AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
5/25/2024
CENTRAL DISTRICT OF CALIFORNIA
BY: VV DEPUTY

United States of America

v.

Tyler Robert Buchanan,

Defendant(s)

Case No. 2:24-mj-03081-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than June 2022 to at least December 2022, in the County of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1349	Wire Fraud Conspiracy
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. §1028A	Aggravated Identity Theft

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/

Complainant's signature

Jeremy Durk, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 5/25/2024

Judge's signature

City and state: Los Angeles, California

Hon. Margo A. Rocconi, U.S. Magistrate Judge

Printed name and title

AUSA: Sue J. Bai, [redacted]

AFFIDAVIT

I, JEREMY DURK, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed in this position since 2020. I am currently assigned to the Los Angeles Field Office. In the course of my duties, I am responsible for investigating criminal and national security matters, and have investigated crimes involving cyber attacks, computer intrusions (hacking), online fraud, and cryptocurrency. Based on my training and experience, I know that criminal violations are often associated with these activities, including conspiracy, wire fraud, computer fraud, identity theft, and money laundering.

2. Before joining the FBI, I worked in the field of information technology for approximately seven years and have extensive experience working with computers, databases, and network infrastructure. During my professional career, I have received both formal and informal training from the FBI and other institutions regarding computer-crime investigations and computer technology.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal complaint against and arrest warrant for TYLER ROBERT BUCHANAN ("BUCHANAN"), for violations of the following:

Wire Fraud Conspiracy	18 U.S.C. § 1349
Conspiracy to Obtain Information by Computer for Private Financial Gain to Access Computer to Defraud & Obtain Value	18 U.S.C. § 371, 18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(i), 18 U.S.C. § 1030(a)(4)
Wire Fraud (Victim E.V.)	18 U.S.C. § 1343
Wire Fraud (Victim J.L.)	18 U.S.C. § 1343
Aggravated Identity Theft	18 U.S.C. § 1028A

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

Further, all dates and amounts are approximate.

III. DEFINITIONS

5. I know from my training, experience, and research as a Special Agent with the FBI that the following definitions apply to the activity discussed in this affidavit.

6. **IP address**: An internet protocol address ("IP address") is a unique numeric address used by each computer on the internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178), or a series of eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:0000:0042:0000:8a2e:0370:7334). Every computer attached to the internet must be assigned an IP address so that internet traffic sent from and directed to that computer may be properly directed from its source to its destination.

7. **Domain**: A domain (short for domain name) is a website's electronic address on the Internet. Examples include www.justice.gov and www.uscourts.gov. Domains are used to help users navigate to websites more easily instead of having to use the site's IP address.

8. **Registration**: "Registration" is the act of reserving a domain on the Internet for a specific time period. In order to do so, the "domain registrant" would usually apply online to a company that managed the reservation of Internet domain names,

known as a registrar. A "registrar" operates in accordance with the guidelines of the designated organizations that manage top-level domains (e.g., ".com" or ".net"), known as registries.

9. **Cryptocurrency:** "Digital currency" or "virtual currency" is currency that exists only in digital form; it has the characteristics of traditional money, but it does not have a physical equivalent. Cryptocurrency, a type of virtual currency, is a 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 or other cryptocurrencies.[1] Bitcoin ("BTC") and ether ("ETH") are examples of cryptocurrency. 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 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. Most 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

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

by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

10. **Cryptocurrency address**: Cryptocurrency addresses are the particular virtual locations to which cryptocurrencies are sent and received. A cryptocurrency address is analogous to a bank account number and is typically represented as a case-sensitive string of letters and numbers.

11. **Cryptocurrency wallet**: A cryptocurrency wallet is an application that holds a user's cryptocurrency addresses and private keys. A cryptocurrency wallet also allows users to send, receive, and store cryptocurrency. It is usually associated with one or more cryptocurrency address(es).

