



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 B. The Victim Companies

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

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

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

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

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

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

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

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

28

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

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

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

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

9 C. Definitions

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

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

18 27. Phishing is a cyber-attack technique whereby the attacker  
19 sends a fraudulent message purporting to be from a legitimate sender  
20 and designed to lure the recipient into visiting a fraudulent  
21 website, known as a phishing website. The phishing website is  
22 designed to appear like it is associated with a legitimate company or  
23 organization for the purpose of luring the message recipient into  
24 providing login credentials and confidential information through the  
25 website. Phishing websites commonly have domain names that are  
26 similar to the domain names of the legitimate company or organization  
27 that they are trying to imitate.

28

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

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

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

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

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

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

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

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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

1 information, including account login credentials.

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

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

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

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

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

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

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

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

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

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

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

3 C. OVERT ACTS

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

10 **SMS Phishing Attacks and Intrusions of Victim Companies**

11 **Victim Company 1**

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

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

25 Overt Act No. 3: Beginning in or around June 2, 2022,  
26 defendants BUCHANAN, ELBADAWY, co-conspirator URBAN, or other co-  
27 conspirators gained unauthorized access to the computers of Victim  
28

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

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

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

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

17 **Victim Company 2**

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

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

1 **Victim Company 3**

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

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

13 **Victim Company 4**

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

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

24 **Victim Company 5**

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

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

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

7 **Victim Company 6**

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

12 **Victim Company 7**

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

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

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

1 **Victim Company 8**

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

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

13 **Victim Company 9**

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

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

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

1 **Maintenance of Online Infrastructure and Possession of Stolen Access**  
2 **Devices**

3 Overt Act No. 24: On December 3, 2021, defendant BUCHANAN  
4 saved a screen capture of messages with defendant EVANS in which  
5 defendant EVANS states, in part, "do u have multiple [Victim Company  
6 5] api accs? They rate limit to 10k per hour by key and ip."

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

11 Overt Act No. 26: Between at least March 21, 2022 and August  
12 1, 2022, along with defendant BUCHANAN, defendant EVANS was an  
13 administrator of a Telegram channel that received fraudulently  
14 obtained login credentials from Victim Company employees.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Company 5 employees, 50 Victim Company 6 employees, 29 Victim Company  
2 8 employees, five Victim Company 10 employees, and 63 Victim Company  
3 11 employees.

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

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

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

18 Overt Act No. 48: On April 12, 2023, on a digital device found  
19 at defendant BUCHANAN's residence, BUCHANAN possessed the names and  
20 email addresses of Individual Victims 18, 19, 20, 22, 23, 24, 27, and  
21 29.

## 22 Virtual Currency Thefts

### 23 **Individual Victim 1**

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

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

3 **Individual Victim 2**

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

12 **Individual Victim 3**

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

19 **Individual Victim 4**

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

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

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

3 **Individual Victim 5**

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

10 **Individual Victim 6**

11 Overt Act No. 55: On July 14, 2022, after gaining unauthorized  
12 access to Individual Victim 6's account at a virtual currency  
13 exchange, co-conspirator URBAN or a co-conspirator conducted false  
14 and fraudulent transfers of virtual currency worth approximately  
15 \$60,010 originating from Individual Victim 6's account to virtual  
16 currency addresses controlled by defendants BUCHANAN, ELBADAWY,  
17 OSIEBO, co-conspirator URBAN, and other co-conspirators.

18 **Individual Victim 7**

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

27 **Individual Victim 8**

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

1 BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or a co-conspirator  
2 conducted or caused to be conducted a SIM swap of Individual Victim  
3 8's telephone number.

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

12 **Individual Victim 9**

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

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

24 **Individual Victim 10**

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

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

4 **Individual Victim 11**

5 Overt Act No. 62: On or before July 21, 2022, defendants  
6 BUCHANAN, ELBADAWY, OSIEBO, co-conspirator URBAN, or a co-conspirator  
7 conducted or caused to be conducted a SIM swap of Individual Victim  
8 11's telephone number.

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

17 **Individual Victim 12**

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

25 **Individual Victim 13**

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

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

6 **Individual Victim 14**

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

14 **Individual Victim 15**

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

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

24 **Individual Victim 16**

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

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

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

7 **Individual Victim 17**

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

15 **Individual Victim 18**

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

23 **Individual Victim 19**

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

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

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

8 **Individual Victim 20**

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

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

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

22 **Individual Victim 21**

23 Overt Act No. 78: On or after December 1, 2022, after gaining  
24 unauthorized access to Individual Victim 21's account at a virtual  
25 currency exchange and a separate virtual currency wallet, defendant  
26 ELBADAWY or a co-conspirator conducted false and fraudulent transfers  
27 of virtual currency worth approximately \$5,382 originating from  
28

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

3 **Individual Victim 22**

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

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

14 **Individual Victim 23**

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

22 **Individual Victim 24**

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

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

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

8 **Individual Victim 25**

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

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

20 **Individual Victim 26**

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

28

1 **Individual Victim 27**

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

10 **Individual Victim 28**

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

18 **Individual Victim 29**

19 Overt Act No. 90: On January 19, 2023, after gaining  
20 unauthorized access to Individual Victim 29's account at a virtual  
21 currency exchange, defendant OSIEBO or a co-conspirator conducted a  
22 false and fraudulent transfer of virtual currency worth approximately  
23 \$4,010 originating from Individual Victim 29's account to a virtual  
24 currency address controlled by defendant OSIEBO and other co-  
25 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).

//

//

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

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

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

9 C. OVERT ACTS

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

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

19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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  
2  
3 1. Pursuant to Rule 32.2 of the Federal Rules of Criminal  
4 Procedure, notice is hereby given that the United States of America  
5 will seek forfeiture as part of any sentence, pursuant to Title 18,  
6 United States Code, Section 981(a)(1)(C) and Title 28, United States  
7 Code, Section 2461(c), in the event of any defendant's conviction of  
8 the offenses set forth in any of Counts One or Three of this First  
9 Superseding Indictment.

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

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

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

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

27 //

28 //

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

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

FORFEITURE ALLEGATION TWO

[18 U.S.C. §§ 982, 1030, and 1029]

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

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

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

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

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

20 3. Pursuant to Title 21, United States Code, Section 853(p),  
21 as incorporated by Title 18, United States Code, Sections 982(b)(1),  
22 1030(i), and 1029(c)(2), any defendant so convicted shall forfeit  
23 substitute property, up to the total value of the property described  
24 in the preceding paragraph if, as the result of any act or omission  
25 of said defendant, the property described in the preceding paragraph,  
26 or any portion thereof: (a) cannot be located upon the exercise of  
27 due diligence; (b) has been transferred, sold to or deposited with a  
28 third party; (c) has been placed beyond the jurisdiction of the

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

4  
5 A TRUE BILL

6  
7 /s/  
8 Foreperson

9 BILAL A. ESSAYLI  
10 United States Attorney

11 

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

15 KHALDOUN SHOBAKI  
16 Assistant United States Attorney  
17 Chief, Cyber and Intellectual  
18 Property Crimes Section

19 LAUREN RESTREPO  
20 Assistant United States Attorney  
21 Deputy Chief, Cyber and  
22 Intellectual Property Crimes  
23 Section