IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on August 1, 2024

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
v.	:	**GRAND JURY ORIGINAL**
	:	
MASOUD JALILI,	:	**VIOLATIONS:**
	:	
a/k/a Masud Jalili,	:	**18 U.S.C. §§ 371, 1028(a)(7), 1028A,**
a/k/a Mas'ud Jalili,	:	**1029(a)(2), 1030(a)(2), 1030(a)(4), 1343,**
a/k/a مسعود جلیلی,	:	**1028A, and 3559(g)**
	:	**(Conspiracy to Obtain Information from**
SEYYED ALI AGHAMIRI,	:	**a Protected Computer; Defraud and**
	:	**Obtain a Thing of Value; Commit Fraud**
a/k/a سید علی آقامیری,	:	**Involving Authentication Features;**
	:	**Commit Aggravated Identity Theft;**
and	:	**Commit Access Device Fraud; and**
	:	**Commit Wire Fraud While Falsely**
YASAR BALAGHI,	:	**Registering Domains)**
	:	
a/k/a یاسر بلاغی,	:	**18 U.S.C. § 2339B(a)(1)**
	:	**(Material Support to Designated Foreign**
	:	**Terrorist Organization)**
	:	
	:	**18 U.S.C. § 1343**
	:	**(Wire Fraud)**
Defendants.	:	
	:	**18 U.S.C. § 1028A**
	:	**(Aggravated Identity Theft)**
	:	
	:	**18 U.S.C. § 2**
	:	**(Aiding and Abetting)**
	:	
	:	**Criminal Forfeiture:**
	:	**18 U.S.C. § 981(a)(1)(C); 18 U.S.C.**
	:	**§ 981 (a)(1)G); 18 U.S.C. § 982(a)(2)(B);**
	:	**18 U.S.C. § 1028(b)(5); 18 U.S.C.**
	:	**§ 1029(c)(1)(C); 18 U.S.C.**
	:	**§§ 1030(i)(1)(A)-(B); 28 U.S.C. § 2461(c);**
	:	**and 21 U.S.C. § 853(p).**

INDICTMENT

The Grand Jury charges that, at all times material to this Indictment, on or about the dates and times stated below:

INTRODUCTION

1. Beginning in or around January 2020, and continuing through at least September 2024, malicious cyber actors employed by the Islamic Republic of Iran's ("Iran") Islamic Revolutionary Guard Corps ("IRGC"), Masoud Jalili ("JALILI"), Seyyed Ali Aghamiri ("AGHAMIRI"), Yaser Balaghi ("BALAGHI"), and other persons known and unknown to the Grand Jury (collectively, "Conspirators"), prepared for and engaged in a wide-ranging hacking campaign that used spearphishing and social engineering techniques to target and compromise the accounts of current and former U.S. government officials, members of the media, nongovernmental organizations, and individuals associated with U.S. political campaigns. Such activity is part of Iran's continuing efforts to stoke discord, erode confidence in the U.S. electoral process, and unlawfully acquire information relating to current and former U.S. officials that could be used to advance the malign activities of the IRGC, including ongoing efforts to avenge the death of Qasem Soleimani, the former commander of the IRGC – Qods Force ("IRGC-QF").

2. Of particular note, in or around May 2024, after several years of focusing on compromising the accounts of current and former U.S. government officials, and using some of the same hacking infrastructure from earlier in the conspiracy, the Conspirators began targeting, and successfully gaining unauthorized access to, personal accounts belonging to persons associated with an identified U.S. presidential campaign ("U.S. Presidential Campaign 1"), including campaign officials. The Conspirators used their access to those accounts to steal, among other information, non-public campaign documents and emails ("campaign material"). The

activity broadened in late June 2024, when the Conspirators engaged in a "hack-and-leak" operation, in which they sought to weaponize campaign material stolen from U.S. Presidential Campaign 1 by leaking such materials to members of the media and individuals that the Conspirators believed were associated with what was then another identified U.S. presidential campaign ("U.S. Presidential Campaign 2"), in a deliberate effort to, as reflected in the Conspirators' own words and actions, undermine U.S. Presidential Campaign 1 in advance of the 2024 U.S. presidential election.

3. The Conspirators used sophisticated means to fraudulently access the victims' protected computers and accounts without authorization. The Conspirators created multiple fraudulent persona email accounts ("persona accounts")—that is, email accounts that impersonated publicly known persons or organizations, including current and former U.S. government officials, by using their names in the email account name or domain name, but which accounts were actually controlled by the Conspirators. These persona accounts were designed to trick recipients of emails from the persona accounts into believing that they were interacting with a trusted or known source. In fact, the persona accounts were used to send spearphishing emails—that is, emails designed to further deceive the victim into clicking a link or opening an attachment that would download malware or navigate to a malicious website—to compromise victim computers and accounts. Upon a successful compromise, the Conspirators often used their resulting unauthorized access to such victim computers and accounts to send new spearphishing emails to additional victims, leveraging those additional victims' misplaced trust in the compromised sending email accounts. After obtaining unauthorized access to victim computers and accounts, the Conspirators would also steal data from those accounts.