12. **Seed Phrase**: A seed phrase is a sequence of random words that stores the data required to access or recover cryptocurrency. Seed phrases are generated by cryptocurrency wallet software and are crucial for the safety of digital assets. Many cryptocurrency thefts are facilitated by victims keeping their cryptocurrency seed phrases in online accounts, which are subsequently compromised.

13. **Blockchain**: Cryptocurrency transactions are typically recorded on what is known as a blockchain. A blockchain is

[2] Some cryptocurrencies operate on blockchains that are not public.

essentially a distributed public ledger that keeps track of all transactions involving a specific cryptocurrency. The blockchain records every cryptocurrency address that has ever received cryptocurrency and maintains records of every transaction and all the known balances for each cryptocurrency address. As a result, forensic analytical tools are able to review the blockchain, identify which cryptocurrency addresses are related and owned by the same individual or entity (called a cluster), and calculate the total amount of cryptocurrency in all of these related cryptocurrency addresses.

14. **Blockchain Explorer:** Blockchain explorers are tools used to view and explore all the information on a blockchain, including specific transactions and addresses involved in each transaction.

15. **Server:** A server is a computer or operating system that provides resources, data, services, or programs to other computers (commonly referred to as "clients") over a network. There are many types of servers, including web servers that provide content to web browsers, email servers that act as a post office to send and receive email messages, print servers, virtual private servers, and proxy servers.

16. **VPS:** A virtual private server is a virtual operating system that resides within a physical parent server and uses virtualization technology to provide dedicated, private

resources to other servers. A VPS runs its own copy of an operating system, and customers can have access to that operating system to install almost any software that runs on that operating system. For many purposes, a VPS is functionally equivalent to a dedicated physical server but, being software-defined, can be created and configured more easily. Many companies offer virtual private server hosting or virtual dedicated server hosting as an extension for web hosting services.

17. **SMS phishing:** Phishing is a cyber attack technique where the attacker sends a message to lure the recipient into clicking on a link (often to a website or program) and then provide sensitive information or download malicious software on to the recipient device. SMS phishing refers to a type of phishing that uses text messages, which are commonly sent over SMS (Short Message Service) channels but also can be sent using non-SMS channels like data-based messaging applications.

18. **Phishing website:** A phishing website is a website that is designed to appear like it is associated with a legitimate company or organization for the purpose of luring the victim into opening the website and/or providing sensitive information through the website. Phishing websites commonly have domain names that are similar to the domain names of the legitimate company or organization that they are trying to imitate.

19. **Phishing kit:** A phishing kit is a collection of software tools that makes it easier for people with limited technical skills to launch a phishing attack. Phishing kits make it easier for users to create phishing websites as well as to collect and organize information received from victims through those phishing websites.

20. **Hash value:** A hash value is a string of letters and numbers obtained by applying a mathematical function to a piece of data. Each data set has a unique hash value that is generated based on the specific information contained in the data set. When the hash value of one data set matches the hash value of another, this indicates that the data sets are identical to one another.

21. **SIM swapping:** SIM swapping is a type of account takeover fraud that generally targets weaknesses in authentication mechanisms of mobile telephones, allowing criminals to take over a victim's telephone and its communications. Criminals will generally change the SIM card (a physical or virtual memory storage device) that is associated with a telephone number with a SIM card that the criminals control. Once the SIM card is changed, the criminals can control the victim's telephone number.

22. **Social engineering:** Social engineering refers to deceptive techniques that are designed to convince another

person to reveal specific information or perform a specific action when the perpetrator would not otherwise have access to that information or action. Phishing is a type of social engineering technique.

IV. STATEMENT OF PROBABLE CAUSE

A. SMS Phishing Scheme Targeting U.S. Companies

23. Based on information provided by three victim companies, whose identities are known to the FBI (Victim Companies 1, 2, and 3), and publicly available information about those companies, I know the following information.

1. Victim Company 1

24. Victim Company 1 is a [redacted] company with offices in the Central District of California.

25. On June 2, 2022, Victim Company 1 employees in the Central District of California received SMS messages on their phones informing them that their accounts were about to be deactivated.

