UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

January 2025 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. TYLER ROBERT BUCHANAN, aka "Dread Pirate Roberts," aka "Evefan," AHMED HOSSAM ELDIN ELBADAWY, aka "AD," EVANS ONYEAKA OSIEBO, and JOEL MARTIN EVANS, aka "joeleoli," Defendants.	2:24-cr-595(A)-JWH F I R S T S U P E R S E D I N G I N D I C T M E N T [18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud; 18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1028A(a)(1): Aggravated Identity Theft; 18 U.S.C. §§ 981, 982, 1029, 1030 and 28 U.S.C. § 2461(c): Criminal Forfeiture]

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this First Superseding Indictment:

A. The Conspiracy and Defendants

1. The conspirators were members of a loosely organized financially motivated cybercriminal group whose members primarily target large companies and their contracted telecommunications, information technology ("IT"), and business process outsourcing

("BPO") suppliers (each a "Victim Company" and collectively, the "Victim Companies"). The group employed a variety of social engineering techniques, including Short Messaging Service ("SMS") phishing, to fraudulently obtain credentials of Victim Company employees in order to gain unauthorized access to employee accounts and Victim Company computers, and steal confidential Victim Company data.

2. In addition to Victim Company intrusions, and combined with other social engineering techniques, members of the group used information obtained from Victim Company intrusions to identify and gain access to virtual currency accounts and wallets belonging to individual victims to steal virtual currency worth millions of dollars.

3. Defendant TYLER ROBERT BUCHANAN, also known as ("aka") "Dread Pirate Roberts," aka "Evefan," ("BUCHANAN"), was a resident of Scotland.

4. Defendant AHMED HOSSAM ELDIN ELBADAWY, aka "AD" ("ELBADAWY"), was a resident of College Station, Texas.

5. Defendant EVANS ONYEAKA OSIEBO ("OSIEBO") was a resident of Dallas, Texas.

6. Defendant JOEL MARTIN EVANS, aka "joeleoli" ("EVANS"), was a resident of Wilmington, North Carolina.

7. Co-conspirator NOAH MICHAEL URBAN ("co-conspirator URBAN") was a resident of Palm Coast, Florida.

8. BUCHANAN, ELBADAWY, OSIEBO, EVANS, and co-conspirator URBAN knowingly and intentionally conspired with each other, and with persons known and unknown to the Grand Jury, to conduct criminal cyber intrusions and virtual currency thefts. The conspirators'

victims and intended victims included interactive entertainment companies, telecommunications companies, technology companies, BPO suppliers, cloud communications providers, virtual currency companies, and individuals. The conspirators hacked and defrauded Victim Companies and individual victims around the United States, including in the Central District of California.

9. The conspirators often targeted victims by sending SMS phishing messages to Victim Company employees intended to make the victims enter their employee login credentials into websites designed to look like legitimate websites of a Victim Company or a Victim Company's contracted telecommunications, IT, and BPO suppliers. Once they gained unauthorized access to a Victim Company computer system, defendants BUCHANAN, ELBADAWY, OSIEBO, and co-conspirator URBAN, together with other co-conspirators, would conduct research within the system and attempt to locate and copy confidential Victim Company data.

10. In some instances, defendants BUCHANAN, ELBADAWY, OSIEBO, and co-conspirator URBAN together with other co-conspirators, would gain access to the computer systems of certain interactive entertainment Victim Companies and use that access to give themselves or other co-conspirators privileges or gifts. In other instances, defendants BUCHANAN, ELBADAWY, OSIEBO, and co-conspirator URBAN, together with other co-conspirators, would copy confidential databases from Victim Companies and attempt to sell the information to others.

11. Using information obtained from Victim Company intrusions, and combined with information from other sources, defendants BUCHANAN, ELBADAWY, OSIEBO, and co-conspirator URBAN, together with

other co-conspirators, would also gain access to individual victims' virtual currency accounts and wallets.

12. Defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and other co-conspirators, attacked or attempted to attack dozens of companies, including Victim Companies 1 through 12, and stole at least 11 million dollars' worth of virtual currency from individual victims, including Individual Victims 1 through 29.

B. The Victim Companies

13. "Victim Company 1" was a company with offices in Los Angeles County, within the Central District of California, that provided interactive entertainment products and software.

14. "Victim Company 2" was a company with offices in Orange County, within the Central District of California, that provided BPO services and products.

