

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANT

I, Leah Bogdanowicz, having been duly sworn on oath, state as follows:

Affiant's Background

1. I have been employed as a Special Agent with the Federal Bureau of Investigation (FBI) since December of 2021. I am currently assigned to FBI's Albany Office, investigating cybercrimes including computer intrusions and fraud related crimes. I also have experience working counterintelligence matters. As a Special Agent with the FBI, I have received training related to cyber security and open-source intelligence. I have participated in the execution of search warrants involving physical and 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 warrant, 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 warrant.
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 an application for a warrant to seize all Tether (USDT) in the cryptocurrency wallet with address 0x90E16E6FBaAfd644ea9020B7B49DF08da90118b8 (“0x90”). The wallet 0x90 will be referred to as the SUBJECT WALLET. The USDT within the SUBJECT WALLET is the SUBJECT PROPERTY. As of April 18, 2024, the SUBJECT PROPERTY was described as 36,552 USDT, with a value of \$36,552, contained within the SUBJECT WALLET.

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 SUBJECT PROPERTY constitutes proceeds of a “pig butchering¹” fraud scheme or was involved in the commission of a fraudulent offense, in violation of Title 18, United States Code (U.S.C), 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 is:

- a. Subject to civil forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) and subject to seizure via a civil seizure warrant pursuant to 18 U.S.C. § 981(b)(1), and

¹ According to chainalysis.com, “Romance scams, also known as ‘pig butchering scams’ for the way bad actors say they ‘fatten up’ their victims to extract the most possible value, are a large and growing problem with a significant crypto nexus. Romance scammers start by building a relationship over time with the victim (usually of a romantic nature, as the name implies), often initiating contact by pretending to have text messaged a wrong number or via dating apps. As the relationship deepens, the scammer will eventually push the victim to invest money (sometimes cryptocurrency, sometimes fiat) in a fake investment opportunity, and continue to do so until they eventually sever contact.”

- b. Subject to criminal forfeiture under 18 U.S.C. § 982(a)(1) and subject to seizure via a criminal seizure warrant pursuant to 21 U.S.C. §§ 853(e) and (f) by 18 U.S.C. § 982(b)(1).
6. This affidavit requests that the Court issue a warrant allowing law enforcement to seize the SUBJECT PROPERTY and transfer it to a wallet controlled by law enforcement.

BACKGROUND

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 currency² to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin (“BTC”), Ethereum (“ETH”), and Tether (“USDT”). 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 in section b 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 (i.e. Kraken, Gemini), or through other intermediaries. Most cryptocurrencies have a

² Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen. 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.

“blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.³ Cryptocurrency is not illegal in the United States (US).

- b. 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.
- c. Bitcoin (“BTC”) is the first decentralized cryptocurrency, created in 2009 to facilitate instant payments without central oversight. It uses peer-to-peer

³ 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.

technology and cryptography to record transactions in a public ledger, called a blockchain, without central oversight.

- d. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. Dollar, or to a different virtual currency. For example, USDC is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.
- e. “TetherUS” (USDT), also referred to as “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. Tether Limited (“Tether”) is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens.
- f. Although cryptocurrencies such as BTC, ETH, and USDT 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.

Facts Supporting Findings of Probable Cause

8. Since August 2023, the FBI has been investigating a fraud scheme being used to steal currency and cryptocurrency from individuals located throughout the United States. The scheme utilizes social engineering to lure victims into cryptocurrency investment via either directly messaging the victim through a messaging platform to discuss such investments or as a "wrong number" message that ends up leading into an investment discussion. Through discussions, the "threat actors," or Target Subjects, purporting to be investment experts, convince these victims to exchange US dollars into cryptocurrency on a legitimate cryptocurrency exchange (i.e. Kraken, Gemini) and then instruct the victims to navigate to a specific website (i.e. www.safepal6.com), where the victims have a view of a fraudulent investment platform on 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 January 2023, victims of the scheme have been convinced to transfer custody of their cryptocurrency 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 when attempting to withdraw. This scheme is known as pig butchering.

The Subject Property

9. The initial victim, Victim 1, is a Vermont resident who lost approximately \$746,000 US dollars to the scheme detailed in paragraph 8, between February and April 2023. Victim 1 provided their initial transactions from Kraken, a known cryptocurrency exchange. Each of the initial cryptocurrency purchases were in USDT on the Ethereum (ERC-20) blockchain. Through blockchain analysis, the victim funds were traced in USDT by investigators to the SUBJECT WALLET. Between February and April 2023, up to 611,223 USDT of Victim 1's funds were deposited to the SUBJECT WALLET, which is equal to approximately \$611,223 US dollars. Various withdrawals and peer-to-peer exchanges occurred between February 2023 and April 18, 2024, resulting in a balance in the SUBJECT WALLET on April 18, 2024 of 36,552 USDT, or a value of approximately \$36,552 US dollars.

