United States District Court

EASTERN District of **CALIFORNIA**

In the Matter of the Seizure of
(*Briefly describe the property to be seized*)

Up to 0.5 Bitcoin, held by ChangeNow, for an attempted cryptocurrency swap identified as ID 90efae6ccaf877, to an account with an address beginning with 3JQfvk.

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

CASE NUMBER: 2:24-sw-0408 JDP

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Country of SAINT VINCENT AND THE GRENADINES is subject to forfeiture to the United States of America (*describe the property*):

Up to 0.5 Bitcoin, held by ChangeNow, for an attempted cryptocurrency swap identified as ID 90efae6ccaf877, to an account with an address beginning with 3JQfvk.

The property is subject to seizure pursuant to 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C), concerning violations of 18 U.S.C. § 1343.

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

/s/ Austin Miller
Applicant's signature

Austin S. Miller, Special Agent, USSS
Printed name and title

Sworn to before me and signed telephonically.

April 22, 2024
Date

Judge's signature

Sacramento, California
City and State

Jeremy D. Peterson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEIZURE WARRANTS

I, Austin S. Miller, having been duly sworn, depose and state as follows:

INTRODUCTION AND PURPOSE OF AFFIDAVIT

1. This affidavit is submitted in support of applications for issuance of seizure warrants for the funds transferred illegally in separate transactions, into two cryptocurrency exchange accounts held at ChangeNow cryptocurrency exchange (collectively, the "**Subject Addresses**"), to wit:

   a. Up to 0.5 Bitcoin, held by ChangeNow, for an attempted cryptocurrency swap identified as ID 90efae6ccaf877, to an account with an address beginning with ***3JQfvk*** ("**Subject Address A**"); and

   b. Up to 0.54282417 Bitcoin, held by ChangeNow, for an attempted cryptocurrency swap identified as ID 379c7c7a0ca0c2, to an account with an address beginning with ***3GLT2r*** ("**Subject Address B**").

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that unknown subject(s) ("UNSUB") have violated Title 18, United States Code, Section 1343 (Wire Fraud), and that the **Subject Addresses** contain the proceeds of UNSUB's participation in the wire fraud activity described below. The **Subject Addresses** are accordingly subject to seizure pursuant to 18 U.S.C. § 981(b) and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

3. The facts in this affidavit come from my personal observations and knowledge, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested

warrants and does not set forth all of my knowledge about this matter. All dates are on or about the date specified. All amounts are approximate.

AFFIANT BACKGROUND

4. I am a Special Agent ("SA") with the United States Secret Service ("USSS") and have been so employed since November 2020. The USSS is the primary investigative agency charged with safeguarding the payment and financial systems of the United States. I am currently assigned to the San Francisco Field Office.

5. In my capacity as a Special Agent, I attended and completed the eighteen-week USSS Special Agent Training Course at the James J. Rowley Training Center in Beltsville, Maryland. This program included comprehensive, formalized instruction in, among other things: fraud investigations, counterfeit identification and detection, familiarization with United States' fraud and counterfeit laws, financial investigations and money laundering, identification and seizure of assets, physical and electronic surveillance, and undercover operations. In my capacity as a Special Agent, I have also completed approximately 480 hours of academic and practical training at the Federal Law Enforcement Training Center in the Criminal Investigator Training Program. Furthermore, I have completed 120 hours of additional training in the DFIR-NI (Digital Forensics Incident Response) dedicated to instructing agents on how computers and devices are used to facilitate criminal activity via means of network intrusion, including how to investigate these incidents.

6. During my time in federal law enforcement, I have participated in criminal investigations. This casework has involved investigation into the unlawful takeover of financial accounts, business email compromise schemes, network intrusions, counterfeit currency investigations, and protective intelligence investigations.

7. The facts in this affidavit come from my personal observations and knowledge, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

APPLICABLE STATUTORY AUTHORITY

8. Title 18, United States Code, Section 1343, makes it a crime to knowingly execute, or attempt to execute, a scheme or artifice to (1) obtain money or property by means of false or fraudulent pretenses, representations, or promises; (2) that are material; (3) with the intent to defraud; and (4) where the defendant used, or caused to be used, a wire communication to carry out or attempt to carry out an essential part of the scheme.

9. Title 18, United States Code, Section 981(a)(1)(C) provides that "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable" to the violation of an enumerated statute constituting a specified unlawful activity "is subject to forfeiture to the United States." Specified unlawful activities are detailed therein, as well as at Title 18, United States Code, Sections 1956(c)(7) and 1961(1), which enumerates Title 18, United States Code, Section 1343 as a specified unlawful activity.

10. Title 18, United States Code, Section 981(b) provides that seizures executed for purposes of civil forfeiture shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under the Federal Rules of Criminal Procedure. Moreover, seizure warrants may be issued in any district in which a forfeiture action may be filed and may be executed in any district in which the property is found. Federal Rule of Criminal Procedure 41 governs the issuance of criminal search and seizure warrants.