15. "Victim Company 3" was a company based in the United States that provided interactive entertainment products and software.

16. "Victim Company 4" was a company with offices in Los Angeles County, within the Central District of California, that provided technology products and services.

17. "Victim Company 5" was a company based in the United States that provided virtual currency services and products.

18. "Victim Company 6" was a company based in the United States that provided BPO services and products.

19. "Victim Company 7" was a company based in the United States that provided cloud communications platforms and products.

20. "Victim Company 8" was a company based in the United States that provided BPO services and products.

21. "Victim Company 9" was a company based in the United States that provided cable, internet, telephone, and related products.

22. "Victim Company 10" was a company based in the United States that provided telecommunications services.

23. "Victim Company 11" was a company based in the United States that provided telecommunications services.

24. "Victim Company 12" was a company based in the United States that provided BPO services and products.

C. Definitions

25. A domain or domain name is an alphanumeric address for a computer on the Internet. Examples include www.justice.gov and www.uscourts.gov. Domains are used to navigate to websites.

26. Domain registration is the act of purchasing a domain on the Internet for a specific time period. In order to do so, the domain registrant typically applies to a company that manages the reservation of Internet domain names, known as a registrar, and pays an associated fee.

27. Phishing is a cyber-attack technique whereby the attacker sends a fraudulent message purporting to be from a legitimate sender and designed to lure the recipient into visiting a fraudulent website, known as a phishing website. The phishing website is designed to appear like it is associated with a legitimate company or organization for the purpose of luring the message recipient into providing login credentials and confidential 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.

28. SMS phishing is a type of phishing that transmits the phishing message through text messages that are commonly sent over Short Message Service (SMS) channels to mobile telephones but also can be sent using non-SMS channels like data-based messaging applications.

29. A server is a computer that provides resources, data, services, or programs to other computers over a network. A virtual private server ("VPS") is a virtual operating system that resides within a physical server and uses virtualization technology to provide dedicated, private resources as though it were a separate computer. VPSs are commonly sold as a service by hosting providers. A VPS runs its own copy of an operating system, and VPS customers have access to that operating system to install almost any software that runs on that operating system, including to host phishing websites.

30. A Subscriber Identity Module or Subscriber Identification Module ("SIM") is a technology used to identify and authenticate subscribers on mobile telephone devices.

31. SIM swapping is a type of account takeover whereby attackers take over a victim's mobile telephone number and the associated communications. Attackers will generally change the SIM that is associated with a mobile telephone number to a SIM associated with a device that the attacker controls. Once the telephone number is transferred, the attacker controls the victim's telephone number.

32. Virtual currency or cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure financial transactions, control the creation of additional units of the currency, and verify the transfer of assets. Virtual

currency is typically accessed using secret or private encryption keys which are commonly stored using a wallet. A virtual currency wallet is a software application or hardware device that holds and stores a user's virtual currency addresses and private keys. Some wallets also allow users to send and receive cryptocurrency. Virtual currency exchanges are platforms for buying, selling, and storing virtual assets and can also allow for the exchange between different types of virtual currencies, or between virtual currency and fiat currency (e.g., U.S. dollars).

33. Telegram is a cloud-based encrypted messaging service that allowed users to post messages in public channels and message other users directly.

COUNT ONE

[18 U.S.C. § 1349]

[ALL DEFENDANTS]

The Grand Jury hereby realleges and incorporates by reference paragraphs 1 through 33 of the Introductory Allegations and Definitions of this First Superseding Indictment as though fully set forth herein.

A. OBJECT OF THE CONSPIRACY

34. Beginning on a date unknown to the Grand Jury, but no later than September 25, 2021, and continuing through on or about April 12, 2023, in Los Angeles and Orange Counties, within the Central District of California, and elsewhere, defendants BUCHANAN, ELBADAWY, OSIEBO, EVANS, co-conspirator URBAN, and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

B. MEANS BY WHICH THE OBJECT OF THE CONSPIRACY WAS TO BE ACCOMPLISHED

35. The object of the conspiracy was to be accomplished in substance as follows:

a. Defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators, would conduct phishing attacks by sending SMS phishing messages to the mobile telephones of Victim Company employees that purported to be from a Victim Company or a Victim Company contracted BPO supplier (itself a Victim Company). The SMS phishing messages would contain links to phishing websites designed to look like legitimate websites of a Victim Company or a contracted BPO supplier and lure the recipient into providing confidential

information, including account login credentials.

