



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
June 2024 Grand Jury

UNITED STATES OF AMERICA,

CR No. 2:24-CR-00595-JWH

Plaintiff,

I N D I C T M E N T

v.

[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]

AHMED HOSSAM ELDIN ELBADAWY,
aka "AD,"
NOAH MICHAEL URBAN,
aka "Sosa,"
aka "Elijah,"
EVANS ONYEAKA OSIEBO, and
JOEL MARTIN EVANS,
aka "joeleoli,"

Defendants.

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS AND DEFINITIONS

At all times relevant to this 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 AHMED HOSSAM ELDIN ELBADAWY, also known as
15 ("aka") "AD" ("ELBADAWY"), was a resident of College Station, Texas.

16 4. Defendant NOAH MICHAEL URBAN, aka "Sosa," aka "Elijah"
17 ("URBAN"), was a resident of Palm Coast, Florida.

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

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

22 7. Unindicted co-conspirator 1 ("UICC 1") was a member of the
23 group, whose identity is known to the Grand Jury.

24 8. ELBADAWY, URBAN, OSIEBO, EVANS, and UICC 1 knowingly and
25 intentionally conspired with each other, and with persons known and
26 unknown to the Grand Jury, to conduct criminal cyber intrusions and
27 virtual currency thefts. The conspirators' victims and intended
28 victims included interactive entertainment companies,

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

6 9. The conspirators often targeted victims by sending SMS
7 phishing messages to Victim Company employees intended to make the
8 victims enter their employee login credentials into websites designed
9 to look like legitimate websites of a Victim Company or a Victim
10 Company's contracted telecommunications, IT, and BPO suppliers. Once
11 they gained unauthorized access to a Victim Company computer system,
12 defendants ELBADAWY, URBAN, OSIEBO, and UICC 1, together with other
13 co-conspirators, would conduct research within the system and attempt
14 to locate and copy confidential Victim Company data.

15 10. In some instances, defendants ELBADAWY, URBAN, OSIEBO, and
16 UICC 1, together with other co-conspirators, would gain access to the
17 computer systems of certain interactive entertainment Victim
18 Companies and use that access to give themselves or other co-
19 conspirators privileges or gifts. In other instances, defendants
20 ELBADAWY, URBAN, OSIEBO, and UICC 1, together with other co-
21 conspirators, would copy confidential databases from Victim Companies
22 and attempt to sell the information to others.

23 11. Using information obtained from Victim Company intrusions,
24 and combined with information from other sources, defendants
25 ELBADAWY, URBAN, OSIEBO, and UICC 1, together with other co-
26 conspirators, would also gain access to individual victims' virtual
27 currency accounts and wallets.

28

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

6 B. The Victim Companies

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

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

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

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

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

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

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

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

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

28

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

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

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

7 C. Definitions

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

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

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

26 28. SMS phishing is a type of phishing that transmits the
27 phishing message through text messages that are commonly sent over
28 Short Message Service (SMS) channels to mobile telephones but also

1 can be sent using non-SMS channels like data-based messaging
2 applications.

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

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

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

22 32. Virtual currency or cryptocurrency is a digital asset
23 designed to work as a medium of exchange that uses cryptography to
24 secure financial transactions, control the creation of additional
25 units of the currency, and verify the transfer of assets. Virtual
26 currency is typically accessed using secret or private encryption
27 keys which are commonly stored using a wallet. A virtual currency
28 wallet is a software application or hardware device that holds and

1 stores a user's virtual currency addresses and private keys. Some
2 wallets also allow users to send and receive cryptocurrency. Virtual
3 currency exchanges are platforms for buying, selling, and storing
4 virtual assets and can also allow for the exchange between different
5 types of virtual currencies, or between virtual currency and fiat
6 currency (e.g., U.S. dollars).

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

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 messages, defendants ELBADAWY, URBAN, OSIEBO, UICC 1, and co-
2 conspirators, would conduct internet research about their intended
3 victims and would send test SMS phishing messages to each other or
4 themselves.

5 c. Defendants ELBADAWY, URBAN, OSIEBO, UICC 1, and co-
6 conspirators would then use credentials stolen through SMS phishing
7 to access the accounts of Victim Company employees and the computer
8 systems of Victim Companies, to steal confidential information,
9 including confidential work product, intellectual property, and
10 personal identifying information, such as account access credentials,
11 names, email addresses, and telephone numbers.

