JOSHUA D. HURWIT, IDAHO STATE BAR NO. 9527
UNITED STATES ATTORNEY
WILLIAM M. HUMPHRIES, IDAHO STATE BAR NO. 11709
ASSISTANT UNITED STATES ATTORNEY
DISTRICT OF IDAHO
1290 W. MYRTLE STREET, SUITE 500
BOISE, IDAHO 83702
TELEPHONE: (208) 334-1211
FACSIMILE: (208) 334-1413

Attorneys for the United States of America

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

UNITED STATES OF AMERICA, Plaintiff, vs. ANY AND ALL CRYPTOCURRENCY (AND FUNDS DERIVED THEREFROM) SEIZED FROM BINANCE ACCOUNT USER ID 91911251 IN THE NAME OF WANPADET SAE-HENG REGISTERED MARCH 3, 2021, FROM THAILAND AS FOLLOWS: 97.33604121 IN BITCOIN, 2,560,435.71078314 IN DOGECOIN, 884.33368015 IN ETHEREUM, 85,843.844344 IN CARDANO, AND 884.13243271 IN ETHEREUM POW. Defendant.	Case No. **VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

Plaintiff, United States of America, brings this complaint and alleges as follows in accordance with Rule G(2) of the Supplemental Rules for Admiralty or Maritime and Asset Forfeiture Actions, Federal Rules of Civil Procedure:

NATURE OF THE ACTION

1. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(C) for forfeiture of cryptocurrency, which constitutes or is derived from proceeds traceable to a violation of specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), including but not limited to wire fraud, 18 U.S.C. § 1343, or a conspiracy to commit such offense.

2. This is a civil action *in rem*, brought to enforce the provision of 18 U.S.C. § 981(a)(1)(A) for the forfeiture of cryptocurrency, which is involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and/or 1957, or any property traceable to such property.

PLAINTIFF AND THE DEFENDANT *IN REM*

3. The plaintiff is the United States of America (the "Plaintiff" or "Government").

4. The defendant consists of cryptocurrency (the "Defendant Cryptocurrencies") seized by the U.S. Federal Bureau of Investigation ("FBI") from an account at Binance via a federal seizure warrant. The Binance account had a user ID of 91911251 and was in the name of Wanpadet Sae-Heng and was registered on March 3, 2021, from Thailand ("Subject Account"). The seizure warrant was issued by the Honorable Raymond Patricco, U.S. Magistrate Judge, on December 21, 2022.

5. The Defendant Cryptocurrencies are currently in the custody of the FBI.

6. The following quantities of cryptocurrency were seized from the Subject Account and are what constitute the Defendant Cryptocurrencies:

a. 97. 33604121 in Bitcoin,

b. 2,560,435.71078314 in Dogecoin,

c. 884.33368015 in Ethereum,

d. 85,843.844344 in Cardano, and

e. 884.13243271 in Ethereum PoW.

7. The interests of Wanpadet Sae-Heng and the victim(s) identified herein may be adversely affected.

JURISDICTION AND VENUE

8. This Court has jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345 and over an action for forfeiture under 28 U.S.C. § 1355(a) and (b).

9. Venue is proper in this district pursuant to 28 U.S.C. §§ 1355(b)(1) and 1395 because the acts or omissions giving rise to the forfeiture occurred in this district.

SUMMARY BASES FOR FORFEITURE

10. The United States alleges that the Defendant Cryptocurrencies were involved in transactions and attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (Money Laundering) and 1956(h) (Conspiracy to Commit Money Laundering), and constitute or were derived from proceeds traceable to violations of 18 U.S.C. §§ 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), 1956(a)(1)(B)(i) (Money Laundering), and 1956(h) (Conspiracy to Commit Money Laundering). The Defendant Cryptocurrencies are, therefore, subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) and 28 U.S.C. § 2461.