b. To hone the effectiveness of the SMS phishing messages, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators, would conduct internet research about their intended victims and would send test SMS phishing messages to each other or themselves.

c. Defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators would then use credentials stolen through SMS phishing to access the accounts of Victim Company employees and the computer systems of Victim Companies, to steal confidential information, including confidential work product, intellectual property, and personal identifying information, such as account access credentials, names, email addresses, and telephone numbers.

d. Defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators would commit computer intrusions in order to obtain personal identifying information of Victim Company employees and customers that they would later use to identify potential victims, fraudulently gain access to virtual currency accounts and wallets, and transfer virtual currency from individual victims' virtual currency accounts and wallets to accounts controlled by defendants BUCHANAN, ELBADAWY, OSIEBO, EVANS, co-conspirator URBAN, and co-conspirators.

e. In order to fraudulently gain access to individual victims' virtual currency wallets and accounts, and to bypass two factor authentication security features, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators, would (i) gain unauthorized access to various online accounts of victims, including email accounts; and (ii) conduct, or cause to be conducted,

SIM swaps of individual victims' mobile telephone numbers to devices that the conspirators controlled.

f. In some instances, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators would gain unauthorized access to the computer systems of Victim Companies and use that access to modify software configurations on the Victim Company system. In other instances, after gaining unauthorized access to Victim Company computer systems, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators would copy confidential databases from Victim Companies and attempt to sell the stolen information to others.

g. Defendants BUCHANAN, ELBADAWY, OSIEBO, EVANS, co-conspirator URBAN, and co-conspirators would create, manage, and pay for infrastructure needed for phishing attacks, including VPSs used to host phishing websites and domain names for the phishing websites.

h. Defendant EVANS would create software used by defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and co-conspirators to conduct phishing attacks on Victim Company employees.

i. Defendant EVANS would assist in creating and managing online infrastructure used during SMS phishing attacks, including a Telegram channel that received the fraudulently obtained login credentials from Victim Company employees, and would receive from co-conspirators stolen virtual currency from Individual Victims as payment.

j. Defendants BUCHANAN, ELBADAWY, OSIEBO, and co-conspirator URBAN would possess the stolen login credentials and personal identifying information of Victim Company employees and customers, and Individual Victims, on digital devices for use in

later SMS phishing attacks, computer intrusions, and virtual currency thefts.

C. OVERT ACTS

36. On or about the following dates, in furtherance of the conspiracy and to accomplish its object, defendants BUCHANAN, ELBADAWY, OSIEBO, EVANS, co-conspirator URBAN, and other co-conspirators committed various overt acts within the Central District of California and elsewhere, including, but not limited to, the following:

SMS Phishing Attacks and Intrusions of Victim Companies

Victim Company 1

Overt Act No. 1: Between May 29, 2022 and June 2, 2022, defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 1 employees, causing at least one Victim Company 1 employee to transmit their credentials via the fraudulent phishing websites provided in the SMS phishing messages.

Overt Act No. 2: On June 2, 2022, defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted a phishing message to at least one Victim Company 1 employee which stated, "WARNING!! Your [Victim Company 1] VPN is being deactivated, to keep your VPN active, please head over to [Victim Company 1]-vpn.net."

Overt Act No. 3: Beginning in or around June 2, 2022, defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim

Company 1 and used the access to modify software configurations on Victim Company 1's computers.

Overt Act No. 4: On January 16, 2023, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 1 employees, causing at least one Victim Company 1 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 5: Beginning in or around January 16, 2023, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim Company 1 and copied confidential data from Victim Company 1.

Overt Act No. 6: On January 16, 2023, on a messaging platform, co-conspirator URBAN sent messages stating, in part, "I have one of the rarest . . . account in all of history" and " . . . I just hacked htis [sic] one off [Victim Company 1]."

Victim Company 2

Overt Act No. 7: Beginning in or around May 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 2 employees, causing at least one Victim Company 2 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 8: On an unknown date in May or June 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim Company 2 and copied confidential data from Victim Company 2.

Victim Company 3

Overt Act No. 9: On June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 3 employees, causing at least one Victim Company 3 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 10: On or around June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim Company 3, accessed confidential data from Victim Company 3, and made changes to Victim Company 3 user accounts.