12 d. Defendants ELBADAWY, URBAN, OSIEBO, UICC 1, and co-
13 conspirators would commit computer intrusions in order to obtain
14 personal identifying information of Victim Company employees and
15 customers that they would later use to identify potential victims,
16 fraudulently gain access to virtual currency accounts and wallets,
17 and transfer virtual currency from individual victims' virtual
18 currency accounts and wallets to accounts controlled by defendants
19 ELBADAWY, URBAN, OSIEBO, EVANS, UICC 1, and co-conspirators.

20 e. In order to fraudulently gain access to individual
21 victims' virtual currency wallets and accounts, and to bypass two
22 factor authentication security features, defendants ELBADAWY, URBAN,
23 OSIEBO, UICC 1, and co-conspirators, would (i) gain unauthorized
24 access to various online accounts of victims, including email
25 accounts; and (ii) conduct, or cause to be conducted, SIM swaps of
26 individual victims' mobile telephone numbers to devices that the
27 conspirators controlled.

28 f. In some instances, defendants ELBADAWY, URBAN, OSIEBO,

1 UICC 1, and co-conspirators would gain unauthorized access to the
2 computer systems of Victim Companies and use that access to modify
3 software configurations on the Victim Company system. In other
4 instances, after gaining unauthorized access to Victim Company
5 computer systems, defendants ELBADAWY, URBAN, OSIEBO, UICC 1, and co-
6 conspirators would copy confidential databases from Victim Companies
7 and attempt to sell the stolen information to others.

8 g. Defendants ELBADAWY, URBAN, OSIEBO, EVANS, UICC 1, and
9 co-conspirators would create, manage, and pay for infrastructure
10 needed for phishing attacks, including VPSs used to host phishing
11 websites and domain names for the phishing websites.

12 h. Defendant EVANS would create software used by
13 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, and co-conspirators to
14 conduct phishing attacks on Victim Company employees.

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

21 j. Defendants ELBADAWY, URBAN, OSIEBO, and UICC 1 would
22 possess the stolen login credentials and personal identifying
23 information of Victim Company employees and customers, and Individual
24 Victims, on digital devices for use in later SMS phishing attacks,
25 computer intrusions, and virtual currency thefts.

26 C. OVERT ACTS

27 36. On or about the following dates, in furtherance of the
28 conspiracy and to accomplish its object, defendants ELBADAWY, URBAN,

1 OSIEBO, EVANS, UICC 1, and co-conspirators committed various overt
2 acts within the Central District of California and elsewhere,
3 including, but not limited to, the following:

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

5 **Victim Company 1**

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

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

18 Overt Act No. 3: Beginning in or around June 2, 2022,
19 defendants ELBADAWY, URBAN, UICC 1, or other co-conspirators gained
20 unauthorized access to the computers of Victim Company 1 and used the
21 access to modify software configurations on Victim Company 1's
22 computers.

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

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

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

9 **Victim Company 2**

10 Overt Act No. 7: Beginning in or around May 2022, defendants
11 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators transmitted
12 or caused to be transmitted SMS phishing messages to the mobile
13 telephones of Victim Company 2 employees, causing at least one Victim
14 Company 2 employee to transmit their credentials via the phishing
15 websites provided in the SMS phishing messages.

16 Overt Act No. 8: On an unknown date in May or June 2022,
17 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators
18 gained unauthorized access to the computers of Victim Company 2 and
19 copied confidential data from Victim Company 2.

20 **Victim Company 3**

21 Overt Act No. 9: On June 2, 2022, defendants ELBADAWY, URBAN,
22 OSIEBO, UICC 1, or other co-conspirators transmitted or caused to be
23 transmitted SMS phishing messages to the mobile telephones of Victim
24 Company 3 employees, causing at least one Victim Company 3 employee
25 to transmit their credentials via the phishing websites provided in
26 the SMS phishing messages.

27 Overt Act No. 10: On or around June 2, 2022, defendants
28 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators gained

1 unauthorized access to the computers of Victim Company 3, accessed
2 confidential data from Victim Company 3, and made changes to Victim
3 Company 3 user accounts.

4 **Victim Company 4**

5 Overt Act No. 11: On June 2, 2022, defendants ELBADAWY, URBAN,
6 OSIEBO, UICC 1, or other co-conspirators transmitted or caused to be
7 transmitted SMS phishing messages to the mobile telephones of Victim
8 Company 4 employees, causing at least one Victim Company 4 employee
9 to transmit their credentials via the phishing websites provided in
10 the SMS phishing messages.