PURPOSE OF FORFEITURE

11. The purpose of this forfeiture action *in rem* is two-fold. First, forfeiture of the Defendant Cryptocurrencies provides a means for the Government to help victims of the scam recover their funds. Second, forfeiture deters criminal activity by forfeiting and vesting title of the Defendant Cryptocurrencies with the Government so that criminals do not maintain the fruits of crime and do not keep facilitating or involved in property of crime. The Defendant Cryptocurrencies are the remnants of funds swindled from victims, including those in the District of Idaho, through the course of an investment fraud scam. The funds were subsequently laundered through a circuitous web of virtual currency exchanges, wallet addresses, and blockchains. Thus, in summary, the Defendant Cryptocurrencies constitute proceeds subject to forfeiture as proceeds, facilitating property, and property involved in wire fraud, conspiracy to commit wire fraud, money laundering, and conspiracy to commit money laundering.

BACKGROUND ON DIGITAL OR VIRTUAL CURRENCY

12. **Virtual or Digital Currency:** Digital currency (also known as cryptocurrency or virtual currency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currencies exhibit properties similar to other currencies, but do not have a physical form, existing entirely on the internet. Digital currency is not issued by any government or bank (in contrast with "fiat" or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network.

[1] For purposes of this complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

13. **Virtual or Digital Currency Addresses:** Digital or virtual currency addresses are the virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

14. **Private Key:** Each virtual currency address is controlled through a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

15. **Address Owner:** The identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), but analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

16. **Blockchain:** Many virtual currencies publicly record their transactions on what is referred to as the "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. Investigators can follow or "trace" funds on public blockchains, a practice known as "blockchain analysis."

17. **Blockchain Analysis:** It is virtually impossible to look at a single transaction on a blockchain and immediately ascertain the identity of the individual behind the transaction. That is because blockchain data generally consist only of alphanumeric strings and timestamps. But law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To analyze blockchain data, law enforcement can use blockchain explorers as well as commercial services offered by blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

18. **Virtual Currency Wallet:** A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a digital currency exchange to make a transaction between digital currency and fiat currency, or through digital currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

19. **Virtual Currency Exchange:** A digital or virtual currency exchange (an "exchange") is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. Many exchanges are located outside the boundaries of the United States to avoid regulation and legal requirements. One of the largest and most popular exchanges is Binance.

20. Notwithstanding, because exchanges act as money services businesses, they are legally required to conduct due diligence of their customers (i.e., "know your customer" or "KYC" checks) and to have anti-money laundering programs in place.

21. **Stablecoins:** Stablecoins are a type of virtual currency pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar. USDT (also known as "Tether," the name of its issuer) is a stablecoin cryptocurrency that resides on multiple blockchains, namely the Ethereum and Tron blockchains, among others. The value of USDT is tied to the value of the U.S. dollar; therefore, one unit of USDT is represented to be backed by one U.S. dollar in Tether Ltd.'s (a company based in Hong Kong) reserves, which is what makes it a "stablecoin."

22. **Ethereum:** Ethereum ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH.

23. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, it is also often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership, or control of illegally obtained criminal proceeds. Bitcoin and Ethereum are some of the most commonly used and well-known digital currencies.

FACTS AND THE SCHEME

Background on Pig Butchering Investment Scheme

24. This case involves an investment fraud scam, commonly referred to as "pig butchering," perpetrated on victims throughout the United States, including in the District of Idaho.

25. Pig butchering likely originated in China in 2019. The locus of pig butchering activity moved from China, after the country banned cryptocurrency, to nearby locations in Southeast Asia.

26. The Pig Butchering scheme typically begins when a scammer sends a victim a seemingly innocuous and misdialed text or WhatsApp message. From there, the scammer will attempt to establish a more personal relationship with the victim by using manipulative tactics similar to those used in online romance scams.

27. The victims in Pig Butchering schemes are referred to as "pigs" by the scammers because the scammers will use elaborate storylines to "fatten up" victims into believing they are in a romantic or otherwise close personal relationship. Once the victim places enough trust in the scammer, the scammer brings the victim into a cryptocurrency investment scheme. The investment schemes are fake but have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative or "spoofed" websites that appear related to legitimate

companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns.

28. A common technique used in pig butchering scams is to convince victims to connect their wallet to a decentralized application (dApp) created by the scammers. Once the victim's wallet is connected to the scammer's dApp and certain permissions are accepted, the scammer then has the ability to withdraw all cryptocurrency tokens in the victim's wallet, without the victim's knowledge.