Victim Company 4

Overt Act No. 11: On June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 4 employees, causing at least one Victim Company 4 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 12: On or around June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim Company 4.

Victim Company 5

Overt Act No. 13: On June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 5 employees, causing at least one

Victim Company 5 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 14: On an unknown date in June or July 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to computers of Victim Company 5 and accessed confidential data.

Victim Company 6

Overt Act No. 15: On or before June 11, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim Company 6 and copied confidential data from Victim Company 6.

Victim Company 7

Overt Act No. 16: On July 19, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 7 employees, causing at least one Victim Company 7 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 17: On or after July 19, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim Company 7 and copied confidential data from Victim Company 7.

Overt Act No. 18: On September 26, 2022, via Telegram, defendants BUCHANAN and ELBADAWY discussed with another Telegram user selling an exported database of registration identifiers, email addresses, and partial telephone numbers of accountholders of a virtual currency exchange, stolen from the computers of Victim Company 7.

Victim Company 8

Overt Act No. 19: On an unknown date in 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 8 employees, causing at least one Victim Company 8 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 20: On an unknown date in 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computer network of Victim Company 8 and copied data from Victim Company 8.

Victim Company 9

Overt Act No. 21: On or before December 19, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators transmitted or caused to be transmitted SMS phishing messages to the mobile telephones of Victim Company 9 employees, causing at least one Victim Company 9 employee to transmit their credentials via the phishing websites provided in the SMS phishing messages.

Overt Act No. 22: On or after December 19, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to at least one Victim Company 9 employee account and reset their password.

Overt Act No. 23: On or after December 19, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators gained unauthorized access to the computers of Victim Company 9 and accessed confidential data of Victim Company 9.

Maintenance of Online Infrastructure and Possession of Stolen Access Devices

Overt Act No. 24: On December 3, 2021, defendant BUCHANAN saved a screen capture of messages with defendant EVANS in which defendant EVANS states, in part, "do u have multiple [Victim Company 5] api accs? They rate limit to 10k per hour by key and ip."

Overt Act No. 25: On March 8, 2022, defendant BUCHANAN saved a screen capture of messages with defendant EVANS in which BUCHANAN sent defendant EVANS a list of potential phishing domain names, including a phishing domain name related to Victim Company 5.

Overt Act No. 26: Between at least March 21, 2022 and August 1, 2022, along with defendant BUCHANAN, defendant EVANS was an administrator of a Telegram channel that received fraudulently obtained login credentials from Victim Company employees.

Overt Act No. 27: On May 14, 2022, defendant EVANS accessed a VPS account used to register a phishing website.

Overt Act No. 28: Between May 21, 2022 and June 17, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 10.

Overt Act No. 29: On May 28, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered a phishing domain with a name suggesting it was associated with Victim Company 2.

Overt Act No. 30: Between May 28, 2022 and July 25, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 8.

Overt Act No. 31: Between May 29, 2022 and June 3, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 1.

Overt Act No. 32: Between May 29, 2022 and June 3, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 11.

Overt Act No. 33: On an unknown date prior to May 31, 2022, defendant EVANS created software designed to capture login credentials entered into fraudulent phishing websites by Victim Company employees and transmit the fraudulently obtained credentials to a Telegram channel accessible to co-conspirators.

Overt Act No. 34: On May 31, 2022, co-conspirator URBAN entered test credentials into a phishing website to confirm the website was properly functioning.

Overt Act No. 35: On June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered a phishing domain with a name suggesting it was associated with Victim Company 3.

Overt Act No. 36: On June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 4.

Overt Act No. 37: On June 2, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 5.

Overt Act No. 38: Between June 4, 2022 and June 9, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 11.

Overt Act No. 39: Between June 12, 2022 and July 27, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or other co-conspirators registered phishing domains with names suggesting they were associated with Victim Company 6.

Overt Act No. 40: In July 2022, defendant OSIEBO logged in to at least 25 accounts used to register phishing domains and host phishing websites.

Overt Act No. 41: On October 14, 2022, via Telegram, defendant ELBADAWY sent a co-conspirator a message with the following content for an SMS phishing message: "sms_content = Your [Victim Company 5] password has been changed. Please tap [Victim Company 5.net] if this wasn't you."

Overt Act No. 42: On December 8, 2022, defendant ELBADAWY conducted online research on Individual Victim 28.

