

1 William A. Delgado (SBN 222666)
wdelgado@dtolaw.com
2 Nicole G. Malick (SBN 335754)
nmalick@dtolaw.com
3 DTO LAW
4 915 Wilshire Boulevard, Suite 1950
Los Angeles, California 90017
5 Telephone: (213) 335-6999
6 Facsimile: (213) 335-7802

7 Shaun Martin (SBN 158480)
smartin@sandiego.edu
8 5998 Alcala Park, Warren Hall
San Diego, CA 92110
9 Telephone (619) 260-2347
10 Facsimile: (619) 260-7933

11 Attorneys for Plaintiff
YOUNES YOUNES
12

13 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**

14 **COUNTY OF LOS ANGELES**

15 YOUNES YOUNES, on behalf of himself
16 and all others similarly situated,

17 Plaintiff,

18 v.

19 ELVIRA TAYLOR and DOES 1 through 200,
20 inclusive,

21 Defendants.

Case No. 24STCV12520

**DECLARATION OF ADAM ZARAZINSKI
IN SUPPORT OF PLAINTIFF'S MOTION
FOR CLASS CERTIFICATION**

[Notice of Motion, Memorandum of Points and
Authorities, Statement Regarding Class Notice,
Proposed Notice of Pending Class Action,
Declarations of Younes Younes, Shaun Martin,
and Nicole G. Malick and Proposed Order Filed
Concurrently Herewith]

Assigned for All Purposes to Hon. Elihu Berle

Date: May 7, 2025
Time: 11:00 A.M.
Place: 312 N. Spring Street,
Los Angeles, CA 90012
Dept. 6

Action Filed: May 17, 2024
Trial Date: None

1 I, Adam Zarazinski, declare under penalty of perjury as follows:

2 1. I am employed as the Chief Executive Officer of Inca Digital (“Inca”), a company that
3 specializes in financial risk intelligence and investigating cryptocurrency schemes, including “pig
4 butchering.” As part of my employment at Inca, I have investigated matters related to the above-
5 captioned action. I have personal knowledge of the facts stated in this declaration, and if called as a
6 witness, I could and would testify competently to these facts.

7 2. I hold a J.D. from the University of Michigan Law School, a master’s degree in
8 international relations from the University of Nottingham, and a Bachelor of Arts in Political Science
9 from DePaul University. I have leveraged my specialized knowledge of blockchain technology, digital
10 asset ecosystems, and regulatory frameworks to serve as an expert witness in cryptocurrency-related
11 litigation. In this capacity, I have testified before the House Financial Services Subcommittee on
12 National Security, Illicit Finance, and International Financial Institutions on issues related to terrorist
13 financing and the misuse of blockchain technology. Prior to my work at Inca Digital, I worked as an
14 intelligence analyst at INTERPOL and served in the United States Air Force as a judge advocate. I
15 continue to serve as a Major in the USAF JAG Corps Reserve.

16 3. Inca Digital is a financial risk intelligence company that specializes in blockchain
17 analysis and cryptocurrency investigations. Inca has extensive expertise in tracing stolen digital assets
18 across complex fraud schemes, including pig butchering scams — a type of cryptocurrency fraud in
19 which victims are manipulated into transferring funds under false pretenses, often through fake online
20 platforms. Inca’s investigative work frequently involves analyzing structured laundering tactics
21 designed to obscure the origin and movement of misappropriated assets. Inca’s forensic tracing
22 capabilities are widely recognized in the industry for identifying victim funds, tracking those funds
23 across fragmented transaction pathways, and mapping their movement to their final destination in
24 controlled wallets.

1 4. **Forward Tracing:** Inca conducted a forensic tracing analysis mapping the movement
2 of Plaintiff's cryptocurrency assets from their origins to their final known destinations. The analysis
3 revealed that, at Defendants' direction, Plaintiff and other victims were instructed to send funds to
4 specific wallets controlled by Defendants. These funds were then routed through additional wallets,
5 fragmented via conversion services, and ultimately consolidated in deposit wallets at Binance and
6 OKX. This tracing analysis identified Defendants' structured laundering tactics and the deliberate
7 effort to obscure the origin of victim funds.

8 5. **Pivot Wallets:** The Defendant-controlled wallets, which initially received Plaintiff's
9 and other class members' funds, are referred to as "Pivot Wallets." They operated as key control points
10 where victim deposits were aggregated before being redirected through multiple onward transactions
11 — effectively "pivoting" the flow of stolen funds to break clean transaction links and obscure their
12 origin. This deliberate blending tactic ensured individual victim transactions became indistinguishable
13 before being routed onward through services designed to further frustrate traceability. After this
14 aggregation and dispersal, Plaintiff's funds, like those of other victims, were fragmented through
15 conversion services and ultimately consolidated in specific wallets at Binance and OKX. In this case,
16 Defendants consistently relied on the following four Pivot Wallets to receive and consolidate victim
17 deposits:

18 0x49f8B7feEE8C0B85ff61F2d7c38Af809614515Df

19 0x64E5f1a2480a3967EDD30b0b400Daf18422cE552

20 0x26196D89281e89f910c187b992C47C90D8200283

21 0x803BD7f6346127E0098d8a6f4aA3996410097aC1

22 6. **Conversion Tactics and Blockchain Obfuscation:** After consolidating victim funds
23 in these specific Pivot Wallets, Defendants employed cryptocurrency conversion services — including
24 SWFT.PRO and OKX DEX Aggregation — to convert stolen Ethereum (ETH) into USDT on the
25 TRON blockchain. This conversion tactic severed the original Ethereum transaction trail that linked
26 victim deposits to Defendants' accounts. By shifting assets to the TRON blockchain, Defendants
27 effectively fragmented the transaction history, breaking identifiable links between victim deposits and
28 endpoint wallets and further complicating recovery efforts.

