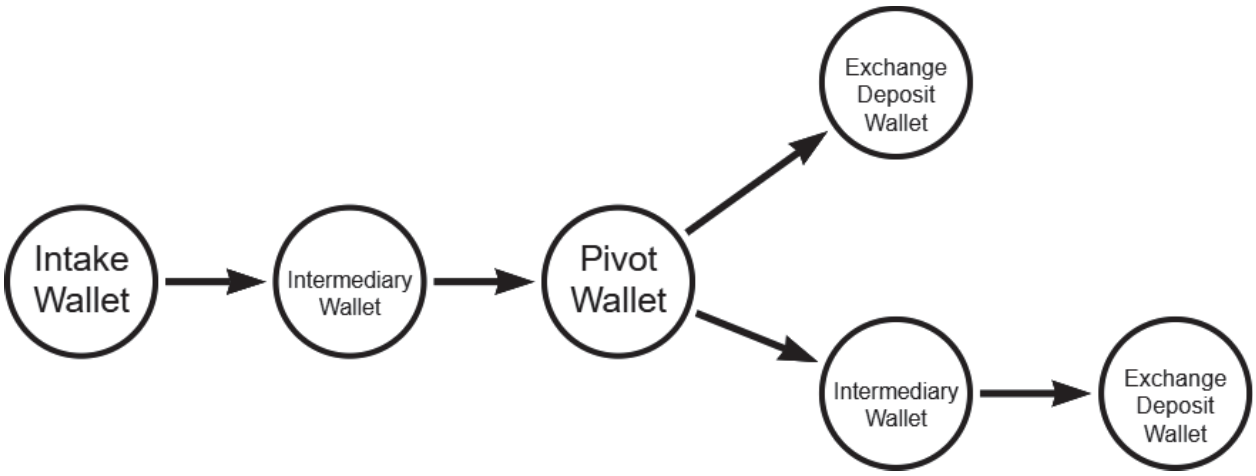
• Then funds passed through 1 intermediary wallet and were then aggregated at **Pivot Wallet [#4]: TGjzAFEaTwDTPSvmwMPQVGtFAbMYdkjRif** and then passed through 9 additional intermediary wallets.

• After layering transactions across multiple wallets, the funds were ultimately deposited into Deposit Wallets at Binance and OKX.

22. Below is an analysis of Pathway 6.

Pathway 6: Transfer to Intake Wallet to Intermediary Wallets to Pivot Wallet to Additional Intermediary Wallets to Exchange-Hosted Deposit Wallets to Additional Intermediary and Deposit Wallets.

• The Victim transferred funds from their personally controlled wallets to Intake Wallet 0x525ccc3e1631657d2bc00ff1684c7109d3d27336. • Funds passed through 4 intermediary wallets and then crypto was swapped through Bridge and after that funds underwent a series of splits and merges. • After layering transactions across the additional intermediary wallet, a portion of the funds were deposited into a Deposit Wallet at Binance. • The remaining funds were layered across 11 more intermediary wallet addresses before being deposited into a Deposit Wallet at OKX. • This movement is illustrated in the Simplified Flow of Funds Graph below.



Currently Unrecoverable or Untraceable Funds

23. The Victim sent 14 transactions to Intake Wallet 0x525ccc3e1631657d2bc00ff1684c7109d3d27336. Some of these funds are still on balance in these perpetrator-controlled wallets and currently unrecoverable. These perpetrator controlled wallets are not on a centralized exchange, and therefore there is no intermediary that can freeze the funds. The Intake Wallet 0x525ccc3e1631657d2bc00ff1684c7109d3d27336 sent some of

victim's funds, to decentralized/unlicensed exchanges (HTX, NoKYC, HitBTC, HiFiSwap). Once transferred there, the funds could not be traced further and may be unrecoverable.