26. At least one of the SMS messages instructed the employee to navigate to a linked website with the domain "[Name of Victim Company 1]-okta.net" ("Phishing Domain 1") which appeared to be associated with Okta.[3]

[3] Okta is U.S. company that provides security services to authenticate employee or user identity and was at the time used by Victim Company 1 for this purpose.

27. At least one employee of Victim Company 1 navigated to the linked website, entered the employee's company credentials, and then authenticated the employee's identity through the two-factor authentication request sent to their phone.

2. Victim Company 2

28. Victim Company 2 is a [redacted] company with offices in the Central District of California.

29. Similar to Victim Company 1, on June 2, 2022, multiple employees of Victim Company 2 in the Central District of California received SMS messages on their phones, informing them that their accounts were about to be deactivated and instructing them to navigate to the linked website.

30. Victim Company 2 employees saw that the linked website appeared to be associated with Okta. The linked websites included a website with the domain "[Victim Company 2 Name]-vpn.net" ("Phishing Domain 2").

31. At least one employee of Victim Company 2 navigated to the linked website, entered the employee's company credentials, and then authenticated the employee's identity through the two-factor authentication request sent to their phone.

3. Victim Company 3

32. Victim Company 3 is a [redacted] company outside of the Central District of California.

33. As with Victim Company 1 and 2, on June 2, 2022,

multiple employees of Victim Company 3 received SMS messages on their phones, similarly informing them that their accounts were about to be deactivated. These SMS messages instructed the employees to navigate to a linked website with the domain "[Name of Victim Company 3]-okta.com," which also appeared to be associated with Okta.

34. At least one employee of Victim Company 3 navigated to the linked website, entered the employee's company credentials, and then authenticated the employee's identity through the two-factor authentication request sent to their phone.

B. Identification of BUCHANAN in the SMS Phishing Scheme

35. Domain registration records from NameCheap for Phishing Domain 1 and Phishing Domain 2 showed that both domains were registered under the same NameCheap account ("Subject NameCheap Account"), which had the username bobsagetfaget and listed the account email address as lululongstaffihw98@gmail.com ("Subject Gmail Account"). These records showed that both phishing domains were registered on June 2, 2022--the same date that Victim Companies 1, 2, and 3 were targeted in the phishing scheme described above.

36. Records from NameCheap for the Subject NameCheap Account also showed that the account was used to register other phishing domains with names that suggested that they were designed to similarly target additional telecommunication,

cryptocurrency exchange, social media, and technology companies.

37. The NameCheap records also showed that less than one month before the phishing attacks, on May 4, 2022, the Subject NameCheap Account was logged in from the IP address [redacted] ("BUCHANAN IP Address").

38. Virgin Media records showed that the BUCHANAN IP Address was leased to BUCHANAN from January 26, 2022 to November 7, 2022.

39. The FBI subsequently confirmed, based on information from the Police Service of Scotland ("Police Scotland"), that BUCHANAN was a U.K. citizen who was at that time living in Scotland, United Kingdom.

C. Evidence from Buchanan's Digital Devices Tied to Phishing Scheme, Hacking, and Cryptocurrency Theft

40. Based on information from Police Scotland and records from Virgin Media, in April 2023, Police Scotland searched the residence of BUCHANAN, located at the address associated with the BUCHANAN IP Address, and seized approximately twenty digital devices in connection with a separate investigation (collectively, "BUCHANAN's devices"). Between November 2023 and January 2024, the FBI obtained forensic copies of the desktop computers, laptop computers, external storage devices, and phones seized during the search. Two of the devices contained information relating to a proton email address that had been

used by BUCHANAN to book a flight, based on information provided by British Airways; this flight reservation was associated with BUCHANAN's true U.K. passport number, based on information provided by Police Scotland.