4. The Conspirators obtained initial unauthorized access to protected computers through U.S. wires and using a variety of tools, techniques, and procedures that they shared among themselves over the course of the conspiracy, including: using static Internet Protocol ("IP") addresses provided by Respina Networks and Beyond ("Respina Networks") and Farabord Dadeh Haye Iranian Company ("FDI"); using virtual private networks ("VPNs") to obscure their true location; creating persona accounts; creating "spoofed" login pages; sending emails using compromised accounts; using social engineering to obtain victims' login information and multi-factor recovery/authentication codes; using malware to gain remote access to compromised computers and accounts; and using cloud service providers to host malware and other hacking infrastructure. In some cases, the Conspirators also maintained long-term, persistent access to compromised accounts.

Background on Relevant Individuals and Entities

5. On April 15, 2019, the United States Secretary of State designated the IRGC as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act. To date, the IRGC remains a designated FTO.[1] On October 22, 2020, the IRGC was

[1] Also known as IRGC; Islamic Revolutionary Guards Corps; Islamic Revolution Guards Corps; Iran's Revolutionary Guard Corps; Islamic Revolutionary Corps; IRG; The Iranian Revolutionary Guards; Islamic Revolutionary Guards; Iran's Revolutionary Guards; Revolutionary Guards; Revolutionary Guard; Army of the Guardians of the Islamic Revolution; The Army of the Guardians of the Islamic Revolution; AGIR; Pasdaran; Pasdaran-e Inqilab; Pasdarn-e Enghelab-e Islami; Sepah; Sepah Pasdaran; Sepah-e Pasdaran-e Enghelab-e Eslami; Sepah-e Pasdaran Enghelab Islami; Islamic Revolutionary Guard Corps-Qods Force; IRGC-Quds Force; IRGC-QF; Qods Force; Sepah-e Qods; Jerusalem Force; Al Qods; Islamic Revolutionary Guard Corps (IRGC)-Qods Force; Pasdaran-e Enghelab-e Islami (Pasdaran); Sepah-e Qods (Jerusalem Force); Qods (Jerusalem) Force of the IRGC; Quds Force; IRGC Ground Forces; Islamic Revolution Guards Corps Ground Force; Basij; Baseej; Basij-e Melli; Islamic Revolution Guards Corps Resistance Force; Basij Resistance Forces; Mobilization of the Oppressed; Mobilization of the Oppressed Unit; Mobilization of the Oppressed Organization; Organization of the Mobilisation of the Oppressed; Sazman Basij Melli; Sazman-e Moghavemat-e Basij; Sazeman-e Basij-e Mostazafan; Vahed-e Basij-e Mostazafeen; Vahed-e Basij Mostaza'feen; National Mobilization

designated by the U.S. Department of the Treasury, Office of Foreign Asset Control, pursuant to Executive Order 13848, for having directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign influence in the 2020 U.S. presidential election.

6. Among its activities hostile to the United States and its allies, the IRGC actively targeted nationals of the United States and its allies living in countries around the world for kidnapping and/or execution, both to repress and silence dissidents critical of the Iranian regime and to take vengeance for the death of Qasem Soleimani, who was killed by a U.S. drone strike in Baghdad on or about January 3, 2020. For example, in 2022, U.S. law enforcement detected and disrupted an IRGC plot to murder a former U.S. National Security Advisor in or around Washington, D.C.

7. The Basij Resistance Force, also known as بسیج, Niru-ye Moghavamat-e Basij, and Sazman-e Basij-e Mostaz'afin ("Basij"), was a paramilitary volunteer militia of the IRGC.

8. During all times material to this Indictment, JALILI was a citizen of Iran, whose last known residence is in Tehran, Iran. The following was a passport/identification photograph of JALILI (Image One):

Organization; National Resistance Mobilization; Resistance Mobilization Force; Nirooye Moghavemate Basij; Niruyeh Moghavemat Basij; IRGC Air Force; Islamic Revolution Guards Corps Air Force; Islamic Revolutionary Guards Corps Air Force; Islamic Revolutionary Guard Corps Air Force; IRGCAF; Sepah Pasdaran Air Force; Air Force, IRGC (Pasdaran); Islamic Revolutionary Guards Corps Aerospace Force; Aerospace Force of the Army of the Guardians of the Islamic Revolution; AFAGIR; Aerospace Division of IRGC; IRGC Aerospace Force; IRGCASF; IRGC Navy; Islamic Revolution Guards Corps Naval Force.

Image One

9. JALILI was a skilled computer hacking operator since at least 2012, who taught others computer networking and hacking skills, and has identified himself as a "Master of Information Technology." JALILI worked for the Basij since at least 2005, and claimed to have hacked a number of targets, including Israeli targets. JALILI worked with known Basij members who have specialized skills in cyberattacks, including AGHAMIRI and BALAGHI.

10. JALILI also had a business relationship with Respina Networks, a telecommunications and internet service provider based in Iran, since at least 2018, when he entered into a contract to purchase dedicated, high-speed internet access from Respina Networks. JALILI's purpose in entering into this contract was to obtain infrastructure and unrestricted internet access outside of Iran for the Conspirators to use in furtherance of covert hacking campaigns on behalf of the IRGC. Specifically, the contract provided high bandwidth and high-speed internet access with access outside Iran to a block of eight static IP addresses for a location

in and around the address of No. 68/1 Maleklou Street, Tehran, Iran ("Malekloo Office"), which was located in the area of the map below (Image Two).