11 Overt Act No. 12: On or around June 2, 2022, defendants
12 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators gained
13 unauthorized access to the computers of Victim Company 4.

14 **Victim Company 5**

15 Overt Act No. 13: On June 2, 2022, defendants ELBADAWY, URBAN,
16 OSIEBO, UICC 1, or other co-conspirators transmitted or caused to be
17 transmitted SMS phishing messages to the mobile telephones of Victim
18 Company 5 employees, causing at least one Victim Company 5 employee
19 to transmit their credentials via the phishing websites provided in
20 the SMS phishing messages.

21 Overt Act No. 14: On an unknown date in June or July 2022,
22 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators
23 gained unauthorized access to computers of Victim Company 5 and
24 accessed confidential data.

25 **Victim Company 6**

26 Overt Act No. 15: On or before June 11, 2022, defendants
27 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators gained
28 unauthorized access to the computers of Victim Company 6 and copied

1 confidential data from Victim Company 6.

2 **Victim Company 7**

3 Overt Act No. 16: On July 19, 2022, defendants ELBADAWY,
4 URBAN, OSIEBO, UICC 1, or other co-conspirators transmitted or caused
5 to be transmitted SMS phishing messages to the mobile telephones of
6 Victim Company 7 employees, causing at least one Victim Company 7 to
7 employee transmit their credentials via the phishing websites
8 provided in the SMS phishing messages.

9 Overt Act No. 17: On or after July 19, 2022, defendants
10 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators gained
11 unauthorized access to the computers of Victim Company 7 and copied
12 confidential data from Victim Company 7.

13 Overt Act No. 18: On September 26, 2022, via Telegram,
14 defendant ELBADAWY and UICC 1 discussed with another Telegram user
15 selling an exported database of registration identifiers, email
16 addresses, and partial telephone numbers of accountholders of a
17 virtual currency exchange, stolen from the computers of Victim
18 Company 7.

19 **Victim Company 8**

20 Overt Act No. 19: On an unknown date in 2022, defendants
21 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators transmitted
22 or caused to be transmitted SMS phishing messages to the mobile
23 telephones of Victim Company 8 employees, causing at least one Victim
24 Company 8 employee to transmit their credentials via the phishing
25 websites provided in the SMS phishing messages.

26 Overt Act No. 20: On an unknown date in 2022, defendants
27 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators gained
28 unauthorized access to the computer network of Victim Company 8 and

1 copied data from Victim Company 8.

2 **Victim Company 9**

3 Overt Act No. 21: On or before December 19, 2022, defendants
4 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators transmitted
5 or caused to be transmitted SMS phishing messages to the mobile
6 telephones of Victim Company 9 employees, causing at least one Victim
7 Company 9 employee to transmit their credentials via the phishing
8 websites provided in the SMS phishing messages.

9 Overt Act No. 22: On or after December 19, 2022, defendants
10 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators gained
11 unauthorized access to at least one Victim Company 9 employee account
12 and reset their password.

13 Overt Act No. 23: On or after December 19, 2022, defendants
14 ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators gained
15 unauthorized access to the computers of Victim Company 9 and accessed
16 confidential data of Victim Company 9.

17 **Maintenance of Online Infrastructure and Possession of Stolen Access**

18 **Devices**

19 Overt Act No. 24: On December 3, 2021, UICC 1 saved a screen
20 capture of messages with defendant EVANS in which defendant EVANS
21 states, in part, "do u have multiple [Victim Company 5] api accs?
22 They rate limit to 10k per hour by key and ip."

23 Overt Act No. 25: On March 8, 2022, UICC 1 saved a screen
24 capture of messages with defendant EVANS in which UICC 1 sent
25 defendant EVANS a list of potential phishing domain names, including
26 a phishing domain name related to Victim Company 5.

27 Overt Act No. 26: Between at least March 21, 2022 and August
28 1, 2022, along with UICC 1, defendant EVANS was an administrator of a

1 Telegram channel that received fraudulently obtained login
2 credentials from Victim Company employees.

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

5 Overt Act No. 28: Between May 21, 2022 and June 17, 2022,
6 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators
7 registered phishing domains with names suggesting they were
8 associated with Victim Company 10.