Overt Act No. 43: On February 4, 2023, via Telegram, defendant OSIEBO sent defendant ELBADAWY messages stating, in part "[Victim Company 11] up as well. 2.5k per swap. Dm me if want to buy" and provided a virtual currency address.

Overt Act No. 44: On March 1, 2023, at his residence in College Station, Texas, in a Telegram export file, defendant ELBADAWY possessed the login credentials for numerous Victim Company employees, including the login credentials for approximately 7 Victim Company 1 employees, 36 Victim Company 2 employees, two Victim Company 3 employees, one Victim Company 4 employee, four Victim

Company 5 employees, 50 Victim Company 6 employees, 29 Victim Company 8 employees, five Victim Company 10 employees, and 63 Victim Company 11 employees.

Overt Act No. 45: On March 1, 2023, at his residence in College Station, Texas, defendant ELBADAWY possessed an exported database of registration identifiers, email addresses, and partial telephone numbers of accountholders of a virtual currency exchange.

Overt Act No. 46: On April 12, 2023, on digital devices found at defendant BUCHANAN's residence, BUCHANAN possessed files related to Victim Companies, including employee directories of Victim Companies 6, 8, 9, and 12; email addresses for approximately 80 Victim Company 10 employees; and nonpublic files containing business-related information for Victim Company 11.

Overt Act No. 47: On April 12, 2023, on a digital device found at defendant BUCHANAN's residence, BUCHANAN possessed an exported database of registration identifiers, email addresses, and partial telephone numbers of accountholders of a virtual currency exchange.

Overt Act No. 48: On April 12, 2023, on a digital device found at defendant BUCHANAN's residence, BUCHANAN possessed the names and email addresses of Individual Victims 18, 19, 20, 22, 23, 24, 27, and 29.

Virtual Currency Thefts

Individual Victim 1

Overt Act No. 49: On September 25 and 26, 2021, after gaining unauthorized access to Individual Victim 1's personal email account and virtual currency wallets, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $6,347,605 originating from Individual Victim 1's

wallets to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, and other co-conspirators.

Individual Victim 2

Overt Act No. 50: On May 31, 2022, after gaining unauthorized access to Individual Victim 2's virtual currency wallet, defendants ELBADAWY, BUCHANAN, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $266,988 originating from Individual Victim 2's wallet to virtual currency addresses controlled by defendants ELBADAWY, BUCHANAN, and other co-conspirators. Individual Victim 2 was a resident of the Central District of California.

Individual Victim 3

Overt Act No. 51: On June 6, 2022, after gaining unauthorized access to Individual Victim 3's account at a virtual currency exchange, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $571,413 originating from Individual Victim 3's account to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 4

Overt Act No. 52: On June 10, 2022, after gaining unauthorized access to Individual Victim 4's account at a virtual currency exchange, defendants ELBADAWY, OSIEBO, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $95,606 originating from Individual Victim 4's account to virtual currency addresses controlled by defendants ELBADAWY, OSIEBO, and other co-conspirators.

Overt Act No. 53: On June 11, 2022, defendant ELBADAWY or another co-conspirator used a portion of the funds stolen from

Individual Victim 4 to pay for an account used to register phishing domains.

Individual Victim 5

Overt Act No. 54: On June 23, 2022, after gaining unauthorized access to Individual Victim 5's virtual currency wallet, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $131,290 originating from Individual Victim 5's wallet to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 6

Overt Act No. 55: On July 14, 2022, after gaining unauthorized access to Individual Victim 6's account at a virtual currency exchange, co-conspirator URBAN or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $60,010 originating from Individual Victim 6's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and other co-conspirators.

Individual Victim 7

Overt Act No. 56: On July 15, 2022, after gaining unauthorized access to Individual Victim 7's account at a virtual currency exchange, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $199,456 originating from Individual Victim 7's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, and other co-conspirators.

Individual Victim 8

Overt Act No. 57: On or before July 15, 2022, defendants

BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or a co-conspirator conducted or caused to be conducted a SIM swap of Individual Victim 8's telephone number.

Overt Act No. 58: On July 15, 2022, after gaining unauthorized access to Individual Victim 8's account at a virtual currency exchange, defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $199,116 originating from Individual Victim 8's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, and other co-conspirators.