Image Two

Image Three was an open source photograph of the area around the exterior of the Malekoo Office:

Image Three

The nameplate above the left door in Image Three in Farsi matches the name on the Respina Networks contract entered into by JALILI for the static IP addresses.

11. During all times material to this Indictment, AGHAMIRI was a citizen of Iran, whose last known residence is in Tehran, Iran. The following was a photograph of AGHAMIRI (Image Four):

Image Four

AGHAMIRI was a graduate of Islamic Azad University and a skilled computer hacking operator. AGHAMIRI also worked for the Basij during the conspiracy period. On numerous occasions in or around 2020, 2021, 2022 and 2023, AGHAMIRI regularly traveled to and from the Malekloo Office.

12. During all times material to this Indictment, Asghar Balaghi ("BALAGHI") was a citizen of Iran, whose last known residence is in Tehran, Iran. The following was a photograph of BALAGHI associated with a public software account (Image Five):

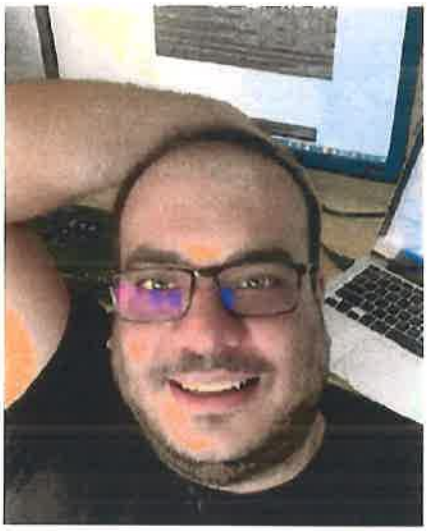

Image Five

BALAGHI was a skilled computer hacking operator who has been hacking in Iran since at least 2012 and who worked for the Basij during the conspiracy period. According to a 2013 resume (originally in Farsi and English), BALAGHI held a bachelor's degree in computer software from Islamic Azad University—the same university as JALILI and AGHAMIRI—and was the "Head of Security and Hacking (legal and ethical)" for an undisclosed client. BALAGHI's public resume claimed the following accomplishments and projects: designed "Phishing Attacks Systems," "Brute Force Software," "File Binder Software," "a Windows Malware in Python language," and "accomplished tens of hacking projects," that were "ordered by a cyber-organization." BALAGHI also indicated he had experience "designing and executing a lot of software projects and also hack tools and miscellaneous projects." On at least ten separate days in or around 2020, 2021, 2022 and 2023, BALAGHI traveled to and from the Malekloo Office.

13. At all relevant times, all of the Conspirators known to the Grand Jury were foreign nationals, and none of the Conspirators were known to have ever resided in the United States.

14. Respina Networks and FDI were telecommunications and internet service providers based in Iran. As mentioned in paragraph 10, JALILI had a long-term contractual relationship with Respina Networks. Since at least 2018, Respina Networks and FDI provided dedicated and unrestricted internet services to the Conspirators that they used in their hacking campaigns, including a Respina Networks IP address ending in 106 ("Respina Networks 106 IP") and an FDI IP address ending in 117 ("FDI 117 IP"). As detailed herein, the Conspirators used FDI 117 IP, in particular, throughout the entire conspiracy period.

15. On or about December 19, 2018, the Conspirators fraudulently opened an account in the name of an Israeli politician based in Tel Aviv with a U.S. service provider that hosts email accounts and registers internet domains ("Provider 1"). Between July 2021 and May 2022, the Conspirators used this account to knowingly falsely register at least four domains, which they used in their hacking activity described below.

U.S. Government, Members of the Media, and Nongovernmental Organization Victims and Attempted Victims

16. The Conspirators' hacking activity, from at least January 2020 to May 2024, targeted and attempted to compromise (without indications of success) the personal or official email accounts of dozens of senior, current and former prominent public officials (including heads of departments and agencies, deputies of departments and agencies, senior National Security Council officials, and ambassadors), and in some cases their aids or assistants, who served across several presidential administrations. These officials held or currently hold positions at: the U.S. Department of Justice; the U.S. Department of Defense; the U.S. State Department; the U.S. Agency for International Development; the National Security Agency; the Central Intelligence Agency ("C.I.A."); the White House; the National Security Council; the U.S. Senate; and the U.S. House of Representatives. During this period, the Conspirators' hacking activity also targeted,

and attempted to compromise (without indications of success), former officials for the U.N., Afghanistan, and a foreign government's intelligence service; three members of the media, including a national security correspondent for a major newspaper, an author and a columnist for a major U.S. newspaper and their assistant; and at least five employees of nongovernmental organizations, including two individuals specializing in human rights advocacy and senior fellows at three Washington, D.C.-based think tanks.

17. In addition to the attempted compromises described in paragraph 16, between in or around July 2021 and through at least May 2024, the Conspirators' targeting efforts led to successful compromises of numerous persons and entities, including but not limited to, persons and entities like those listed below in paragraphs 18 through 26, alongside the positions that the persons held at the at the time of such targeting.