9 Overt Act No. 29: On May 28, 2022, defendants ELBADAWY, URBAN,
10 OSIEBO, UICC 1, or other co-conspirators registered a phishing domain
11 with a name suggesting it was associated with Victim Company 2.

12 Overt Act No. 30: Between May 28, 2022 and July 25, 2022,
13 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators
14 registered phishing domains with names suggesting they were
15 associated with Victim Company 8.

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

20 Overt Act No. 32: Between May 29, 2022 and June 3, 2022,
21 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators
22 registered phishing domains with names suggesting they were
23 associated with Victim Company 11.

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

1 Overt Act No. 34: On May 31, 2022, defendant URBAN entered
2 test credentials into a phishing website to confirm the website was
3 properly functioning.

4 Overt Act No. 35: On June 2, 2022, defendants ELBADAWY, URBAN,
5 OSIEBO, UICC 1, or other co-conspirators registered a phishing domain
6 with a name suggesting it was associated with Victim Company 3.

7 Overt Act No. 36: On June 2, 2022, defendants ELBADAWY, URBAN,
8 OSIEBO, UICC 1, or other co-conspirators registered phishing domains
9 with names suggesting they were associated with Victim Company 4.

10 Overt Act No. 37: On June 2, 2022, defendants ELBADAWY, URBAN,
11 OSIEBO, UICC 1, or other co-conspirators registered phishing domains
12 with names suggesting they were associated with Victim Company 5.

13 Overt Act No. 38: Between June 4, 2022 and June 9, 2022,
14 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators
15 registered phishing domains with names suggesting they were
16 associated with Victim Company 11.

17 Overt Act No. 39: Between June 12, 2022 and July 27, 2022,
18 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or other co-conspirators
19 registered phishing domains with names suggesting they were
20 associated with Victim Company 6.

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

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

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

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

7 Overt Act No. 44: On March 1, 2023, at his residence in
8 College Station, Texas, in a Telegram export file, defendant ELBADAWY
9 possessed the login credentials for numerous Victim Company
10 employees, including the login credentials for approximately 7 Victim
11 Company 1 employees, 36 Victim Company 2 employees, two Victim
12 Company 3 employees, one Victim Company 4 employee, four Victim
13 Company 5 employees, 50 Victim Company 6 employees, 29 Victim Company
14 8 employees, five Victim Company 10 employees, and 63 Victim Company
15 11 employees.

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

20 Overt Act No. 46: On April 12, 2023, on digital devices found
21 at UICC 1’s residence, UICC 1 possessed files related to Victim
22 Companies, including employee directories of Victim Companies 6, 8,
23 9, and 12; email addresses for approximately 80 Victim Company 10
24 employees; and nonpublic files containing business-related
25 information for Victim Company 11.

26 Overt Act No. 47: On April 12, 2023, on a digital device found
27 at UICC 1’s residence, UICC 1 possessed an exported database of
28 registration identifiers, email addresses, and partial telephone

1 numbers of accountholders of a virtual currency exchange.

2 Overt Act No. 48: On April 12, 2023, on a digital device found
3 at UICC 1's residence, UICC 1 possessed the names and email addresses
4 of Individual Victims 18, 19, 20, 22, 23, 24, 27, and 29.

5 **Virtual Currency Thefts**

6 **Individual Victim 1**

7 Overt Act No. 49: On September 25 and 26, 2021, after gaining
8 unauthorized access to Individual Victim 1's personal email account
9 and virtual currency wallets, defendant ELBADAWY or a co-conspirator
10 conducted false and fraudulent transfers of virtual currency worth
11 approximately \$6,347,605 originating from Individual Victim 1's
12 wallets to virtual currency addresses controlled by defendant
13 ELBADAWY, UICC 1, and other co-conspirators.

14 **Individual Victim 2**

15 Overt Act No. 50: On May 31, 2022, after gaining unauthorized
16 access to Individual Victim 2's virtual currency wallet, defendant
17 ELBADAWY, UICC 1, or a co-conspirator conducted false and fraudulent
18 transfers of virtual currency worth approximately \$266,988
19 originating from Individual Victim 2's wallet to virtual currency
20 addresses controlled by defendant ELBADAWY, UICC 1, and other co-
21 conspirators. Individual Victim 2 was a resident of the Central
22 District of California.

