AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Justin M. Woodford, having been duly sworn on oath, state as follows:

Affiant's Background

1. I am a Special Agent with the Federal Bureau of Investigation and have been since January 2021. Since becoming a Special Agent, I have been assigned to a Cyber Crime Task Force in Albany, NY. I am responsible for investigating complex criminal computer intrusions and cyber fraud, including fraud involving cryptocurrency. I have experience working ransomware, business email compromise, and cryptocurrency trading platform fraud cases, commonly known as "Pig Butchering". I have received training related to cyber security, open-source intelligence, and reverse malware engineering and have a bachelor's degree in computer and information Science. I have participated in the execution of search warrants involving electronic evidence, including searches of email accounts and computers.

2. Because I am submitting this affidavit for the limited purpose of establishing probable cause for the requested seizure warrants, I have not included in this affidavit every detail I know about this investigation. Rather, I have included only the information necessary to establish probable cause for the requested seizure warrants.

3. The facts set forth in this affidavit are based on my personal knowledge, including what I have learned through my training and experience as a law enforcement officer, my review of documents and other records obtained in the course of this investigation, and information I have obtained in the course of this investigation from witnesses having

personal knowledge of the events and circumstances described herein and other law enforcement officers, all of whom I believe to be truthful and reliable.

Introduction

4. I submit this affidavit in support of applications for warrants to seize all cryptocurrency and fiat currency associated with certain digital wallets owned and controlled by Feng Chen, which wallets are specifically described as follows::[1]

a. A seed phrase labeled "metamask Feng – iphone 13 pro max" starting with the word "caught" and ending with the word "slide".

b. A seed phrase labeled "imtoken – June – proj" starting with the word "venue" and ending with the word "pledge".

c. A seed phrase labeled with unknown characters and "iphone13promax meta" starting with the word "sad" and ending with the word "web".

d. A seed phrase labeled with unknown characters and "Feng TP (ip 13 pro max)" starting with the word "proud" and ending with the word "Satoshi".

e. A seed phrase labeled "August – imtoken" starting with the word "fiber" and ending with the word "twice".

f. A seed phrase labeled "iphone 14 imtoken – Sept" starting with the word "table" and ending with the word "myself".

[1] Identifying information about each of the subject wallets, such as the username and pin or the complete wallet recover seed, is redacted to protect the wallets from being accessed by the subject or anyone else, either before or after the warrants are executed.

g. A seed phrase labeled "iphone 14 imtoken – Oct" starting with the word "depth" and ending with the word "vendor".

h. A seed phrase labeled "iphone 14 pro max – Jan 2023" starting with the word "host" and ending with the word "orange."

i. A seed phrase labeled "iphone 14 pro max – Feb 2023" starting with the word "produce" and ending with the word "property".

j. A seed phrase labeled "iphone 14 pro max – April 2023" starting with the word "soldier" and ending with the word "kind".

k. A seed phrase labeled "iphone 8 imtoken 11/30/2023" starting with the word "fame" and ending with the word "art".

l. A seed phrase labeled with unknown characters and "Metamask" starting with the word "art" and ending with the word "volume".

m. A seed phrase labeled with unknown characters and "Wallet" starting with the word "image" and ending with the word "such".

n. A seed phrase labeled "imtoken windy2" starting with the word "easily" and ending with the word "finish".

o. A seed phrase labeled "imtoken fcbqs" starting with the word "crash" and ending with the word "soccer".

p. A seed phrase labeled "Trust Wallet" starting with the word "company" and ending with the word "office".

q. A seed phrase labeled "TronLink Xutq1989" starting with the word "rather" and ending with the word "frequent".

r. A seed phrase labeled "MetaMask Xutq1989" starting with the word "caution" and ending with the word "mention".

s. A seed phrase labeled "mtc" starting with the word "produce" and ending with the word "spirit".

t. A seed phrase labeled "Coinbase wallet" starting with the word "tone" and ending with the word "crowd".

u. A seed phrase labeled "TokenPocket" starting with the word "desk" and ending with the word "husband".

v. A seed phrase labeled "TronLink" starting with the word "blouse" and ending with the word "glass".

(hereinafter, collectively referred to as the "Subject Wallets").

5. Based on my training and experience and the facts as set forth in this affidavit, I submit that there exists probable cause to believe that the funds contained in the Subject Wallets constitute proceeds of a "pig butchering" fraud scheme or were involved in the commission of a fraudulent offense, in violation of Title 18, United States Code, Sections 1956 (laundering of monetary instruments and conspiracy to commit money laundering) and 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and therefore are:

a. Subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A) and 19 U.S.C. §§ 1607-09 by 18 U.S.C. § 981(d); and

b. Subject to seizure via a civil seizure warrant under 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).

