

1 SHAUN P. MARTIN (SBN 158480)
2 5998 Alcala Park, Warren Hall
3 San Diego, CA 92110
4 T: (619) 260-2347 | F: (619) 260-7933
5 smartin@sandiego.edu

6 *Counsel for Plaintiff Howard Mann*

Electronically FILED by
Superior Court of California,
County of Los Angeles
7/15/2024 9:51 AM
David W. Slayton,
Executive Officer/Clerk of Court,
By J. Lara, Deputy Clerk

8 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
9 **COUNTY OF LOS ANGELES**

10
11 HOWARD MANN, on behalf of himself and
12 all others similarly situated,

13 Plaintiff,

14 v.

15 SEAN MOORE, MIRANDA GOMEZ, and
16 DOES 1 through 200, inclusive,

17 Defendants.

Case No. 24STCV17012

**DECLARATION OF CHARLES ZACH IN
SUPPORT OF PLAINTIFF'S EX PARTE
APPLICATION FOR TEMPORARY
RESTRAINING ORDER AND OSC RE:
PRELIMINARY INJUNCTION**

Assigned for All Purposes to:

Judge: William F. Highberger

Date: July 16, 2024

Time: 8:30 a.m.

Place: 312 N. Spring Street

Los Angeles, CA 90012, Dept. 10

1 I, Charles Zach, declare under penalty of perjury as follows:

2
3 1. My name is Charles Zach. I am an employee at Inca Digital, a company that
4 investigates cryptocurrency schemes, including “pig butchering.” As part of my employment at Inca
5 Digital, I have investigated matters related to the complaint by Howard Mann (“Plaintiff”) in the
6 above-captioned action. I am over 18 years of age, of sound mind, and am competent to make this
7 Declaration. The evidence set forth in the foregoing Declaration is based upon my personal knowledge
8 unless expressly stated otherwise, and if called and sworn as a witness, I could and would testify to
9 each of the facts set forth herein.

10 2. Inca Digital is a digital asset intelligence company that provides data, analytics, and
11 expertise to many of the world's leading exchanges, financial institutions, regulators, and government
12 agencies. Inca Digital's clients use its unique and comprehensive intelligence to surveil digital asset
13 markets, fight crime, generate alpha, and more. For more information about Inca Digital and our work,
14 please visit: <https://inca.digital/>.

15 3. Inca Digital has been investigating “pig butchering” cases for over two years. “Pig
16 butchering” victims in the United States have lost billions of dollars and “pig butchering” schemes
17 have been the subject of state and federal government investigation and prosecution.¹ Based on my
18 expertise and experience, this is a clear case of “pig butchering.”

19 4. I understand that this class action is brought to freeze wallets containing class member
20 funds that Defendants converted and to return these funds to class member victims. Based on Inca’s
21 investigation to date, Defendants conversion scheme involved approximately 100 class member
22 victims, who lost approximately \$850,000 combined.

23
24
25
26

27 ¹ See FinCEN Alert of Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering,” U.S.
28 Treasury Financial Crimes Enforcement Network Sep. 8, 2023,
https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf

1 5. Through my investigation, I discovered that Defendants attempted to conceal their
2 conversion of the cryptocurrency of the members of the class through a series of online transactions
3 designed to hide their trail. However, to date, an investigation by Inca has been able to trace and
4 connect Defendants' transactions, follow the trail, and identify several of the cryptocurrency wallets
5 that held and/or hold the cryptocurrency funds of Mr. Mann and members of the class.

6 6. Inca's investigation involved two phases, each of which is precise, reliable, and
7 replicable. First, in phase one, Inca "forward traced" funds from the Bitcoin ATM where Mr. Mann
8 deposited his money to identify the cryptocurrency wallet addresses to which Mr. Mann's funds were
9 transferred as Bitcoin. This process involved three steps: (1) identifying the addresses of wallets that
10 initially received Mr. Mann's assets from the ATM; (2) tracking the transfer of his assets from there
11 to two or three different wallet addresses; and (3) determining that the assets were ultimately deposited
12 directly to a known fraud shop wallet address or to wallets at the cryptocurrency exchanges Binance
13 and KuCoin ("Deposit Addresses").