18. U.S. Victim 1 was a former senior government employee at the U.S. Department of State, who was previously responsible for Middle East policy for the U.S. government and involved in negotiating diplomatic efforts, including the Abraham Accords. Two of U.S. Victim 1's personal email accounts were successfully compromised by the Conspirators.

19. United Arab Emirates ("U.A.E.") Victim 2 was an organization that promotes security and peace in the Middle East and was funded by the U.A.E. Ministry of Foreign Affairs.

20. U.S. Victim 3 was a U.S.-based author of at least two books about Iran. U.S. Victim 3's personal email account was successfully compromised by the Conspirators.

21. U.S. Victim 4 was a journalist, a fellow at a Washington, D.C.-based think tank, and a fellow at the United States Institute of Peace, who has expertise in U.S. foreign policy in the Middle East. U.S. Victim 4's personal email account was successfully compromised by the Conspirators.

22. U.S. Victim 5 was the former Homeland Security Advisor to a former U.S. President. U.S. Victim 5's personal email account was successfully compromised by the Conspirators.

23. U.S. Victim 6 was a former senior official at the C.I.A. U.S. Victim 6's work email account was successfully compromised by the Conspirators.

24. U.S. Victim 7 was a former U.S. Ambassador to Israel and a fellow at a Washington, D.C. based think tank that advises policy makers on U.S. foreign policy in the Middle East. U.S. Victim 7's personal email account was successfully compromised by the Conspirators.

25. U.S. Victim 8 was a former deputy director of the C.I.A. U.S. Victim 8's personal email account was successfully compromised by the Conspirators.

26. U.S. Victim 9 was a human rights advocate and co-founder and research director of an Iranian human rights organization. U.S. Victim 9's personal email account was successfully compromised by the Conspirators.

The Campaign-Related Victims and Attempted Victims

27. Between in or around May 2024 and through at least September 2024, the Conspirators' targeting efforts led to the attempted compromises and successful compromises of the following individuals associated with a U.S. presidential campaign listed below in paragraphs 29 through 33, alongside the positions that the persons held at the at the time of such targeting.

28. U.S. Presidential Campaign 1 was a U.S. presidential campaign in the 2024 election.

29. U.S. Victim 10 was a former, informal political consultant to the Presidential candidate of U.S. Presidential Campaign 1. Two of U.S. Victim 10's personal email accounts were successfully compromised by the Conspirators.

30. U.S. Victim 11 was an official for U.S. Presidential Campaign 1. U.S. Victim 11's personal email account was successfully compromised by the Conspirators.

31. U.S. Victim 12 was an attorney representing the Presidential candidate of U.S. Presidential Campaign 1. U.S. Victim 12's personal email account was successfully compromised by the Conspirators.

32. Attempted U.S. Victim 13 was an official for U.S. Presidential Campaign 1.

33. U.S. Victim 14 was a former U.S. Department of State official, who was also an advisor to a presidential campaign that was suspended prior to May 2024. As a result of the compromise of U.S. Victim 11's account, the Conspirators gained access to communications between U.S. Victim 11 and U.S. Victim 14.

COUNT ONE

(Conspiracy to Obtain Information from a Protected Computer; Defraud and Obtain a Thing of Value; Commit Fraud Involving Authentication Features; Commit Aggravated Identity Theft; Commit Access Device Fraud; and Commit Wire Fraud While Falsely Registering Domains)

34. Paragraphs 1 through 33 are re-alleged here.

35. Beginning in or around January 2020 and continuing at least until in or around September 2024, within the District of Columbia and elsewhere, and begun and committed outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, the defendants, MASOUD JALILI, SEYYED ALI AGHAMIRI, YASAR BALAGHI, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, and agree with each other to commit the following offenses against the United States:

a. To intentionally access a computer without authorization, thereby obtaining information from a protected computer (i) in furtherance of a criminal and

tortious act in violation of the Constitution and the laws of the United States, that is, wire fraud and (ii) with the value of the information obtained exceeded $5,000, and knowingly falsely register and knowingly use domain names in the course of this offense; in violation of Title 18, United States Code, Sections 1030(a)(2); 1030(c)(2)(B)(ii); 1030(c)(2)(B)(iii) and 3559(g)(1);

b. To knowingly, and with intent to defraud, access a protected computer without authorization and by means of such conduct further the intended fraud and obtain something of value, specifically, payment for their services, access to other accounts, and a first class plane ticket, and knowingly falsely register and knowingly use domain names in the course of this offense; in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A) and 3559(g)(1);

c. To knowingly to transfer, possess and use, without lawful authority, a means of identification of another person with the intent to commit, and in connection with, wire fraud, in violation of Title 18, United States Code, Section 1343, and obtaining information by access to protected computers, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(a)(4), and knowingly falsely register and knowingly use domain names in the course of the offense, in violation of Title 18, United States Code, Sections 1028(a)(7) and 3559(g);

d. To use, with the intent to defraud, one or more unauthorized access devices and to obtain information and things of value in excess of $1,000, and knowingly falsely register and knowingly use domain names in the course of the offense, in violation of Title 18, United States Code, Sections 1029(a)(2) and 3559(g);