Background on Cryptocurrency

6. Based on my training, research, education, and experience, I know that cryptocurrencies are different from traditional currencies in that cryptocurrencies are not issued by or backed by any government. In addition, cryptocurrency accounts and wallets are different from traditional bank accounts in that these accounts are held in digital format in one of any number of various types of digital wallets or exchanges. Likewise, cryptocurrency is accessible only by the account holder or someone who has access to the account password or account "recovery seed phrase," a mnemonic passphrase made up of a series of words, or in some circumstances, by the company hosting the virtual wallet containing the cryptocurrency. Account holders have the ability to send and receive cryptocurrency using a unique and complex wallet address, often referred to as the private key.

7. Based on my training, research, education, and experience, as well as conversations with other investigators with specifically related training and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat

currency to buy goods or services or exchanged for fiat currency[1] or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, Ethereum, and Tether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

b. Tether is an alternative type of cryptocurrency or altcoin token. Payments or transfers of value made with Tether are recorded in the blockchain network, but unlike decentralized cryptocurrencies like bitcoin, Tether has some anatomical features of centralization. One centralized feature is that Tether is a stablecoin or a fiat-collateralized token that is backed by fiat currencies, or currencies issued by governments like the dollar and euro. Tether is backed with a matching one to one fiat

[1] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

amount, making it much less violate than its counterpart, bitcoin. Due to Tether's stable nature, wallet holders typically use a fundamental strategy to hedge their cryptocurrency holdings into Tether to hedge their receipt or earnings value, so it is not affected by the rest of the volatile cryptocurrency market. "TetherUS" (USDT), also referred to a "Tether," is a cryptocurrency purportedly backed by United States dollars. Tether was originally designed to always be worth $1, and the company responsible for issuing Tether purportedly maintained $1 in reserves for each Tether issued. As of January 1, 2024, one Tether coin was worth approximately $1 USD.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26-36 characters long. Each public address is controlled and/or accessed using a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address's private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Although cryptocurrencies such as bitcoin and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal

purposes such as money laundering and is an oft used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track the flow of victims' funds.

e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including 1) on a tangible, external device ("hardware wallet"), 2) downloaded on a PC or laptop ("desktop wallet"), 3) with an Internet-based cloud storage provider ("online wallet"), 4) as a mobile application on a smartphone or tablet ("mobile wallet"), 5) printed public and private keys ("paper wallet"), and 6) as an online account associated with a cryptocurrency exchange.

Facts Supporting Findings of Probable Cause

8. Since on or around September of 2021, the United States Secret Service and the Federal Bureau of Investigation (the "Investigating Agencies") have been investigating a fraud scheme being used to steal fiat currency and cryptocurrency from individuals located throughout the United States. The scheme utilizes the social engineering of victims who independently navigate on the Internet to platforms for stock and or cryptocurrency investment advice. While on these platforms, the "threat actors" purporting to be investment experts convince these victims to navigate to specific website URLs where they download fraudulent investment platforms to their electronic devices. The fraudulent investment platforms appear to be legitimate cryptocurrency exchanges where the victims can log in and see their investments grow. However, as soon as the victims send their cryptocurrency, the

funds begin making their way through a complex laundering scheme. Since at least February 2021, victims of the scheme have been convinced to transfer custody of their cryptocurrency and/or fiat currency to the Target Subjects under the guise of customer deposits to these cryptocurrency exchanges. The victims later discovered they were unable to withdraw funds they deposited to their accounts, and in some cases, they were extorted for more cryptocurrency or fiat currency when attempting to withdraw. On 12/13/2023, FBI Agents executed a search warrant issued out of the Eastern District of Texas to search 1039 Echols Drive, Frisco, TX 75306, the "SUBJECT PREMISES". The affidavit in support of that warrant is attached as Exhibit 1 and incorporated herein. At this time, the FBI has identified approximately 120 victims with losses of approximately $9,547,180 associated with this scheme.