23 **Individual Victim 3**

24 Overt Act No. 51: On June 6, 2022, after gaining unauthorized
25 access to Individual Victim 3's account at a virtual currency
26 exchange, defendant ELBADAWY or a co-conspirator conducted false and
27 fraudulent transfers of virtual currency worth approximately \$571,413
28

1 originating from Individual Victim 3's account to virtual currency
2 addresses controlled by defendant ELBADAWY and other co-conspirators.

3 **Individual Victim 4**

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

11 Overt Act No. 53: On June 11, 2022, defendant ELBADAWY or
12 another co-conspirator used a portion of the funds stolen from
13 Individual Victim 4 to pay for an account used to register phishing
14 domains.

15 **Individual Victim 5**

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

22 **Individual Victim 6**

23 Overt Act No. 55: On July 14, 2022, after gaining unauthorized
24 access to Individual Victim 6's account at a virtual currency
25 exchange, defendant URBAN or a co-conspirator conducted false and
26 fraudulent transfers of virtual currency worth approximately \$60,010
27 originating from Individual Victim 6's account to virtual currency
28 addresses controlled by defendants ELBADAWY, URBAN, OSIEBO, UICC 1,

1 and other co-conspirators.

2 **Individual Victim 7**

3 Overt Act No. 56: On July 15, 2022, after gaining unauthorized
4 access to Individual Victim 7's account at a virtual currency
5 exchange, defendants ELBADAWY, URBAN, OSIEBO, UICC 1, or a co-
6 conspirator conducted false and fraudulent transfers of virtual
7 currency worth approximately \$199,456 originating from Individual
8 Victim 7's account to virtual currency addresses controlled by
9 defendants ELBADAWY, URBAN, OSIEBO, UICC 1, and other co-
10 conspirators.

11 **Individual Victim 8**

12 Overt Act No. 57: On or before July 15, 2022, defendants
13 ELBADAWY, URBAN, OSIEBO, UICC 1, or a co-conspirator conducted or
14 caused to be conducted a SIM swap of Individual Victim 8's telephone
15 number.

16 Overt Act No. 58: On July 15, 2022, after gaining unauthorized
17 access to Individual Victim 8's account at a virtual currency
18 exchange, defendants ELBADAWY, URBAN, UICC 1 or a co-conspirator
19 conducted false and fraudulent transfers of virtual currency worth
20 approximately \$199,116 originating from Individual Victim 8's account
21 to virtual currency addresses controlled by defendants ELBADAWY,
22 URBAN, UICC 1, and other co-conspirators.

23 **Individual Victim 9**

24 Overt Act No. 59: On July 18, 2022, after gaining unauthorized
25 access to Individual Victim 9's personal email account and virtual
26 currency wallet, defendant ELBADAWY or a co-conspirator, conducted
27 false and fraudulent transfers of virtual currency worth
28 approximately \$413,004 originating from Individual Victim 9's wallet

1 to virtual currency addresses controlled by defendant ELBADAWY and
2 other co-conspirators. Individual Victim 9 was a resident of the
3 Central District of California.

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

7 **Individual Victim 10**

8 Overt Act No. 61: On July 18, 2022, after gaining unauthorized
9 access to Individual Victim 10's account at a virtual currency
10 exchange, defendants ELBADAWY, OSIEBO, or a co-conspirator conducted
11 false and fraudulent transfers of virtual currency worth
12 approximately \$19,573 originating from Individual Victim 10's account
13 to virtual currency addresses controlled by defendant ELBADAWY and
14 other co-conspirators.

15 **Individual Victim 11**

16 Overt Act No. 62: On or before July 21, 2022, defendants
17 ELBADAWY, URBAN, OSIEBO, UICC 1, or a co-conspirator conducted or
18 caused to be conducted a SIM swap of Individual Victim 11's telephone
19 number.

20 Overt Act No. 63: On July 21, 2022, after gaining unauthorized
21 access to Individual Victim 11's account at a virtual currency
22 exchange, defendants URBAN, OSIEBO, UICC 1, or a co-conspirator
23 conducted false and fraudulent transfers of virtual currency worth
24 approximately \$40,411 originating from Individual Victim 11's account
25 to virtual currency addresses controlled by defendants URBAN, OSIEBO,
26 EVANS, UICC 1, and other co-conspirators.

27 **Individual Victim 12**

28 Overt Act No. 64: On July 21, 2022, after gaining unauthorized

1 access to Individual Victim 12's account at a virtual currency
2 exchange, defendant URBAN, UICC 1, or a co-conspirator conducted
3 false and fraudulent transfers of virtual currency worth
4 approximately \$9,179 originating from Individual Victim 12's account
5 to virtual currency addresses controlled by defendant URBAN, UICC 1,
6 and other co-conspirators.