e. To devise, execute, and attempt to execute a scheme by means of false and fraudulent pretenses, representations, and promises, and to cause the transmission of wire communications in interstate and foreign commerce, various signals and sounds constituting wire transmissions, for the purpose of executing such scheme or artifice to defraud, and knowingly falsely register and knowingly use domain names in the course of the offense, in violation of Title 18, United States Code, Sections 1343 and 3559(g); and

f. During and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, and the crimes of obtaining information by access to protected computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and 1030(a)(4), and the crime of fraud involving the use of authentication features, in violation of Title 18, United States Code, Section 1028(a)(7), and the crime of access device fraud, in violation of Title 18, United States Code, Section 1029(a)(2), to knowingly transfer, possess, and use without lawful authority, a means of identification of another person, and knowingly falsely register and knowingly use domain names in the course of the offense, in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), 1028A(c)(5), and 3559(g);

in violation of Title 18, United States Code, Sections 371 and 3559(g).

Purposes of the Conspiracy

36. The purposes of the conspiracy were for the Conspirators to gain unauthorized access to victim computers and accounts using access devices and fraudulent means to accomplish the following objectives, among others, depending on the particular intrusion:

(i) create and maintain illegal, unauthorized access to victim computers and accounts; (ii) use victim accounts and persona accounts to target other victims for the purpose of gaining unauthorized access to those other victim computers and accounts; (iii) steal victims' data, such as information relating to U.S. government and foreign policy concerning the Middle East; (iv) steal information relating to current and former U.S. officials that could be used to advance the IRGC's malign activities, including ongoing efforts to avenge the death of Qasem Soleimani; (v) disrupt U.S. foreign policy in the Middle East; (vi) stoke discord and erode confidence in the U.S. electoral process; (vii) steal personal and private information from persons who had access to information relating to U.S. Presidential Campaign 1, including campaign material; and (viii) undermine U.S. Presidential Campaign 1 in advance of the 2024 U.S. presidential election by leaking stolen campaign material.

Manner and Means of the Conspiracy

37. As part of the conspiracy, the Conspirators supported one another, and aided and abetted computer hacking committed by one another, through the use of a variety of malicious techniques, including using static IP addresses provided by Respina Networks and FDI; using VPNs and virtual private servers ("VPSs") to obscure their true location; creating fraudulent email accounts in the names of prominent U.S. persons and international institutions; creating spoofed login pages; sending emails using compromised accounts; using social engineering to obtain victims' login information and multi-factor recovery/authentication codes; using malware to command-and-control compromised computers and accounts; and using cloud service providers to host malware and other hacking infrastructure. The Conspirators also maintained, in some cases, long-term, persistent access to compromised accounts. These techniques included knowingly falsely registering internet domains using fraudulent information for the purpose of compromising

victim computers and accounts, obtaining password credentials and tokens from their victims, and circumventing multi-factor authentication features. Specifically, Conspirators used stolen credentials and multi-factor authentication codes to gain access to and steal sensitive information related to, among other things, the information listed in paragraph 36(iii), (iv), (vii), and (viii).

38. As part of the conspiracy, the Conspirators used internet-connected computers and servers, including VPSs with remote access, which they leased directly and indirectly from web hosting providers. These computer servers were used to register and access operational email accounts, often impersonating real persons who were involved or associated with the U.S. government, including current and former U.S. officials and well-known non-governmental organizations. These computer servers also served as "hop points" between the computers owned or operated by the Conspirators and victim computers and were used to obfuscate the Conspirators' identities. The Conspirators' infrastructure included U.S. and foreign VPNs, VPSs, email accounts, and dedicated IP addresses, including the static IP addresses Respina Networks 106 IP and at FDI 117 IP, that they used regularly in furtherance of the conspiracy (hereafter, "IRGC infrastructure").

39. As part of the conspiracy, the Conspirators obtained and used servers, domains, encrypted messaging accounts, social media accounts, and dozens of email accounts from U.S. service providers to conduct online reconnaissance and research of victims and victim accounts for vulnerabilities, create online persona accounts to perpetrate the scheme, and to exploit such vulnerabilities to gain and maintain unauthorized access to the victim computers and accounts. The Conspirators used the persona accounts to gain victims' trust, socially engineer access to victim accounts, and, ultimately, gain access to victim computers and accounts. The Conspirators also used the persona accounts to communicate with one another and engage with internet service

providers and web hosting providers to purchase their services. In some cases, the Conspirators also sent malicious emails from compromised victim accounts to further their hacking efforts.

40. After establishing their unauthorized access to victim computers and accounts, as part of the conspiracy, the Conspirators made efforts to conceal their presence to maintain long-term, persistent access. During their persistent access, the Conspirators stole data and campaign material from the victim accounts and associated computers and, in some instances, later distributed stolen campaign materials to members of the media and individuals that the Conspirators believed were associated with U.S. Presidential Campaign 2, in an effort stoke discord and erode confidence in the U.S. electoral process, as well as undermine Presidential Campaign 1 in advance of the 2024 presidential election.