Individual Victim 9

Overt Act No. 59: On July 18, 2022, after gaining unauthorized access to Individual Victim 9's personal email account and virtual currency wallet, defendant ELBADAWY or a co-conspirator, conducted false and fraudulent transfers of virtual currency worth approximately $413,004 originating from Individual Victim 9's wallet to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators. Individual Victim 9 was a resident of the Central District of California.

Overt Act No. 60: On August 1, 2022, defendant ELBADAWY or a co-conspirator used a portion of the funds stolen from Individual Victim 9 to pay for an account used to register phishing domains.

Individual Victim 10

Overt Act No. 61: On July 18, 2022, after gaining unauthorized access to Individual Victim 10's account at a virtual currency exchange, defendants ELBADAWY, OSIEBO, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth

approximately $19,573 originating from Individual Victim 10's account to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 11

Overt Act No. 62: On or before July 21, 2022, defendants BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or a co-conspirator conducted or caused to be conducted a SIM swap of Individual Victim 11's telephone number.

Overt Act No. 63: On July 21, 2022, after gaining unauthorized access to Individual Victim 11's account at a virtual currency exchange, defendants BUCHANAN, OSIEBO, co-conspirator URBAN, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $40,411 originating from Individual Victim 11's account to virtual currency addresses controlled by defendants BUCHANAN, OSIEBO, EVANS, co-conspirator URBAN, and other co-conspirators.

Individual Victim 12

Overt Act No. 64: On July 21, 2022, after gaining unauthorized access to Individual Victim 12's account at a virtual currency exchange, defendant BUCHANAN, co-conspirator URBAN, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $9,179 originating from Individual Victim 12's account to virtual currency addresses controlled by defendant BUCHANAN, co-conspirator URBAN, and other co-conspirators.

Individual Victim 13

Overt Act No. 65: On July 22, 2022, after gaining unauthorized access to Individual Victim 13's account at a virtual currency exchange, defendants BUCHANAN, ELBAWADY, co-conspirator URBAN, or a

co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $16,910 originating from Individual Victim 13's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, EVANS, co-conspirator URBAN, and other co-conspirators.

Individual Victim 14

Overt Act No. 66: On October 31, 2022, after gaining unauthorized access to Individual Victim 14's account at a virtual currency exchange, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $32,302 originating from Individual Victim 14's account to virtual currency addresses and wallets controlled by defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, and other co-conspirators.

Individual Victim 15

Overt Act No. 67: On or before November 9, 2022, defendant ELBADAWY or co-conspirator conducted or caused to be conducted a SIM swap of Individual Victim 15's telephone number.

Overt Act No. 68: On November 9, 2022, after gaining unauthorized access to Individual Victim 15's virtual currency wallet, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $152,205 originating from Individual Victim 15's wallets to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 16

Overt Act No. 69: On or before November 9, 2022, defendant ELBADAWY or a co-conspirator conducted or caused to be conducted a SIM swap of Individual Victim 16's telephone number.

Overt Act No. 70: On November 17, 2022, after gaining

unauthorized access to Individual Victim 16's virtual currency wallet, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $35,647 originating from Individual Victim 16's wallet to virtual currency addresses and wallets controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 17

Overt Act No. 71: On November 22, 2022, after gaining unauthorized access to Individual Victim 17's account at a virtual currency exchange, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $20,093 originating from Individual Victim 17's account to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 18

Overt Act No. 72: On November 29, 2022, after gaining unauthorized access to Individual Victim 18's account at a virtual currency exchange, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $11,842 originating from Individual Victim 18's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, OSIEBO, and other co-conspirators.

Individual Victim 19

Overt Act No. 73: On December 3, 2022, via Telegram, defendant BUCHANAN sent defendant ELBADAWY the name and email address of Individual Victim 19 with the words "highnetworth" and "funded."

Overt Act No. 74: On December 4, 2022, after gaining unauthorized access to Individual Victim 19's account at a virtual

currency exchange and a separate virtual currency wallet, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $195,766 originating from Individual Victim 19's account and wallet to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, and other co-conspirators. Individual Victim 19 was a resident of the Central District of California.

Individual Victim 20

Overt Act No. 75: On December 1, 2022, via Telegram, defendant BUCHANAN sent defendant ELBADAWY the name and email address of Individual Victim 20 with the words "highnetworth" and "funded."