14 7. Subsequently, in phase two, Inca "reverse traced" the flow of funds assets from the
15 addresses identified in Phase One and identified additional wallet addresses involved in the same
16 transaction patterns matching Plaintiff's flow of funds, revealing more victims of the same scheme.
17 Based on this analysis, Inca concluded that the class affected by this scam includes approximately 100
18 victims, who collectively lost about \$850,000. Like Mr. Mann, most victims' assets originated from
19 Bitcoin ATMs (with some also coming from centralized exchanges), and then passed through two or
20 three different wallet addresses before being directly transferred to a known fraud shop wallet address
21 or deposited to Binance or KuCoin wallets.

22 8. The Deposit Addresses of wallets containing funds stolen from Mr. Mann and other
23 victim class members are set forth below, categorized by cryptocurrency exchange (Binance and
24 Kucoin):

25 Binance

26 15PGbkbXoVSQXWTHXwrcJPevq8NV5Ffdho

27 1A2PWvYo8EmysLFbYL99gGHK3haqRo9fiN

28 13GJh5kyqfgtsb5GP6VqH2fvAEQLPzPp5X

1 1LF7Vo9qsx1KLvUnRJc3yqhXYkzCjic1zw
2 14rTVLjXHasdcqRH2p24kFVnkcWSvahCzU
3 166r3x91TfWh8D27Ej2QkcUT3qTyHPLJmZ
4 1MoYksuZoQwpvrGUAkXYtrwrrPK9ByG4Tj
5 1CGbRD4qfFjkQpNggKF3EJzj9wJhSatWt2
6 1LZQbKLCHzMeHPEq52hLrjEnoSJz39ahsq
7 1FQqrmfVoVQuUQEMAzsXkHeT4nkYja4gm
8 1Ntq5herKqrKa3iGUA9rQvcVwB3VAEKCNI
9 12QAqsBQUQXwniXA21gRrASbpokjdvhz15
10 19vLaAuy16Cbh7zfxaHoBvG4Nof3QwbtoR
11 1KBVi3EdFfDsXJvd6Xuyeum8oKugnaCffP
12 1J9hSv4yBgz2xWUbfhZMQHSw8yFAqFw7m
13 1PCJbKmF1aZSeeodMQNbS6dKe6FDv4JqFF
14 1HS7voGRhq73mg4dmoy4jt8We8Zthnqd6p
15 1CGbRD4qfFjkQpNggKF3EJzj9wJhSatWt2
16 1DF2tninBnokz9L4Tb61U8Pv8zc3Rggg8P
17 1EyKJN6JT xvQergHhcJUWyYzgcdhZ1Lqeo

18
19 KuCoin

20 3L5HM9PvUqu9YwKgNLVyLggCZ84sCp8KWZ
21

22 9. Inca's investigation found that many of the above-listed Binance wallet addresses are
23 connected by deposits from one or more common counterparty wallet addresses. This connectivity
24 provides compelling evidence of a systematic fraud network used to funnel stolen funds,
25 demonstrating a coordinated effort to launder money. The pattern of transactions through multiple
26 addresses before reaching the Deposit Addresses highlights Defendants' deliberate measures to
27 obscure the origin of the funds.
28

10. Based upon my substantial experience involving pig butchering schemes similar to this one, if Plaintiff is required to wait until after the Defendants receive notice of this action, it is highly likely that the Defendants will transfer cryptocurrency at issue beyond the reach of discovery or recovery.

11. I am familiar with the process of providing notice via the deposit of airdropped or similar service tokens to cryptocurrency accounts, and in my experience, the method of notice proposed in the Proposed Order is reasonably calculated to and would likely result in actual notice of those documents to the individuals or entities that control those wallets, and the existence and contents of those service tokens would be readily apparent to the owners.

Executed this 15th day of July, 2024, in Sinj, Croatia.

Charles Zach
Charles Zach