OVERT ACTS

41. In furtherance of the conspiracy, the following overt acts, among others, were committed by Conspirators, who at all relevant times resided and were located outside of the United States:

OVERT ACTS RELATED TO CURRENT U.S. OFFICIALS, FORMER U.S. OFFICIALS AND OTHER PERSONS TO ADVANCE IRGC MALIGN ACTIVITIES

42. On or about April 11, 2020, the Conspirators used a commercial VPN to create a persona account ("Persona Account 1") with a U.S.-based email provider in the name of a spouse of a sitting U.S. Supreme Court Justice.

43. On or about July 7, 2021, the Conspirators knowingly falsely registered the domain mailerdaemon.online with Provider 1 and used that domain for malicious purposes.

44. On or about November 9, 2021, the Conspirators knowingly falsely registered the domain mailer-daemon.live with Provider 1 and used that domain for malicious purposes.

45. On or about December 12, 2021, the Conspirators knowingly falsely registered the domain tinyurl.ink with Provider 1 and used that domain for malicious purposes.

46. Starting on or about December 14, 2021, the Conspirators used IRGC infrastructure to create a persona email account with a U.S.-based email provider in the name of an employee of a Washington, D.C.-based think tank ("Persona Account 2"). In registering Persona Account 1, the Conspirators set Persona Account 2 as the recovery account. (Recovery accounts are controlled by the same persons who control the primary account because recovery accounts are used to access a primary account. They can be used to reset passwords, to regain account access after forgetting a password, or for two-factor authentication access to an account.)

47. Starting on or about December 14, 2021, the Conspirators used Persona Account 2 to email U.S. Victim 1 and trick U.S. Victim 1 to click on a malicious link to a spoofed website controlled by the Conspirators. The Conspirators used that website to fraudulently obtain a means of authentication to U.S. Victim 1's email account so that they could obtain persistent access to that account without alerting the victim. Such persistent access enabled the Conspirators to obtain travel, lodging and other information regarding U.S. Victim 1, who was a senior U.S. Department of State official at the time of Qasem Soleimani's death and therefore of interest to the IRGC.

48. On or about April 30, 2022, the Conspirators used a commercial VPN to create a persona account ("Persona Account 3") with a U.S.-based email provider. Persona Account 3 was accessed from the same Conspirator computer and user profile as Persona Account 1.

49. On or about May 9, 2022, at approximately 6:15 UTC, JALILI logged into Persona Account 3 from a different commercial VPN.

50. On or about May 9, 2022, at approximately 7:10 UTC, BALAGHI arrived in or around the Malekloo Office.

51. On or about May 9, 2022, at approximately 8:01 UTC, AGHAMIRI arrived in or around the Malekloo Office.

52. On or about May 9, 2022, at approximately 9:49 UTC, the Conspirators logged into U.S. Victim 3's personal email account and sent the test email, "hi. for test" to Persona Account 3.

53. On or about May 9, 2022, at approximately 9:50 UTC, the Conspirators, while logged into U.S. to Persona Account 3, acknowledged receipt of the test email sent from U.S. Victim 3's compromised account by stating, "Hi, I got it. Tnx".

54. On or about May 31, 2022, the Conspirators knowingly falsely registered the domain mailer-daemon.me with Provider 1 and used that domain for malicious purposes.

55. On or about June 18, 2022, the Conspirators created and used another persona account ("Persona Account 4") with a U.S.-based email provider and used IRGC infrastructure to email U.S. Victim 1. The Conspirators fraudulently claimed to be the Chief Executive Officer of a fake non-profit organization called Democracy in the Middle East, and they sent an email that contained an embedded link that purported to be an invitation to U.S. Victim 1 for a conference in Dubai. The embedded link was malicious and directed the user to a website on domain mailer-daemon.me, which was used to harvest the credentials of the victim. Specifically, the website initiated a splash page that spoofed a U.S. service provider's login page, which called for the victim to enter their login credentials to gain access to the invitation. After the entry of any login credentials (whether accurate or not), the website posted a PDF invitation to the fake conference. Persona Account 4 was accessed from the same Conspirator computer and user profile as Persona Account 1.

56. On or about August 2, 2022, the Conspirators used IRGC infrastructure to create a U.S.-based domain mimicking the name of a think tank based in Washington, D.C. and three persona email accounts in the names of the think tank's employees (including "Persona Account 5" and "Persona Account 6").

57. Starting on or about August 2, 2022, the Conspirators used IRGC infrastructure to send test spearphishing emails from Persona Account 5 to Persona Account 3. According to the service provider, Persona Account 3 was the identified recovery email account for Persona Account 4. Persona Account 3 was also accessed from the same Conspirator computer and user profile as Persona Account 1.

58. On or about August 6, 2022, the Conspirators logged into U.S. Victim 1's email account from the Respina Networks 106 IP. Among the items that were in U.S. Victim 1's email was a copy of U.S. Victim 1's U.S. passport. The Conspirators used IRGC infrastructure to regularly access U.S. Victim 1's email accounts.