29. The investment platforms are a ruse, and the funds contributed are routed directly to a cryptocurrency address the scammers control (this is when the scammers refer to "butchering" or "slaughtering" the victims). When the victims attempt to withdraw their funds, they are unable to do so and are often met with various excuses or even required to pay "taxes" to release their funds. The "tax" payments are an attempt by the scammers to elicit even more money out of the victims. Eventually, most victims are completely locked out of their accounts and lose all of their funds.

Victim and Tracing of Victim Funds to the Subject Account

30. In this case, the FBI has identified a victim from Idaho with an estimated loss of at least $509,000 related to these various fraudulent investment platforms. The fraudulent investment platforms are sometimes offshoots of legitimate platforms. The domain name iteration in this case is as follows: www.eth-defis.co.

31. Some of the funds of the identified victim of this scheme, whose funds were directed to the Subject Account, have been traced from the initial wallet address to the Subject Account.

32. Based upon the Know Your Customer ("KYC") information provided to Binance, the Subject Account in this case was registered from a country, Thailand.

33. This complaint does not include all of the cryptocurrency and blockchain analysis performed, but rather focuses on the tracing of specific funds from victims into the Subject Account in order to demonstrate the concerted effort to launder and obfuscate the flow of funds into the Subject Account. Cryptocurrency addresses are truncated throughout this complaint.

Victim T.C.

34. An unknown purported female, and purportedly Chinese, reached out to T.C. on WhatsApp. T.C. is a victim and resides in Idaho. She told T.C. her name was Liai Hui ("HUI"). HUI claimed to know T.C. through a mutual friend. HUI told T.C. she was a teacher. HUI presented a cryptocurrency (ETH) investment opportunity to T.C. HUI told T.C. she would walk him through setting up his account.

35. HUI instructed T.C. to deposit money from his bank account to a newly opened account with OKCoin. T.C started his investment with a smaller amount of $50,000 in November 2021. Shortly thereafter, T.C. wired $153,000 and $305,000 in separate transactions to his OKCoin account in December 2021. HUI provided instructions to then convert these funds to Tether (USDT). HUI sent T.C. a link to his cell phone for an app, instructing T.C. to click on the link to an account that HUI had told him would be at Coinbase. T.C. sent his entire investment account from OKCoin to what he thought was his account at Coinbase.