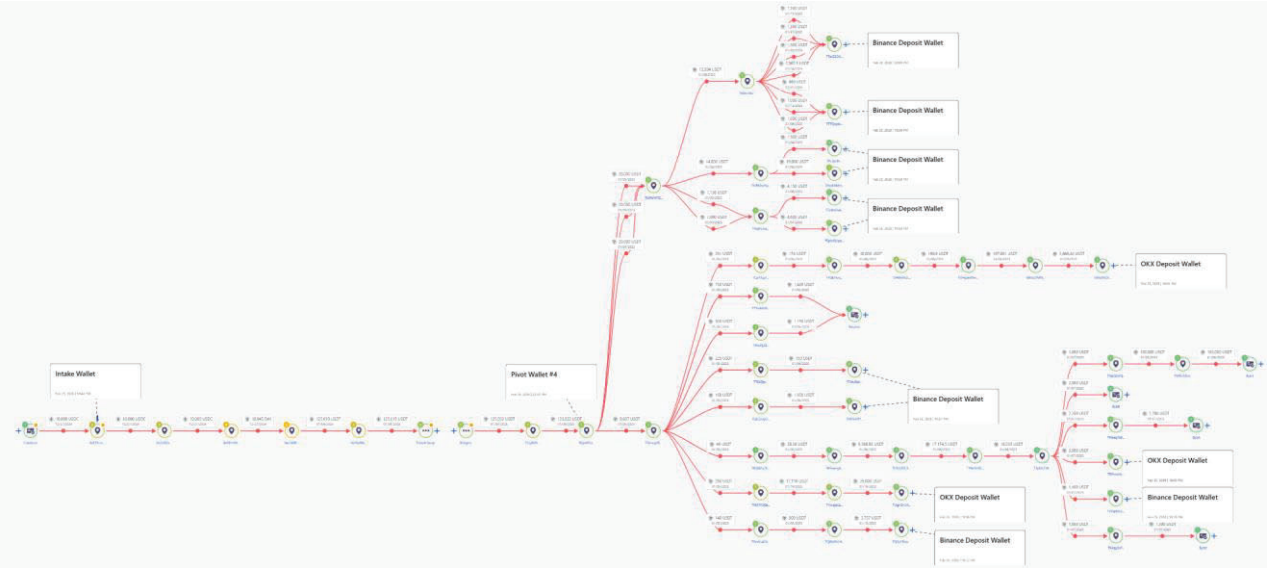
C. Individual Transfer Details and Tracing Graphs

24. Due to the nature and complexity of this trace, transactions in this trace were randomly sampled and visualized in order to visualize the different types of transaction behavior and how funds were routed.

Transfer 1

25. Funds first passed through 6 intermediary wallets, including a bridge, before being aggregated at Pivot Wallet TGjzAFEaTwDTPSvmwMPQVGtFAbMYdkjRif and then passed through 2-8 intermediary wallets before distribution to an Exchange-Hosted Deposit Wallets at Binance and OKX.

This movement is illustrated in the Flow of Funds Graph below.



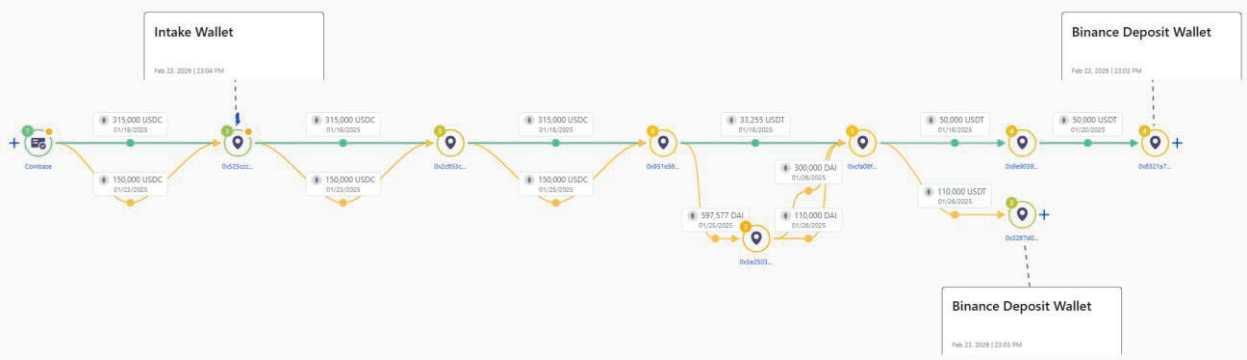
Transfer 5 and 6

26. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0x525ccc3e1631657d2bc00ff1684c7109d3d27336.

27. Funds from transfer 5 first passed through 2 intermediary wallets before being swapped from USDC to USDT. Then funds passed through 2 more intermediary wallets before the part of funds was distributed to an Exchange-Hosted Deposit Wallet at Binance.