1 7. **Final Destination of Stolen Funds:** Following the conversion process, Defendants
2 transferred the laundered funds through additional intermediary wallets before consolidating the stolen
3 assets in specific wallets at Binance and OKX. These wallets — identified as the final known
4 destinations for misappropriated funds — reflect the endpoint of the structured laundering scheme.

5 8. **Reverse Tracing and Identification of Victim Wallets:** Inca also conducted a reverse
6 tracing analysis, mapping the flow of funds from their final destination back to their originating
7 sources. This reverse tracing analysis revealed that the originating wallets — referred to as “Victim
8 Wallets” — belonged to class members whose assets were misappropriated through the same scheme.
9 Inca identified 325 Victim Wallets that followed the same movement pattern, allowing reliable
10 identification of class members.

11 9. **Staged Return Payments:** In addition to the structured movement of victim funds,
12 Inca’s forensic analysis identified a pattern of staged return payments — a tactic commonly seen in
13 pig butchering schemes. Perpetrators in such schemes often send small payments back to victims’
14 wallets to create the appearance of legitimate returns, encouraging continued deposits. In this case,
15 Defendants used two designated wallets — identified as “Staged Return Wallets” — to send staged
16 payments back to Victim Wallets that had previously transferred funds. This pattern mirrored
17 manipulation tactics designed to reinforce victim trust and prompt additional deposits. Defendants
18 consistently used the following two wallets to issue these payments (Staged Return Wallets):

19 0xA86545f9DCDd98869536401A76759Fd1227aAf29

20 0xe0227298588541484E81c44f7C3D107e3C3aAEaf.

21 By deceitfully creating the illusion that victims’ accounts were active and profitable, this tactic
22 encouraged victims to send increasingly larger deposits. This pattern — repeatedly observed across
23 numerous victim transactions — reflected a calculated deception strategy consistent with those seen
24 in similar schemes.

1 10. **Class Identification Process:** Inca’s identification of class members relied on two
2 consistent data points observed across victim transactions: (a) Victim Wallet deposits into identified
3 Pivot Wallets, and (b) Staged return payments to Victim Wallets from the two identified Staged Return
4 Wallets. By analyzing these recurring markers in combination with broader tracing patterns, Inca
5 identified 325 class members with precision. This recurring pattern provided a distinct and verifiable
6 indicator of class membership.

7 11. **Reliability of Blockchain Evidence:** The methods and conclusions described in this
8 declaration rely on blockchain transaction records, which are public, immutable, and independently
9 verifiable. Blockchain data is widely recognized as a reliable method for tracing cryptocurrency
10 transactions due to its transparency and permanence. These records conclusively demonstrate the
11 systematic nature of Defendants’ fraudulent scheme and establish a reliable basis for identifying class
12 members, quantifying losses, and validating the findings.


13 12. **Challenges in Victim Recovery:** Based on my experience investigating pig butchering
14 schemes, these operations are deliberately designed to frustrate recovery efforts by exploiting victims’
15 limited technical knowledge and resources. Victims are often geographically dispersed and lack access
16 to the forensic tracing tools necessary to track their stolen assets. Pig butchering scams rely on
17 structured fund movement tactics that deliberately obscure the origin and flow of victim deposits,
18 making it particularly difficult for victims to trace their stolen cryptocurrency or connect their losses
19 to the broader scheme. Identifying and tracing Defendants’ cryptocurrency transactions required
20 specialized forensic analysis to overcome these deliberate obfuscation tactics.

21 13. **Class Notification Process:** Inca, alongside Counsel for Plaintiff, will notify potential
22 class members of this action by collaborating with cryptocurrency exchanges that maintain contact
23 details for account holders linked to identified Victim Wallets. If exchange-facilitated notification is
24 ineffective, Plaintiff and Inca will also employ alternative methods such as token dropping to ensure
25 class members are properly informed.

1 14. Based on my extensive experience investigating these schemes and the forensic tracing
2 analysis, I have concluded that this case involves a highly coordinated, large-scale pig butchering
3 operation. Defendants employed a structured, repeatable laundering process designed to exploit victim
4 trust, obscure the origin of misappropriated assets, and encourage continued deposits. Defendants'
5 calculated tactics ensured that all class members were impacted in the same way — each victim's
6 funds were funneled through a controlled network of wallets before being consolidated in specific
7 wallets at Binance and OKX. To further deceive victims and prolong their belief that the platform was
8 legitimate, Defendants issued staged return payments that deceitfully reinforced victim trust and
9 fraudulently encouraged additional deposits.

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

12
13 Executed this 4 day of April, 2025, in Washington , DC .

14
15 
16 _____
17 Adam Zarazinski
18
19
20
21
22
23
24
25
26
27
28