41. The internet browser history from one of BUCHANAN's devices showed that he accessed (i) a NameCheap registration and control panel page for Phishing Domain 2, which was used to target Victim Company 2; and (ii) the Subject Gmail Account, which was used to register the Subject NameCheap Account that in turn registered Phishing Domain 1, Phishing Domain 2, and many other apparent phishing domains as discussed above.

42. One of Buchanan's devices was found to contain a phishing kit. Based on my review, I believe that this phishing kit was a software program designed to capture information coming into a phishing website (like usernames and passwords) and then transmit that information to another database that could be accessed by the attackers. I analyzed the phishing kit found on BUCHANAN's device and determined that it was designed specifically to transmit the captured information to a Telegram channel.[4] Coconspirator 1 is an uncharged coconspirator with BUCHANAN. The FBI searched more than twenty digital devices, including computers, external storage devices, and phones

[4] Telegram is an end-to-end encrypted messaging application available on mobile devices and desktop computers.

belonging to Coconspirator 1 pursuant to a federal warrant. In one of the external storage devices, the FBI found usernames and passwords for employees of Victim Companies 1, 2, and 3 contained in Telegram data that had been exported to the device. Based on my training an experience, I assess that the presence of those usernames and passwords in Telegram data is consistent with those credentials being harvested by a Telegram-connected phishing kit like that found on BUCHANAN's device.

43. The hash value of the phishing kit on BUCHANAN's device matched the hash value of the phishing kits found on three virtual private servers that were used to host phishing websites, as further described below. The fact that these files all shared the same hash value indicates that they were exact copies of the same phishing kit.

a. During the investigation, the FBI obtained information from Digital Ocean pursuant to a search warrant for the following three virtual private servers: Server with IP Address [redacted] ("Subject Server 1"); Server with IP Address [redacted] ("Subject Server 2"); and Server with [redacted] ("Subject Server 3").[5]

b. Based on a review of the records for Subject

[5] Digital Ocean is a cloud service company based in the United States that provides virtual private servers to customers.

Servers 1, 2, and 3, and information from DomainTools,[6] the FBI determined that the servers were used to host the following domains during the corresponding time periods:

i. From June 15 to 16, 2022, Subject Server 1 hosted [victim company name]-okta.com, [victim company name]-vpn.com, [victim company name]-vpn.com, [victim company name]-okta.com, okta-[victim company name].com, [victim company name]-vpn.com, and [victim company name]-vpn.com.

ii. From June 3 to 6, 2022, Subject Server 2 hosted login[victim company login page name].tv.

iii. From July 22 to 25, 2022, Subject Server 3 hosted [misspelled victim company name]-okta.com, [victim company name]-sso.com, and [victim company name].com.

c. Based on my training and experience, publicly available information, and information obtained from victim companies in this investigation, I believe that these domains are phishing domains designed to appear like they belong to legitimate companies but are not actually associated with those companies.

44. Browser history on one of BUCHANAN's devices showed that the device was used to access administration and control panels for Subject Servers 1 and 3 on June 14 and July 22, 2022.

[6] DomainTools is a service that provides historical information on registered domains, including the associated IP addresses.

A database found on Subject Server 1 contained employee credentials for several U.S.-based companies, including a social media company, an email marketing company, a software company, and a venture capital firm, as well as an Indian information technology company.

45. Records from Bitlaunch[7] show that Subject Server 2 was accessed using IP address [redacted] on June 3, 2022 (one day after the phishing attacks discussed above). On the same day, the Subject NameCheap Account was also accessed from this same IP address. These accesses from the same IP address on the same day indicate that the same person or persons who controlled Subject Server 2 also controlled the Subject Namecheap Account.

46. Records from Bitlaunch show that Subject Server 2 was paid for using a cryptocurrency address. Discord records show that the same address was listed in a message that Coconspirator 1 sent in a chatroom with no other participants.

47. BUCHANAN's digital devices held multiple files containing information from potential victim companies. These included an export of what appeared to be the [redacted] of a large U.S.-based telecommunication company as well as [redacted] from a U.S. cryptocurrency exchange.