7 **Individual Victim 13**

8 Overt Act No. 65: On July 22, 2022, after gaining unauthorized
9 access to Individual Victim 13's account at a virtual currency
10 exchange, defendants ELBAWADY, URBAN, UICC 1, or a co-conspirator
11 conducted false and fraudulent transfers of virtual currency worth
12 approximately \$16,910 originating from Individual Victim 13's account
13 to virtual currency addresses controlled by defendants ELBADAWY,
14 URBAN, EVANS, UICC 1, and other co-conspirators.

15 **Individual Victim 14**

16 Overt Act No. 66: On October 31, 2022, after gaining
17 unauthorized access to Individual Victim 14's account at a virtual
18 currency exchange, defendant ELBADAWY, UICC 1, or a co-conspirator
19 conducted false and fraudulent transfers of virtual currency worth
20 approximately \$32,302 originating from Individual Victim 14's account
21 to virtual currency addresses and wallets controlled by defendants
22 ELBADAWY, URBAN, UICC 1, and other co-conspirators.

23 **Individual Victim 15**

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

27 Overt Act No. 68: On November 9, 2022, after gaining
28 unauthorized access to Individual Victim 15's virtual currency

1 wallet, defendant ELBADAWY or a co-conspirator conducted false and
2 fraudulent transfers of virtual currency worth approximately \$152,205
3 originating from Individual Victim 15's wallets to virtual currency
4 addresses controlled by defendant ELBADAWY and other co-conspirators.

5 **Individual Victim 16**

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

9 Overt Act No. 70: On November 17, 2022, after gaining
10 unauthorized access to Individual Victim 16's virtual currency
11 wallet, defendant ELBADAWY or a co-conspirator conducted false and
12 fraudulent transfers of virtual currency worth approximately \$35,647
13 originating from Individual Victim 16's wallet to virtual currency
14 addresses and wallets controlled by defendant ELBADAWY and other co-
15 conspirators.

16 **Individual Victim 17**

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

24 **Individual Victim 18**

25 Overt Act No. 72: On November 29, 2022, after gaining
26 unauthorized access to Individual Victim 18's account at a virtual
27 currency exchange, defendant ELBADAWY or a co-conspirator conducted
28 false and fraudulent transfers of virtual currency worth

1 approximately \$11,842 originating from Individual Victim 18's account
2 to virtual currency addresses controlled by defendants ELBADAWY,
3 OSIEBO, UICC 1, and other co-conspirators.

4 **Individual Victim 19**

5 Overt Act No. 73: On December 3, 2022, via Telegram, UICC 1
6 sent defendant ELBADAWY the name and email address of Individual
7 Victim 19 with the words "highnetworth" and "funded."

8 Overt Act No. 74: On December 4, 2022, after gaining
9 unauthorized access to Individual Victim 19's account at a virtual
10 currency exchange and a separate virtual currency wallet, defendant
11 ELBADAWY, UICC 1, or a co-conspirator conducted false and fraudulent
12 transfers of virtual currency worth approximately \$195,766
13 originating from Individual Victim 19's account and wallet to virtual
14 currency addresses controlled by defendants ELBADAWY, URBAN, UICC 1,
15 and other co-conspirators. Individual Victim 19 was a resident of
16 the Central District of California.

17 **Individual Victim 20**

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

21 Overt Act No. 76: On or before December 4, 2022, defendant
22 ELBADAWY, UICC 1, or a co-conspirator conducted or caused to be
23 conducted a SIM swap of Individual Victim 20's telephone number.

24 Overt Act No. 77: On December 4, 2022, after gaining
25 unauthorized access to Individual Victim 20's account at a virtual
26 currency exchange, defendant ELBADAWY, UICC 1, or a co-conspirator
27 conducted false and fraudulent transfers of virtual currency worth
28 approximately \$129,586 originating from Individual Victim 20's

1 account to virtual currency addresses controlled by defendant
2 ELBADAWY, UICC 1, and other co-conspirators.

3 **Individual Victim 21**

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

11 **Individual Victim 22**

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

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

22 **Individual Victim 23**

23 Overt Act No. 81: On December 7, 2022, after gaining
24 unauthorized access to Individual Victim 23's virtual currency
25 wallets, defendant ELBADAWY, UICC 1, or a co-conspirator conducted
26 false and fraudulent transfers of virtual currency worth
27 approximately \$57,800 originating from Individual Victim 23's wallet
28

1 to virtual currency addresses controlled by defendant ELBADAWY and
2 other co-conspirators.