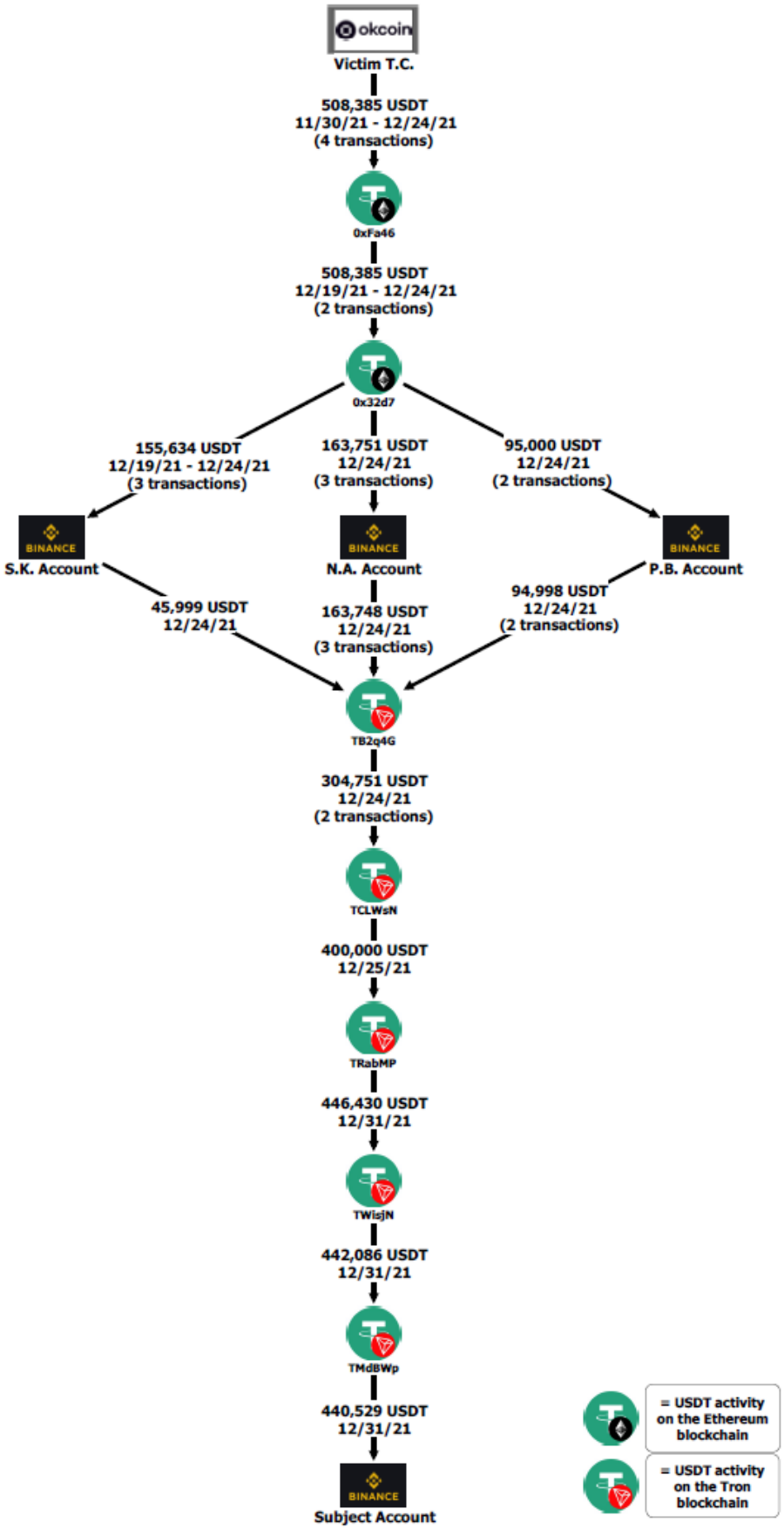
36. However, the funds were sent to the scammer's account and disappeared from there. The scammers gave T.C. an "overlay" that showed on his phone as Coinbase but turned out to be the fraudulent account. The fraudulent account had a URL of: https://eth-defis.co/#/. At one time, T.C.'s account showed a balance of approximately $720,000. By mid-January

2022, T.C.'s account showed a zero balance. T.C. never heard from HUI again after losing his entire investment of $509,100.

Tracing of Victim T.C.'s Funds to the Subject Account

37. From November 29, 2021, through December 23, 2021, T.C. sent three wires and one debit card transaction, for a total of $509,100, from his bank account to an account at OKCoin, a cryptocurrency exchange, which he created at the direction of HUI. T.C. converted the $509,100 into 508,385 USDT and transferred the USDT to a wallet (0xFa46), at the direction of HUI. When T.C. later checked the wallet balance, he saw that the entire 508,385 USDT had been transferred to a wallet address controlled by the scammers, 0x32d7.

38. Within minutes of each deposit into wallet address 0x32d7, the USDT was withdrawn, with the majority being sent to three Binance accounts (the "S.K. Account", the "N.A. Account", and the "P.B. Account", collectively the "Passthrough Accounts"). All the USDT deposits into the Passthrough Accounts were withdrawn within minutes. The USDT was then rapidly transferred into and out of multiple intermediary wallet addresses, where it was commingled with other funds, before a portion (i.e., 304,745 USDT) of the stolen funds arrived at the **Subject Account**, as shown in the graph below:


okcoin
Victim T.C.
508,385 USDT
11/30/21 - 12/24/21
(4 transactions)
0xFa46
508,385 USDT
12/19/21 - 12/24/21
(2 transactions)
0x32d7
155,634 USDT
12/19/21 - 12/24/21
(3 transactions)
163,751 USDT
12/24/21
(3 transactions)
95,000 USDT
12/24/21
(2 transactions)
BINANCE
S.K. Account
BINANCE
N.A. Account
BINANCE
P.B. Account
45,999 USDT
12/24/21
163,748 USDT
12/24/21
(3 transactions)
94,998 USDT
12/24/21
(2 transactions)
TB2q4G
304,751 USDT
12/24/21
(2 transactions)
TCLWsN
400,000 USDT
12/25/21
TRabMP
446,430 USDT
12/31/21
TWisjN
442,086 USDT
12/31/21
TMdBWp
440,529 USDT
12/31/21
BINANCE
Subject Account
= USDT activity on the Ethereum blockchain
= USDT activity on the Tron blockchain

39. After the deposit into the Subject Account, only one withdrawal occurred of 117,473.50 USDT.

40. The use of passthrough accounts, such as depicted in the graph above, is a common method used by individuals who are attempting to launder large amounts of cryptocurrency and, therefore, want to thwart law enforcement's ability to trace, and ultimately recover, criminal proceeds.