48. Browser history on BUCHANAN's device showed that he

[7] Bitlaunch is VPS provider that accepts payment in cryptocurrency for VPS services provided by other companies, including Digital Ocean, Vultr, and Linode.

visited the management consoles for multiple phishing websites, as well as the login page of an email account belonging to an employee of a company that provides call center services.

49. The browser history also indicated numerous attempts to connect to companies targeted in the phishing attacks, including telecommunication and software companies based in the United States.

50. The FBI's investigation to date has gathered evidence showing that BUCHANAN and his coconspirators targeted at least 45 companies in the United States and abroad, including Canada, India, and the United Kingdom.

51. One of BUCHANAN's devices contained a screenshot of Telegram messages between an account known to be used by BUCHANAN and other unidentified coconspirators discussing dividing up the proceeds of SIM swapping. Based on my training and experience, I know that criminals engage in SIM swapping to gain access to a victim's phone number so that the criminal can intercept or access any code or password sent to that phone number. This allows the criminal to use the code or password to access victim accounts, including email, bank, credit card, and cryptocurrency accounts.

52. BUCHANAN's digital devices also contained communications with Coconspirator 1, including Telegram messages where Buchanan provided information about potential victims to

target for cryptocurrency theft, as further discussed below.

D. Hacking Companies to Steal Customer Information and Cryptocurrency

53. Based on information [redacted], the purpose of the phishing scheme targeting companies was in part to access tools necessary for SIM swapping as well as to access customer/identifying information, that could then be used to ultimately steal cryptocurrency.

54. Based on this information as well as information from victims, FBI employees, and other evidence obtained in this investigation, I believe that BUCHANAN and his coconspirators tried to steal cryptocurrency using various methods. One of those methods involved BUCHANAN and his coconspirators accessing a victim's cryptocurrency wallet or account on exchange platforms and transferring cryptocurrency to wallets that they controlled without the victim's knowledge, as further discussed below. Based on messages found on BUCHANAN's digital devices, it appears that BUCHANAN and his coconspirators gained such access through SIM-swapping and social engineering.

55. Throughout the investigation, the FBI identified numerous victims who had their cryptocurrency stolen. Based on information obtained from those victims and BUCHANAN's digital devices, [redacted], and blockchain

explorers, and information from FBI employees, I know that much of the stolen cryptocurrency was transferred to wallets controlled by BUCHANAN and his coconspirators, as discussed below.

1. Victim E.V.

56. On June 1, 2022, over 9 bitcoin (then worth $267,000) belonging to E.V., a resident of the [redacted], was transferred to a cryptocurrency address ending in [redacted], without E.V.'s knowledge. That transaction had a hash value ending in [redacted].

57. The same transaction hash value was found in the transaction history for a wallet associated with BUCHANAN's digital device. Specifically, the FBI found a seed phrase on one of BUCHANAN's devices and used it to access the associated wallet and its transaction history, which included the transaction with the hash value ending in [redacted].

2. Victim J.L.

58. On December 4, 2022, victim J.L., a resident of the [redacted], had bitcoin and ether (then worth $195,000) stolen from multiple accounts including a Coinbase account and an un-hosted wallet.

59. A search of a digital device belonging to Coconspirator 1, obtained pursuant to a warrant, revealed that on December 3, 2022, the day before the theft, a Telegram user

with the name "t" sent the name and email address of J.L. to Coconspirator 1. BUCHANAN's first name is "Tyler."

60. A portion of the stolen funds was sent to a Bitcoin wallet belonging to Coconspirator 1 that was later seized by the FBI pursuant to a warrant.

61. Another portion of the stolen funds was sent to a cryptocurrency address ending in [redacted] (the "[redacted] Address") that is believed to belong to BUCHANAN, as further discussed below.

62. A blockchain explorer page for the [redacted]l Address was saved as a "shortcut" on BUCHANAN's web browser found on one of his devices.