3 **Individual Victim 24**

4 Overt Act No. 82: On December 11, 2022, defendant ELBADAWY
5 sent UICC 1 the name and email addresses of Individual Victim 24.

6 Overt Act No. 83: On or before December 11, 2022, defendant
7 ELBADAWY, UICC 1, or a co-conspirator conducted or caused to be
8 conducted a SIM swap of Individual Victim 24's telephone number.

9 Overt Act No. 84: On December 11, 2022, after gaining
10 unauthorized access to Individual Victim 24's account at a virtual
11 currency exchange, defendant ELBADAWY, UICC 1, or a co-conspirator
12 conducted false and fraudulent transfers of virtual currency worth
13 approximately \$34,861 originating from Individual Victim 24's account
14 to virtual currency addresses controlled by defendant ELBADAWY, UICC
15 1, and other co-conspirators.

16 **Individual Victim 25**

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

20 Overt Act No. 86: On or after December 18, 2022, after gaining
21 unauthorized access to Individual Victim 25's account at a virtual
22 currency exchange and a separate virtual currency wallet, defendant
23 ELBADAWY or a co-conspirator conducted false and fraudulent transfers
24 of virtual currency worth approximately \$209,572 originating from
25 Individual Victim 26's account and wallet to virtual currency
26 addresses controlled by defendants ELBADAWY, OSIEBO, UICC 1, and
27 other co-conspirators.

1 **Individual Victim 26**

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

9 **Individual Victim 27**

10 Overt Act No. 88: On January 1, 2023, after gaining
11 unauthorized access to Individual Victim 27's account at a virtual
12 currency exchange, defendant ELBADAWY, UICC 1, or a co-conspirator
13 conducted false and fraudulent transfers of virtual currency worth
14 approximately \$17,135 originating from Individual Victim 27's account
15 to virtual currency addresses controlled by defendant ELBADAWY, UICC
16 1, and other co-conspirators. Individual Victim 27 was a resident of
17 the Central District of California.

18 **Individual Victim 28**

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

26 **Individual Victim 29**

27 Overt Act No. 90: On January 19, 2023, after gaining
28 unauthorized access to Individual Victim 29's account at a virtual

1 currency exchange, defendant OSIEBO or a co-conspirator conducted a
2 false and fraudulent transfer of virtual currency worth approximately
3 \$4,010 originating from Individual Victim 29's account to a virtual
4 currency address controlled by defendant OSIEBO and other co-
5 conspirators.

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

1 COUNT TWO

2 [18 U.S.C. § 371]

3 [ALL DEFENDANTS]

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

7 A. OBJECTS OF THE CONSPIRACY

8 37. Beginning on a date unknown to the Grand Jury, but no later
9 than September 25, 2021, and continuing through on or about April 12,
10 2023, in Los Angeles and Orange Counties, within the Central District
11 of California, and elsewhere, defendants ELBADAWY, URBAN, OSIEBO,
12 EVANS, and UICC 1, and others known and unknown to the Grand Jury,
13 knowingly conspired and agreed with each other to:

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

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

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

25 //

26 //

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 Indictment as if fully set
8 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 ELBADAWY, URBAN,
12 OSIEBO, EVANS, and UICC 1, and co-conspirators committed various
13 overt acts within the Central District of California and elsewhere,
14 including, but not limited to, the following:

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

18
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 13, 2023, in Los Angeles and Orange Counties, within the Central District of California, and elsewhere, defendants AHMED HOSSAM ELDIN ELBADAWY, also known as ("aka") "AD," ("ELBADAWY"), NOAH MICHAEL URBAN, aka "Sosa," aka "Elijah," ("URBAN"), EVANS ONYEAKA OSIEBO ("OSIEBO"), JOEL MARTIN EVANS, aka "joeleoli," ("EVANS"), each aiding and abetting the other, knowingly transferred, possessed, and used, without lawful authority, a means of identification that defendants ELBADAWY, URBAN, OSIEBO, and EVANS, knew belonged to other persons, 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 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 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

//

//

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 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 E. MARTIN ESTRADA
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

24 SUE BAI
25 Assistant United States Attorney
26 Terrorism and Export Crimes
27 Section
28