11. Under 18 U.S.C. § 981(b), any property subject to forfeiture under 18 U.S.C. § 981(a) may be seized by the Attorney General pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure. Section 981(b)(3) further states that, notwithstanding the provisions of Rule 41(a), a seizure warrant may be "transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement."

12. Section 981(b)(3) of Title 18 provides that a seizure warrant may be issued by a "judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C. § 1355(b)] and may be executed in any district in which the property is found […]."

13. Based on my training, experience, and the information contained in this affidavit, there is probable cause to believe that funds in the Subject Addresses are subject to forfeiture as proceeds traceable to a wire fraud scheme, pursuant to Title 18, United States Code, Section 981(a)(1)(C).

BACKGROUND ON CRYPTOCURRENCY AND VIRTUAL CURRENCY EXCHANGES

14. **Virtual Currencies:** Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. Dollar, but are generated and controlled through computer software. Bitcoin ("BTC") is currently the most well-known virtual currency in use.

15. **Virtual Currency Addresses:** Virtual currency addresses are the specific virtual locations of the electronic accounts to which such currencies are sent and received. An address is analogous to a bank account number and is represented as a string of letters and numbers up to

40 characters long. Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, needed to access the address. Users can operate multiple addresses at any given time, with the possibility of using a unique address for every transaction. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), 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 all their transactions on what is known as a "blockchain." The blockchain is essentially a distributed public record or ledger, run by a decentralized network, for a specific virtual currency. There are different blockchains for different types of virtual currencies. The blockchain for each virtual currency contains an immutable and historical record of every transaction executed utilizing that currency's blockchain technology, that is to say, it maintains a record of every transaction executed with a particular virtual currency. It also records the address of every virtual currency account that ever received that particular currency and maintains records of all the known balances of that currency for each virtual currency address. The blockchain can be updated multiple times per hour.

17. **Virtual Currency Wallet:** A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain. The virtual currency wallet generates and stores a user's accounts' addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies from their accounts. Multiple addresses can be

stored in a wallet. Users' wallets can be either "custodial wallets" or "non-custodial wallets." Custodial wallets are managed by centralized businesses which retain an account holder's private keys and execute the transactions the user asks the host business to execute. Custodial wallets are also referred to as "hosted" wallets. Non-custodial wallets are managed by the account holder directly, retaining their own private keys and full control over the account. Non-custodial wallets are also referred to as "unhosted" wallets.

18. ChangeNow is a decentralized cryptocurrency exchange that receives cryptocurrency for the purpose of swapping, or converting, the funds into a different cryptocurrency. It provides a non-custodial service. ChangeNow is part of CHN Group LLC, a company incorporated in Saint Vincent and the Grenadines.

FACTS SUPPORTING PROBABLE CAUSE

19. On March 13, 2024, an individual (referred to herein as "D.J."), a resident of Vallejo, California, suffered an account takeover of his cryptocurrency wallets, resulting in the unauthorized transfer out of his cryptocurrency accounts of nearly $654,000 U.S. Dollar Equivalent ("USDE") in BTC.

20. On March 13, 2024, DJ contacted the USSS San Francisco Field Office to report the theft. DJ reported that he had received a call from UNSUB, who claimed to be an employee of Coinbase, a cryptocurrency exchange. UNSUB stated that "Coinbase" had identified fraudulent activity on D.J.'s account and told D.J. that he must 'cancel transactions' by clicking a link that UNSUB would send via text message. DJ received a call not long after from another UNSUB, claiming to work for Gemini, another cryptocurrency exchange, also stating that UNSUB had noted suspicious activity on D.J.'s account. UNSUB told DJ that D.J.'s account had been frozen and that he needed to 'accept a push notification,' which UNSUB said he would send, to verify that DJ was the legitimate accountholder before continuing to assist him. DJ reported that he recalls a two-factor authentication prompt appearing on his screen, the

acceptance of which allowed UNSUB access to his account at Gemini. DJ also reported that he took a picture of seed phrases belonging to his unhosted wallet during the scam, but did not pass that information or image to UNSUB. The unhosted wallet was also compromised, however. At the time of the attack, DJ's wallets contained BTC worth approximately $654,000. DJ only became aware of the theft when he checked his wallets later in the evening of March 13, and saw that the accounts were empty.

21. The crime perpetrated against DJ is a known form of "phishing," or deception intended to obtain access credentials to unsuspecting victims' wallets. Some accounts have a single security layer, which an account holder can pass with a username and password, typically. This is "single-factor authentication." "Two-factor authentication" is a security system that requires two separate, distinct forms of identification in order to access something. The first factor is a username/password and the second commonly includes a 'yes' or 'no' prompt sent to an account holder's smartphone. By means of deception, a criminal actor is able to defeat two-factor authentication to cryptocurrency accounts by deceiving the victim into accepting a prompt on their own device and unintentionally allowing the criminal actor's device the ability to access and control the account. It is likely that DJ was speaking with and deceived by a criminal actor who was not actually a representative of Coinbase or Gemini.