63. Records obtained from Discord revealed that the user of a Discord account with user ID [redacted] sent the [redacted] Address to an unidentified Discord user when asking the latter to send funds. Records for the Discord account revealed that the BUCHANAN IP Address (discussed above) was used to log into this Discord account multiple times in July 2022.

64. The publicly available transaction history for the [redacted] Address shows that approximately 391 bitcoin was transferred in and out of this address between October 2022 and February 2023; 391 bitcoin is presently worth more than $26 million.

3. Victims R.G., A.F., and C.T.

65. A cryptocurrency wallet found on one of BUCHANAN's devices contained an address ending in [redacted] (the "[redacted] Address"), indicating that BUCHANAN controlled that address.

66. On July 14, 2022, approximately 55.7 ether (then worth $60,000) was transferred from a Gemini account belonging to R.G., a resident of [redacted], without R.G.'s consent. After a series of transactions, a portion of the funds was received into the [redacted] Address.

67. On July 15, 2022, approximately 166.54 ether (then worth $199,000) was transferred from a Coinbase account belonging to A.F., a resident of [redacted], without A.F.'s consent. After a series of transactions, 44 of the ether was received into the [redacted] Address.

68. On July 21, 2022, approximately 26.52 ether (then worth $40,000) was transferred from a Coinbase account belonging to C.T., an [redacted] resident. After a series of transactions, a portion of the ether was received into the [redacted] Address.

4. Victim N.C.

69. On December 11, 2022, approximately 2.04 bitcoin (then worth $34,900) was transferred from an Coinbase account belonging to N.C., a resident of [redacted], without N.C.'s consent. After a series of transactions, a portion of the funds was sent to the [redacted] Address.

70. As stated above, a blockchain explorer page for the [redacted] Address was saved as a "shortcut" on BUCHANAN's web browser found on one of his devices.

71. That same day, Coconspirator 1 sent the name and email address of N.C. to the same Telegram user "t" connected to the theft from victim J.L.

5. Victim J.B.

72. On December 18, 2022, approximately 10.93 bitcoin (then worth $182,000) was transferred out of an un-hosted wallet belonging to J.B., a resident of [redacted], without J.B.'s consent. After a series of transactions, a portion of the bitcoin was sent to the [redacted] Address.

6. Victim D.H.

73. On December 4, 2022 approximately 7.66 bitcoin (then worth $129,000) was taken from a Coinbase account belonging to D.H., a resident of [redacted], without D.H.'s consent. A portion of the bitcoin was sent in a series of transactions to a wallet controlled by Coconspirator 1 and later seized by the FBI pursuant to a warrant.

74. Three days prior to the theft, the Telegram user "t" sent the name and email address of D.H. to Coconspirator 1.

7. Victim M.L.

75. On December 6, 2022 approximately 98.5 bitcoin (then worth $1,668,000) was transferred from a Coinbase account

belonging to M.L., a resident of [redacted], without M.L.'s consent. A portion of the cryptocurrency was sent through a series of transactions to a wallet belonging to Coconspirator 1 that was seized by the FBI pursuant to a warrant.

76. Five days prior to the theft, the Telegram user "t" sent the email address and phone number of M.L. to Coconspirator 1.

8. Victim J.G.

77. On December 7, 2022, more than $40,000 worth of 17 different cryptocurrencies, including ether and bitcoin, was transferred from un-hosted wallets belonging to J.G., a resident of [redacted], without J.G.'s consent. A portion of the cryptocurrency was sent in a series of transactions to a wallet controlled by Coconspirator 1 and later seized by the FBI pursuant to a warrant.

78. Six days before the theft, Telegram user "t" sent the email address and phone number of J.G. to Coconspirator 1.

//

//

//

//

//

//

//

V. CONCLUSION

79. Based on the above information, I respectfully submit that there is probable cause to believe that **BUCHANAN** committed criminal violations of 18 U.S.C. §S 1349, 371, 1343, and 1028A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 25 day of May, 2024.

HONORABLE MARGO ROCCONI
UNITED STATES MAGISTRATE JUDGE