Overt Act No. 76: On or before December 4, 2022, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted or caused to be conducted a SIM swap of Individual Victim 20's telephone number.

Overt Act No. 77: On December 4, 2022, after gaining unauthorized access to Individual Victim 20's account at a virtual currency exchange, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $129,586 originating from Individual Victim 20's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, and other co-conspirators.

Individual Victim 21

Overt Act No. 78: On or after December 1, 2022, after gaining unauthorized access to Individual Victim 21's account at a virtual currency exchange and a separate virtual currency wallet, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $5,382 originating from

Individual Victim 21's account and wallet to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 22

Overt Act No. 79: On December 1, 2022, via Telegram, defendant BUCHANAN sent defendant ELBADAWY the email address and telephone number for Individual Victim 22.

Overt Act No. 80: On December 6, 2022, after gaining unauthorized access to Individual Victim 22's account at a virtual currency exchange, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $1,668,032 originating from Individual Victim 22's account to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 23

Overt Act No. 81: On December 7, 2022, after gaining unauthorized access to Individual Victim 23's virtual currency wallets, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $57,800 originating from Individual Victim 23's wallet to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 24

Overt Act No. 82: On December 11, 2022, defendant ELBADAWY sent defendant BUCHANAN the name and email addresses of Individual Victim 24.

Overt Act No. 83: On or before December 11, 2022, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted or caused to be conducted a SIM swap of Individual Victim 24's telephone number.

Overt Act No. 84: On December 11, 2022, after gaining unauthorized access to Individual Victim 24's account at a virtual currency exchange, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $34,861 originating from Individual Victim 24's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, and other co-conspirators.

Individual Victim 25

Overt Act No. 85: On or before December 17, 2022, defendant ELBADAWY or a co-conspirator conducted or caused to be conducted a SIM swap of Individual Victim 25's telephone number.

Overt Act No. 86: On or after December 18, 2022, after gaining unauthorized access to Individual Victim 25's account at a virtual currency exchange and a separate virtual currency wallet, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $209,572 originating from Individual Victim 26's account and wallet to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, OSIEBO, and other co-conspirators.

Individual Victim 26

Overt Act No. 87: On December 28, 2022, after gaining unauthorized access to Individual Victim 26's account at a virtual currency exchange, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $7,180 originating from Individual Victim 26's account to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 27

Overt Act No. 88: On January 1, 2023, after gaining unauthorized access to Individual Victim 27's account at a virtual currency exchange, defendants BUCHANAN, ELBADAWY, or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $17,135 originating from Individual Victim 27's account to virtual currency addresses controlled by defendants BUCHANAN, ELBADAWY, and other co-conspirators. Individual Victim 27 was a resident of the Central District of California.

Individual Victim 28

Overt Act No. 89: On January 17, 2023, after gaining unauthorized access to Individual Victim 28's account at a virtual currency exchange, defendant ELBADAWY or a co-conspirator conducted false and fraudulent transfers of virtual currency worth approximately $97,216 originating from Individual Victim 28's account to virtual currency addresses controlled by defendant ELBADAWY and other co-conspirators.

Individual Victim 29

Overt Act No. 90: On January 19, 2023, after gaining unauthorized access to Individual Victim 29's account at a virtual currency exchange, defendant OSIEBO or a co-conspirator conducted a false and fraudulent transfer of virtual currency worth approximately $4,010 originating from Individual Victim 29's account to a virtual currency address controlled by defendant OSIEBO and other co-conspirators.

COUNT TWO

[18 U.S.C. § 371]

[ALL DEFENDANTS]

The Grand Jury hereby realleges and incorporates by reference paragraphs 1 through 33 of the Introductory Allegations and Definitions of this First Superseding Indictment as though fully set forth herein.

A. OBJECTS OF THE CONSPIRACY

37. Beginning on a date unknown to the Grand Jury, but no later than September 25, 2021, and continuing through on or about April 12, 2023, in Los Angeles and Orange Counties, within the Central District of California, and elsewhere, defendants BUCHANAN, ELBADAWY, OSIEBO, EVANS, co-conspirator URBAN, and others known and unknown to the Grand Jury, knowingly conspired and agreed with each other to:

a. intentionally access computers without authorization and thereby obtain information from protected computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i);

b. knowingly and with intent to defraud access protected computers without authorization, and by means of such conduct, further the intended fraud and obtain a thing of value, in violation of Title 18, United States Code, Section 1030(a)(4), (c)(3)(A); and

c. knowingly and with intent to defraud, possess fifteen or more unauthorized access devices (as defined in Title 18, United States Code, Sections 1029(e)(1) and (3)), in violation of Title 18, United States Code, Section 1029(a)(3).