9. The following items were located at the SUBJECT PREMISES and identified as belonging to Feng Chen:

a. Numerous documents for Feng Chen.

b. A notebook containing the word "clex"[2] followed by two entries of the cryptocurrency, Tether, commonly known as "USDT" valued at 16643 USDT and 26049 USDT. The same notebook contained a page labeled "BFEX" that

[2] CLEX LTD. is a company that was listed as the subscriber on the GoDaddy account that registered the domain bf-ex.com and many other fraudulent cryptocurrency exchange domains used in pig butchering schemes.

contained IP addresses with passwords, appearing to be root credentials to servers.

c. An external hard drive containing numerous folders with source code for websites inside compressed zip folders. There is a folder named "bnbdt-backend-master.zip" and a folder named "bnbdt-frontend-main.zip".

d. A folder labeled "BFEX" that contains the source code for the website, "bf-ex.com".

e. Three notebooks containing handwritten cryptocurrency wallet seed phrases for MetaMask[3], imToken[4], Token Pocket[5], Trust Wallet[6], and TronLink[7].

10. On 1/8/2024, Chen, Xu and their two children received new Chinese passports that expire on 1/8/2026 from the Chinese Consulate in Houston, TX. That same day, Chen purchased tickets for his family to travel to China and they all departed the United States on 1/11/2024.

11. Because law enforcement is now in possession of the recovery seed[8] (also sometimes referred to as mnemonic phrase, root key, backup phrase, or private key) for the

[3] MetaMask is a non-custodial web and mobile cryptocurrency wallet used to interact with the Ethereum blockchain.

[4] imToken is a non-custodial mobile cryptocurrency wallet with multi-chain support.

[5] Token Pocket is a multi-chain decentralized mobile cryptocurrency wallet.

[6] Trust Wallet is a web and mobile cryptocurrency wallet with multi-chain support.

[7] TronLink is a web and mobile cryptocurrency wallet for the Tron blockchain.

[8] A "recovery seed" is a mnemonic passphrase made up of 12 random words. It acts as a backup, ensuring that the wallet's funds can always be accessed. Anyone with the "recovery seed" can gain access to and control the wallet's funds. The recovery seed is a root key, sometimes referred to as a root seed, recovery seed, or mnemonic seed. A root key is a back-up key to the private key and allows a wallet owner to re-generate a new key pair for the corresponding wallet, offline and outside of the company or software that originally generated it. After re-generating the wallet with a root key, the possessor of the new wallet now has the ability to send and receive the value (in this example, cryptocurrency) associated

Subject Wallets as described in paragraph 5 and Attachment A, I know that those particular wallet/exchange balances can be "recovered" or "reconstituted". Law enforcement would transfer the available account balances as seized assets out of the wallets controlled by Chen and into custody in wallets controlled by law enforcement. Based on the location of the seed phrases with other materials related to the scheme and the absence of any indications of legitimately earned cryptocurrency associated with the seed phrases, I believe funds contained within the Subject Wallets would be subject to forfeiture.[9] This warrant therefore seeks authority to seize the funds within the warrants by accessing the wallets with the seed phrases and transferring the fund within the wallets to wallets under law enforcement control.

Conclusion

12. Based on the facts and circumstances set forth in this affidavit, I submit that there exists probable cause to believe that the funds contained in the Subject Wallets constitute proceeds of a "pig butchering" fraud scheme or were involved in the commission of a fraudulent offense, in violation of Title 18, United States Code, Sections 1956 (laundering of monetary instruments and conspiracy to commit money laundering) and 1957 (engaging in monetary transactions in property derived from specified unlawful activity), and therefore are:

a. Subject to civil forfeiture under 18 U.S.C. § 981(a)(1)(A) and 19 U.S.C. §§ 1607-09 by 18 U.S.C. § 981(d); and

---

with the original key pairs using the new private key created by the root key or "recovery seed."

[9] It isn't possible to know if Chen has stored the seed phrases anywhere other than in the notebooks recovered by law enforcement.. He wrote a few of the seed phrases in more than one notebook. Thus, it is possible the Subject Wallets will have been drained of funds by the time of any execution of the requested warrant.

b. Subject to seizure via a civil seizure warrant under 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).

I respectfully request that the Court issue the requested warrant to authorize law enforcement agents to seize the funds in the Subject Wallets by using the available username and/or login information, and recovery seed (mnemonic phrase, root key, backup phrase, or private key) in their lawful possession to recover and reconstitute the Subject Wallets onto a different digital device and subsequently transfer all available cryptocurrency associated with the Subject Wallets to a wallet controlled by law enforcement.

/s/ Justin Woodford
Justin Woodford, FBI Special Agent

Sworn to by the applicant via reliable electronic means under Federal Rule of Criminal Procedure 4.1(b)(2)(A)—specifically, a video call—on this 6th day of February, 2024.

Kevin J. Doyle

HON. KEVIN J. DOYLE
United States Magistrate Judge
District of Vermont