10. Per email conversations with a representative from Tether, a preceding wallet address that transferred money to the SUBJECT WALLET also conducted withdrawals to six different addresses between April 18 and April 19, 2023. In addition, multiple subsequent deposits to and withdrawals from the SUBJECT WALLET occurred after the last transfer of Victim 1's funds. This activity is consistent with the cryptocurrency crime known as pig butchering. Through blockchain analysis, at least two preceding wallets through which victim funds had moved transferred USDT into the SUBJECT WALLET.

11. Based on my conversations with other federal agents familiar with investigating cryptocurrency crimes, multiple sender wallets and deposit wallets are trends that are indicative of

digital money laundering due to the intentional obfuscation of funds. Further, records for the SUBJECT WALLET show many same day deposits and withdrawals. Based on my training and experience and conversations with other agents working in cryptocurrency, these patterns are also consistent with pig butchering.

12. As stated in paragraph 10 above, almost all the USDT, including the USDT transferred from Victim 1, had been moved out of the SUBJECT WALLET as of April 18, 2024. However, the SUBJECT WALLET still contained the SUBJECT PROPERTY, 36,552 USDT, or a value of approximately \$36,552 US dollars, on that date.

13. On April 18, 2024 and April 19, 2024, the Federal Bureau of Investigation and the United States's Attorney's Office for the District of Vermont requested Tether voluntarily restrain the funds in the SUBJECT WALLET such that they could not be further transacted. On April 20, 2024, Tether confirmed it had frozen the SUBJECT PROPERTY at a value of 36,552 USDT, or a value of approximately \$36,552 US dollars, on that date.

14. Based on my training and experience and the information set forth above, I believe the SUBJECT PROPERTY constitutes all Tether in the SUBJECT WALLET and is the proceeds of and involved in money laundering. The SUBJECT PROPERTY is therefore subject to seizure and forfeiture.

Conclusion

15. Based on the facts and circumstances set forth in this affidavit, my training and experience, and information conveyed to me based on the training and experience of other agents working on cryptocurrency frauds, I submit that there exists probable cause to believe that SUBJECT PROPERTY constitutes the proceeds of a "pig butchering" fraud scheme or was

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 is:

- a. Subject to civil forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and (a)(1)(C) and subject to seizure via a civil seizure warrant pursuant to 18 U.S.C. § 981(b)(1), and
- b. Subject to criminal forfeiture under 18 U.S.C. § 982(a)(1) and subject to seizure via a criminal seizure warrant pursuant to 21 U.S.C. §§ 853(e) and (f) by 18 U.S.C. § 982(b)(1).⁴

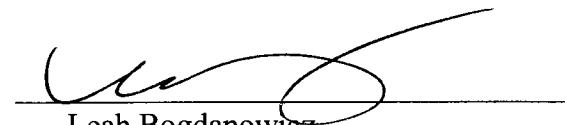
Should this seizure warrant be granted, law enforcement intends to work with Tether to seize the funds associated with the SUBJECT PROPERTY. In sum, the accompanying warrant would be transmitted to Tether, at which time Tether would “burn” (*i.e.*, destroy) the addresses at issue (and by extension the USDT tokens associated with them). Tether would then reissue the equivalent amount of USDT tokens associated with the SUBJECT PROPERTY and transfer that equivalent amount of USDT to the government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of the forfeiture proceedings, to ensure that access to, or manipulation of, the forfeitable property cannot be made

⁴ 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it “determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture.” In this case, a protective order for the SUBJECT PROPERTY would not ensure the property’s availability for forfeiture. The SUBJECT PROPERTY is already voluntarily frozen by Tether. By issuing the seizure warrant, the Court may best ensure the property is available for forfeiture proceedings and begin formal procedures for claims against the property.

absent court order or, if forfeited to the United States, without prior consultation by the United States.

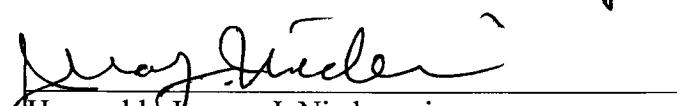
16. Because this warrant seeks only permission to seize funds controlled by Tether and does not involve the physical intrusion onto a premises, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Dated at Burlington, Vermont on this 29 day of August 2024.



Leah Bogdanowicz
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August 29, 2024



Honorable Jerome J. Niedermeier
UNITED STATES MAGISTRATE JUDGE