//

//

B. MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

38. The objects of the conspiracy were to be accomplished in substance as follows:

a. The Grand Jury hereby repeats and realleges the Means by Which the Objects of the Conspiracy Were to be Accomplished as set forth in Section B of Count One of this First Superseding Indictment as if fully set forth herein.

C. OVERT ACTS

39. On or about the following dates, in furtherance of the conspiracy and to accomplish its objects, defendants BUCHANAN, ELBADAWY, OSIEBO, EVANS, co-conspirator URBAN, and co-conspirators committed various overt acts within the Central District of California and elsewhere, including, but not limited to, the following:

Overt Acts Nos. 1-90: The Grand Jury hereby repeats and realleges Overt Acts 1 through 90 set forth in Section C of Count One of this First Superseding Indictment as if fully set forth herein.

COUNT THREE

[18 U.S.C. §§ 1028A(a)(1), 2(a)]

[ALL DEFENDANTS]

Beginning on an unknown date, but no later than September 25, 2021, and continuing to on or about April 12, 2023, in Los Angeles and Orange Counties, within the Central District of California, and elsewhere, defendants TYLER ROBERT BUCHANAN, also known as ("aka") "Dread Pirate Roberts," aka "Evefan," ("BUCHANAN"), AHMED HOSSAM ELDIN ELBADAWY, aka "AD," ("ELBADAWY"), EVANS ONYEAKA OSIEBO ("OSIEBO"), JOEL MARTIN EVANS, aka "joeleoli," ("EVANS"), along with co-conspirator NOAH MICHAEL URBAN ("co-conspirator URBAN"), each aiding and abetting the other, knowingly transferred, possessed, and used, without lawful authority, a means of identification that defendants BUCHANAN, ELBADAWY, OSIEBO, EVANS, and co-conspirator URBAN, knew belonged to another person, during and in relation to the offense of Conspiracy to Commit Wire Fraud, a felony violation of Title 18, United States Code, Section 1349, as charged in Count One of this First Superseding Indictment.

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c)]

1. Pursuant to Rule 32.2 of the Federal Rules of Criminal Procedure, notice is hereby given that the United States of America will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), in the event of any defendant's conviction of the offenses set forth in any of Counts One or Three of this First Superseding Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds traceable to the offenses; and

(b) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraph (a).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), any defendant so convicted shall forfeit substitute property, up to the value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph or any portion thereof (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to, or deposited with a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been

//

//

substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

FORFEITURE ALLEGATION TWO

[18 U.S.C. §§ 982, 1030, and 1029]

1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal Procedure, notice is hereby given that the United States will seek forfeiture as part of any sentence, pursuant to Title 18, United States Code, Sections 982(a)(2), 1030, and 1029, in the event of any defendant's conviction of the offense set forth in Count Two of this First Superseding Indictment.

2. Any defendant so convicted shall forfeit to the United States of America the following:

(a) All right, title, and interest in any and all property, real or personal, constituting, or derived from, any proceeds obtained, directly or indirectly, as a result of the offense;

(b) Any personal property used or intended to be used to commit the offense; and

(c) To the extent such property is not available for forfeiture, a sum of money equal to the total value of the property described in subparagraphs (a) and (b).

3. Pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1), 1030(i), and 1029(c)(2), any defendant so convicted shall forfeit substitute property, up to the total value of the property described in the preceding paragraph if, as the result of any act or omission of said defendant, the property described in the preceding paragraph, or any portion thereof: (a) cannot be located upon the exercise of due diligence; (b) has been transferred, sold to or deposited with a third party; (c) has been placed beyond the jurisdiction of the

court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be divided without difficulty.

A TRUE BILL

/S/
Foreperson

BILAL A. ESSAYLI
United States Attorney

DAVID T. RYAN
Assistant United States Attorney
Chief, National Security Division

KHALDOUN SHOBAKI
Assistant United States Attorney
Chief, Cyber and Intellectual Property Crimes Section

LAUREN RESTREPO
Assistant United States Attorney
Deputy Chief, Cyber and Intellectual Property Crimes Section