59. Between on or about August 4, 2022, and on or about August 9, 2022, the Conspirators used Persona Account 5, Persona Account 6, and a persona account in the name of a person working for U.A.E. Victim 2 ("Persona Account 7") to email U.S. Victim 4 and other targeted persons like those referenced in paragraph 16, above, who were in, or accessed the email from, the District of Columbia and elsewhere in the United States. The email contained what purported to be an invitation to a conference co-hosted by a Washington, D.C.-based think tank and the U.A.E. in November 2022. The invitation offered business class travel to, and accommodations in, the U.A.E., and invited guests to bring their spouses.

60. Between on or about August 4, 2022, and on or about August 9, 2022, once a recipient responded to the email referenced in paragraph 59, the Conspirators responded from

Persona Account 6 and Persona Account 7 with an embedded link to a registration page. The embedded link was a shortened link that would direct the victim to one of a number of malicious domains controlled by the Conspirators, including mailer-daemon.me.

61. Between on or about August 4, 2022, and on or about August 23, 2022, the Conspirators used Persona Account 7 to cause U.S. Victim 4 and others to visit the malicious domain mailer-daemon.me. Specifically, the victims were redirected to a splash page that spoofed a U.S. service provider's login page that called for the victim to enter their login credentials to gain access to a registration form. After the entry of any login credentials (whether accurate or not), the website would post a registration form, which called for the victim to provide personal identifying information and identification documentation, such as a copy of their passport. On or about August 23, 2022, U.S. Victim 4 responded to the fraudulent invitation and submitted personal identifying information and a copy of U.S. Victim 4's passport, including through the link provided by the Conspirators in their email referenced in paragraph 59.

62. On or about August 29, 2022, and continuing through on or about October 5, 2022, the Conspirators used IRGC infrastructure and another persona account with an encrypted messaging application that was connected to Persona Account 5, to make further contact with U.S. Victim 5, and then sent U.S. Victim 5 malicious links that allowed the Conspirators to harvest login credentials to U.S. Victim 5's personal email account. The Conspirators gained fraudulent access to U.S. Victim 5's email account with the stolen credentials.

63. Starting on or about October 4, 2022, the Conspirators used a U.S.-based email provider and used IRGC infrastructure to pose as an assistant to U.S. Victim 1 ("Persona Account 8") and send an email to an employee of U.A.E. Victim 2. The Conspirators falsely stated in the email that U.S. Victim 1 wanted to attend the conference hosted by U.A.E. Victim 2 and provided

a copy of U.S. Victim 1's passport, which had been previously stolen by the Conspirators. The Conspirators opened Persona Account 8 on or about October 20, 2021. The Conspirators defrauded U.A.E. Victim 2 into purchasing a business-class, roundtrip ticket for U.S. Victim 1 valued at approximately $11,825.00 on the date the ticket was purchased. U.S. Victim 1 did not travel to the U.A.E. on the ticket.

64. Continuing through on or about October 26, 2022, the Conspirators used Persona Account 8 to communicate with an employee of U.A.E. Victim 2 to confirm the (fraudulent) registration for U.S. Victim 1, and to try and obtain additional information about other actual attendees to the conference, which included current and former U.S. government officials. On or about October 24, 2022, the Conspirators used Persona Account 8 to send an employee of U.A.E. Victim 2 a stolen copy of U.S. Victim 1's passport to obtain visa and registration confirmation to the conference.

65. Between on or about November 23, 2022, and on or about November 25, 2022, the Conspirators used IRGC infrastructure to create a U.S.-based persona email account that fraudulently claimed to be an employee of the U.A.E. Embassy in Washington, D.C. ("Persona Account 9"). Persona Account 9 was accessed from the same Conspirator computer and user profile as Persona Account 1.

66. Between on or about November 23, 2022, and on or about November 25, 2022, the Conspirators used Persona Account 9 to email U.S. Victims 1, 6, 7, and 8, and other targeted persons like those referenced in paragraph 16, above, who were in, or accessed the email from, the District of Columbia and elsewhere in the United States. The emails contained a purported invitation to a national holiday event being hosted by the U.A.E. Embassy at a venue in Washington, D.C., and contained a shortened link to malicious domains controlled by the

Conspirators, including the domain mailer-daemon.online, which were used to harvest personal information and credentials of the victims. Specifically, the victims were redirected to a splash page that spoofed a U.S. service provider's login page, which called for the victim to enter their login credentials to gain access to the invitation. After the entry of any login credentials (whether accurate or not), the website would provide further information related to the fake event. The Conspirators successfully compromised accounts belonging to U.S. Victims 6, 7, and 8 from this and other related targeting activity.

67. Between at least December 20, 2022, and January 23, 2023, the Conspirators used IRGC infrastructure, including the FDI 117 IP, and a spearphishing attack, to compromise U.S. Victim 6's personal email account.

68. Starting in or around January 2023, the Conspirators used IRGC infrastructure to create and use a U.S.-based persona account for an encrypted messaging application in the true name of an employee for a think tank based in Washington, D.C. The Conspirators fraudulently used this account to claim to be the employee of a Washington, D.C.-based think tank ("Persona Account 10").

69. On or about January 16, 2023, the Conspirators used Persona Account 10 to send two emails to U.S. Victim 9 that contained embedded links to malicious domains controlled by the Conspirators. The Conspirators opened Persona Account 10 in or around January 2023 and regularly accessed it from IRGC infrastructure, including the FDI 117 IP on or about April 12, 2023, and on or about May 17, 2023.