22. Beginning on March 13, 2024, the USSS began efforts to trace the cryptocurrency transferred out of D.J.'s accounts, identify the responsible actors, and effect recovery, if possible.

23. Based on blockchain data, investigators determined that, on March 13, 2024, between 9:07:37 and 9:47:44 UTC, multiple cryptocurrency wallets belonging to DJ were accessed and used to send approximately 7.08614758 BTC (USDE $506,162), to a BTC address beginning with "*bc1qst*," which did not belong to D.J.

24. Later the same day, the *bc1qst* address transferred 3.54303941 BTC (USDE $253,079), to an address beginning with *bc1qgn*.

25. The *bc1qgn* address then began initiating multiple transfers in 0.5 BTC increments to ChangeNow. A review of ChangeNow records revealed that the UNSUB was

swapping, or converting, the stolen BTC for a different cryptocurrency, called Monero ("XMR"). XMR is what is known as a 'privacy coin' and is, by design, meant to be untraceable. Crypto thieves often use XMR in cryptocurrency thefts because its anonymity makes it difficult to trace.

26. USSS then advised ChangeNow that stolen funds were being sent to ChangeNow via the account beginning with *bc1qgn*. With this information, ChangeNow was able to freeze further incoming swap attempts before they could then be converted into XMR and transferred out of ChangeNow's control.

27. The next day, March 14, 2024, at 4:21:29 UTC, 0.5 BTC was sent from *bc1qgn* to an address beginning with *3JQfvk* (**Subject Address A**). ChangeNow has frozen these funds. These funds, associated with **Subject Address A**, are directly traceable as proceeds of the theft from DJ's accounts.

28. On March 14, 2024, at 20:54:25 UTC, 0.542782417 BTC was sent from the *bc1qgn* address to an address beginning with *3GLT2r* (**Subject Address B**). ChangeNow also has frozen these funds. These funds, associated with **Subject Address B**, are directly traceable as proceeds of the theft from DJ's accounts.

29. In summary, the USSS' investigation has determined that the *bc1qgn* address was only ever used to receive funds from the theft of DJ's funds and then to send those funds to the **Subject Addresses**. The transactions associated with the **Subject Addresses** appear to have been part of a series of transactions conducted in an attempt to obfuscate the illicit source of the funds and the balance of **Subject Addresses** represents the proceeds of wire fraud.

CONCLUSION

30. Based on information derived from the foregoing investigation, there is probable cause to believe that the **Subject Addresses** contain the proceeds of a wire fraud scheme executed in violation of Title 18, United States Code, Section 1343. Those proceeds, which include 0.5 BTC ($34,078.35 USDE) from **Subject Address A**, and 0.54282417 BTC

($36,995.37 USDE) from **Subject Address B**, are subject to seizure pursuant to 18 U.S.C. § 981(b) and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C). Accordingly, I respectfully request that warrants be issued authorizing the seizure of the Subject Addresses.

/s/ Austin Miller
Austin S. Miller
Special Agent
United States Secret Service

Reviewed and approved as to form:

/s/ Kevin C. Khasigian
James Connoly
Kevin C. Khasigian
Assistant U.S. Attorneys

Sworn before me and signed telephonically
on this 22nd day of April 2024.

Hon. Jeremy D. Peterson
United States Magistrate Judge

United States District Court

EASTERN District of **CALIFORNIA**

In the Matter of the Seizure of
(*Briefly describe the property to be seized*)

Up to 0.5 Bitcoin, held by ChangeNow, for an attempted cryptocurrency swap identified as ID 90efae6ccaf877, to an account with an address beginning with 3JQfvk.

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

CASE NUMBER: 2:24-sw-0408 JDP

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Country of SAINT VINCENT AND THE GRENADINES be seized as being subject to forfeiture to the United States of America. The property is described as follows:

Up to 0.5 Bitcoin, held by ChangeNow, for an attempted cryptocurrency swap identified as ID 90efae6ccaf877, to an account with an address beginning with 3JQfvk.

The property is subject to seizure pursuant to 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property within 14 days in the daytime 6:00 a.m. to 10:00 p.m. You must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to JEREMY D. PETERSON or Any U.S. Magistrate Judge in the Eastern District of California.

April 22, 2024 at 3:51 p.m.
Date and Time Issued

Judge's signature

Sacramento, California
City and State

Jeremy D. Peterson, U.S. Magistrate Judge
Printed name and title

RETURN

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Subscribed, sworn to telephonically, and returned before me this date.

_____
U.S. Judge or Magistrate

_____
Date