28. Funds from transfer 6 first passed through 2 intermediary wallets before being swapped from USDC to DAI. Then funds passed through 1 more intermediary wallet before the part of funds was distributed to an Exchange-Hosted Deposit Wallet at Binance.

This movement is illustrated in the Flow of Funds Graph below.

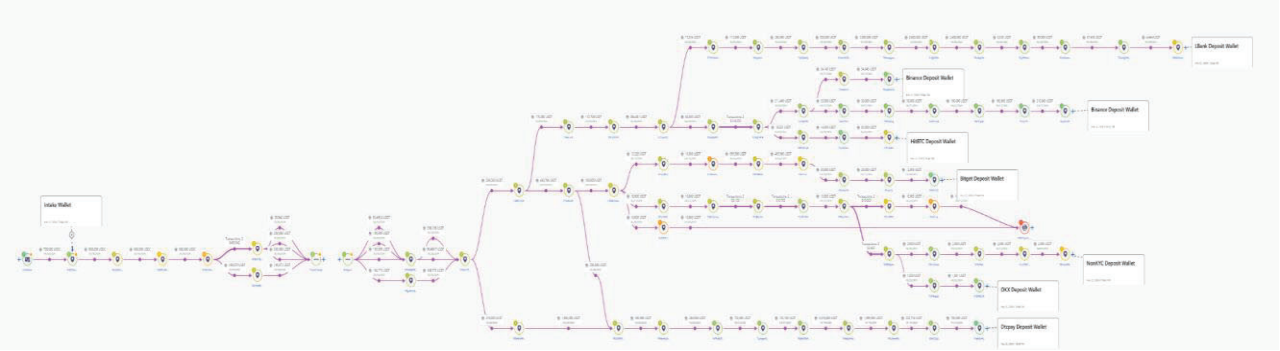


Transfer 14

29. The Victim transferred funds from their personally controlled wallet to Intake Wallet 0x525ccc3e1631657d2bc00ff1684c7109d3d27336.

- Funds first passed through 21 intermediary wallets before distribution to an Exchange-Hosted Deposit Wallet at LBank.
- Funds passed through 16 intermediary wallets before distribution to an Exchange-Hosted Deposit Wallet at Binance.
- Funds passed through 19 intermediary wallets before distribution to an Exchange-Hosted Deposit Wallet at Binance.
- Funds passed through 16 intermediary wallets before distribution to an Exchange-Hosted Deposit Wallet at Bitget.
- Funds passed through 17 intermediary wallets before distribution to an Exchange-Hosted Deposit Wallet at OKX.
- Funds passed through 16 intermediary wallets before distribution to an Exchange-Hosted Deposit Wallet at Dtcpay.

This movement is illustrated in the Flow of Funds Graph below.



III. BROADER FRAUD NETWORK AND CLASS IMPACT

A. Identifying the Broader Fraud Network

30. Forensic blockchain analysis confirms that the theft of the Victim's assets was not an isolated incident but part of a systematic fraud scheme, structured to obscure transaction origins and facilitate large-scale misappropriation of cryptocurrency. The same Pivot Wallets that received the Victim's funds also show structured inflows from multiple unrelated wallets following similar transaction patterns, confirming their role as collection points in a broader fraud network.

How Pivot Wallets Reveal Coordinated Theft Scheme

31. Pivot Wallets are essential to identifying the affected group or class of victims because they establish that multiple victims' funds were controlled by the same bad actor or group. These wallets function as aggregation points where stolen funds from numerous victims converge, demonstrating a systematic, coordinated scheme. Unlike isolated incidents of theft, where funds may follow unique or random paths, the presence of Pivot Wallets reveals a pattern of consolidation and redistribution of misappropriated assets. By consolidating funds from unrelated victims into a single location, Pivot Wallets establish a centralized point of control, linking disparate victims to a unified fraudulent operation.

B. Estimated Class Impact

32. By tracing inflows into known Pivot Wallets, forensic analysts identified several additional victim wallets that followed the same structured fund movement patterns as the Victim's transactions. These wallets exhibited identical laundering behaviors, confirming that they belong to additional victims of the same fraud scheme:

- **Matching structured transaction pathways** observed across multiple cases, following the same laundering techniques.
- **Pivot Wallet aggregation**, confirming that multiple victims' funds were pooled in the same intermediary wallets before onward movement.
- **Consistent transaction behaviors** across victims, reinforcing the presence of a coordinated fraud operation.