41. There is no apparent reason, economic or otherwise, for the use of such a complex movement of cryptocurrency through multiple intermediary wallet addresses, unless the purpose is to conceal the nature, source, location, ownership, or control of the funds at issue.

The Passthrough Accounts

42. The three Binance Passthrough Accounts were each registered utilizing a different Thailand National ID Card and photo verification; however, the Passthrough Accounts are likely under common control, based on the following analysis of these accounts:

a. All three accounts were registered within three days of each other, from December 9, 2021, through December 11, 2021, which was during the time period T.C. was in contact with HUI.

b. All three accounts were registered using IP addresses based in Thailand. After the accounts were created, the majority of the IP address activity on all three accounts resolved to the same IP address leasing service.

c. The photo verification pictures provided to Binance, as part of the required account creation procedures, appear to have been taken in parking lots for all three accounts. It is highly unusual for photo verification pictures to be taken in parking lots.

d. All three accounts have only 8-10 total cryptocurrency deposits each, with the majority of deposits in each account coming from wallet address 0x32d7.

e. Each deposit of T.C.'s funds into all three accounts was withdrawn within six minutes of the respective deposit. Additionally, each withdrawal in all three accounts was for exactly 1 USDT less than the respective deposit.

f. All USDT deposits of T.C.'s funds into the three accounts occurred on the Ethereum blockchain; however, all corresponding withdrawals in all three accounts occurred on the Tron blockchain. This process of swapping from one type of cryptocurrency or blockchain to another is known as "chain-hopping," a common technique used when laundering cryptocurrency because it is a method used to obfuscate the flow of funds.

FIRST CLAIM FOR RELIEF

18 U.S.C. § 981(a)(1)(A)

43. The Government realleges, adopts, and incorporates all allegations in the paragraphs above as though fully set forth herein.

44. The Defendant Cryptocurrencies constitute property involved in transactions or attempted transactions in violation of 18 U.S.C. §§ 1956 & 1957 (relating to money laundering), or property traceable to such property, with the specified unlawful activity being violations of 18 U.S.C. § 1343. The Defendant Cryptocurrencies are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

SECOND CLAIM FOR RELIEF

18 U.S.C. § 981(a)(1)(C)

45. The Government realleges, adopts, and incorporates all allegations in the paragraphs above as though fully set forth herein.

46. Based on the facts set out above, the Government alleges that the Defendant Cryptocurrencies constitute or are derived from proceeds traceable to violations of a specified unlawful activity as defined in 18 U.S.C. § 1956(c)(7), including wire fraud, 18 U.S.C. § 1343, or a conspiracy to commit such offense. The Defendant Cryptocurrencies are, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

WHEREFORE, plaintiff United States of America prays:

a. that due process issue to enforce the forfeiture of the Defendant Cryptocurrencies such that process issue for an arrest warrant *in rem* for the arrest of the Defendant Cryptocurrencies;

b. that due notice be given to all interested parties to appear and show cause why forfeiture should not be decreed;

c. that this Court decree forfeiture of the Defendant Cryptocurrencies to the United States of America for disposition according to law; and

d. for such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

DATED this 15th day of November, 2023.

JOSHUA D. HURWIT
UNITED STATES ATTORNEY
By:
/s/ William M. Humphries
WILLIAM M. HUMPHRIES
Assistant United States Attorney

VERIFICATION

I, John Pollard, hereby verify and declare under penalty of perjury that I am a Special Agent with the Federal Bureau of Investigation, that I have read the foregoing Verified Complaint *In Rem* and know the contents thereof, and that the matters contained in the complaint are true to the best of my knowledge and belief.

The sources of my knowledge and information and the grounds of my belief are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my involvement in the investigation of this case, together with other officers and employees of the FBI.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Dated this 15th day of November, 2023

John Pollard
FBI Special Agent