33. **Estimated Total Class-Wide Losses:** Class-wide losses are estimated to be approximately **$21,083,650 USD**, based on cumulative victim deposits into identified Pivot Wallets.

34. The funds were distributed across the exchanges listed below:

- Binance
- OKX
- Gate.io
- Kraken
- KuCoin
- Bybit
- Bitget

35. The Estimated Total Class-Wide Losses represents the total financial impact on victims. The Estimated Total Funds Traced to Exchange Deposit wallets reflects the portion of those total losses likely traceable to identifiable exchange accounts. The difference between the estimated class losses and the amount traced to Deposit Wallets reflects a combination of currently unrecoverable funds—held in a non-exchange wallet—and untraceable funds that have

been sufficiently laundered in ways that break the chain of traceable transactions.

36. While both figures are relevant to understand the extent and movement of stolen assets, differentiating helps clarify the full scope of victim losses versus the amount that may be subject to a freeze and, ultimately, recovery.

IV. OBSERVED LAUNDERING AND FRAUD INDICATORS

37. Forensic analysis confirms behavioral and technical patterns consistent with fraudulent activity, including structured fund movements that align with known laundering methodologies and existing fraud indicators implicating perpetrators' infrastructure, including the following:

- **Cross-chain** transfers via **Tokenlon** to disrupt tracking (e.g., funds moved from USDC to USDT).
- **Network conversions on Transit Swap and Bridgers** to obscure fund origins (e.g., swapping USDT on Ethereum network for USDT on Tron network to break traceability).
- **Rapid transfers through 6 wallets within 28 minutes** to avoid detection (e.g., assets moved through 6 wallets within 28 minutes to prevent clustering detection by analytics tools).
- **Partial splits into smaller amounts** to evade anti-money laundering thresholds (e.g., splitting $26,000 into multiple transactions under $2,000 to bypass exchange reporting requirements).

A. Identified Laundering Techniques:

38. The on-chain tracing analysis revealed several methods employed by perpetrators to obscure the origin and flow of stolen assets.

a. **Cross-Chain Transfers to Disrupt Tracking**:
Funds were moved across blockchains using Tokenlon, complicating traceability (e.g. assets converted from USDC to another cryptocurrency via Tokenlon service)

b. **Structured Consolidation of Victim Transactions**:
Smaller deposits from various victims were combined to form larger sums, making it difficult to trace individual origins. Several instances of funds consolidation were observed, as identified in the transaction graphs highlighting Pivot Wallets #1 and #2. These wallets obscure the original source of funds and facilitate layering to evade detection.

Tracing Graph

Partial visualization of Samuels trace, transfers 8-14, Crystal Intelligence

V. WALLETS TO FREEZE

39. The following Exchange-Hosted Deposit Wallets listed in below represent the last known locations where misappropriated assets were traced. Forensic blockchain analysis confirms that these wallets were used in structured laundering processes, and the stolen funds remain at imminent risk of further dissipation beyond recovery.

Total Addresses to Freeze: 77

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

40. Based on my forensic blockchain analysis, it is my professional opinion that Plaintiff's cryptocurrency was transferred from his Coinbase account to Defendants' Intake Wallet, routed through Pivot Wallets and intermediary addresses, and deposited into exchange-hosted wallets controlled by or associated with Defendants.

41. It is further my professional opinion that these transactions reflect a structured process involving common wallet infrastructure, including shared Intake Wallets, Pivot Wallets,

and exchange-hosted deposit wallets, consistent with a coordinated cryptocurrency fraud scheme affecting multiple victims.

42. Finally, it is my professional opinion that absent immediate injunctive relief, the remaining misappropriated cryptocurrency is at substantial risk of being transferred, concealed, or dissipated in a manner that would render recovery impracticable or impossible.

43. Based on my experience investigating cryptocurrency exchanges and digital asset platforms, centralized exchanges such as Binance, OKX, Kraken, and KuCoin maintain custody and control over deposit wallets associated with user accounts and have the technical ability to freeze or restrict withdrawals from those accounts when directed by court order."

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

Executed this second day of April 2026.

DocuSigned by:
Maya Vick
452DFBCE7CEF49F...

4/2/2026

Maya Vick