70. On or about May 2, 2023, at approximately 10:36 UTC, the Conspirators logged into Persona Account 1 from IRGC infrastructure.

71. On or about July 20, 2023, at approximately 5:36 UTC, AGHAMIRI arrived in or around the Malekloo Office, and on the same day at approximately 9:02 UTC, he used IRGC infrastructure to log into one of his personal email accounts.

72. Between in or about April 2024, and in or around May 2024, the Conspirators used Persona Account 1 to send spearphishing emails to U.S. Victim 5, and other targeted persons referenced in paragraph 16, above.

OVERT ACTS RELATED TO THE U.S. PRESIDENTIAL ELECTION

73. On or about May 23, 2024, the Conspirators used FDI 117 IP address to attempt to log into, without authorization, a personal email account with a U.S.-based email provider that belonged to U.S. Victim 10 ("U.S. Victim 10's Personal Email Account 1"). The Conspirators' unsuccessful login attempt, on or about May 23, 2024, caused that same U.S.-based email provider to issue a password recovery code for U.S. Victim 10's Personal Email Account 1. On or about May 24, 2024, the Conspirators used IRGC infrastructure, including the FDI 117 IP, to successfully access, without authorization, U.S. Victim 10's Personal Email Account 1 using the same provider-generated recovery code.

74. On or about June 12, 2024, the Conspirators used IRGC infrastructure, including the FDI 117 IP, to access, without authorization, U.S. Victim 10's Personal Email Account 1.

75. On or about June 12, 2024, the Conspirators obtained a means of authentication to access, without authorization, a personal email account with a U.S.-based provider that belonged to U.S. Victim 11—an official for U.S. Presidential Campaign 1. The Conspirators used IRGC infrastructure, including the FDI 117 IP, to access, and maintain access to, U.S. Victim 11's account until on or about August 13, 2024. U.S. Victim 11's account contained campaign material.

76. Between on or about June 12, 2024, and on or about August 13, 2024, the Conspirators used their access to U.S. Victim 11's personal email account to steal campaign material, including debate preparation material, material regarding U.S. Presidential Campaign 1's potential vice-presidential candidates, and email communications with U.S. Victim 14.

77. On or about June 15, 2024, the Conspirators used U.S. Victim 10's Personal Email Account 1—which, as described in paragraphs 73 and 74, they had previously compromised and controlled—to send a spearphishing email to the official U.S. Presidential Campaign 1 email account of a U.S.-based email provider that belonged to Attempted U.S. Victim 13. The spearphishing email contained a link to a malicious domain created by the Conspirators. The attempt was unsuccessful.

78. On or about June 20, 2024, and on or about June 21, 2024, the Conspirators used IRGC infrastructure to access, without authorization, another U.S. Victim 10 personal email account, with a different U.S.-based email provider ("U.S. Victim 10's Personal Email Account 2").

79. On or about June 27, 2024, the Conspirators used IRGC infrastructure to create the email account ("Actor Account 1") with a U.S.-based email provider.

80. On or about June 27, 2024, at approximately 12:59 UTC, the Conspirators used Actor Account 1 to send an unsolicited email containing, in part, an excerpt taken from campaign material stolen from U.S. Victim 11. The email was sent to two personal email accounts that the Conspirators believed belonged to two different individuals associated with U.S. Presidential Campaign 2. The Conspirators' email stated as follows (errors in original; referenced stolen campaign material omitted):

> I'm the one who has access to [U.S. Presidential Campaign 1], but I hate [U.S. Presidential Campaign 1's candidate] and strongly don't

> want to see his second term. So I'm going to pass some materials along to you that would be useful to defeat him.
>
> For the first step, below is the final prep of [U.S. Presidential Campaign 1's candidate] for the first debate tonight. Read and be strong and ready for tonight.
>
> And you must know that the first debate is [U.S. Presidential Campaign 2's candidate]'s "last chance", and if he loses the debate, you [U.S. Presidential Campaign 2's political party] will have to replace [U.S. Presidential Campaign 2's candidate] with another candidates.

One recipient email account was invalid. The second recipient email account was a valid personal email account of a person associated with U.S. Presidential Campaign 2, but the user of that email account did not reply to Actor Account 1's email.

81. On or about June 27, 2024, at approximately 13:03 UTC, the Conspirators used Actor Account 1 to send an unsolicited email forwarding the email described in paragraph 80 to a valid personal email account of another person associated with U.S. Presidential Campaign 2, which was the same individual that the Conspirators had earlier attempted to email at an invalid email account. The user of the recipient email account did not reply to Actor Account 1's second email.

82. On or about July 3, 2024, at approximately 12:28 UTC, the Conspirators used Actor Account 1 to forward the June 27, 2024 email chain described in paragraphs 80 and 81 to two other valid personal email accounts that both belonged to a third individual that the Conspirators believed was associated with U.S. Presidential Campaign 2. In the unsolicited email, the Conspirators stated as follows:

> [Recipient's first name], I sent below email to [the two prior recipients first names] on the morning of the debate day, but it seems nobody cared and nobody contacted me for more materials. I have a lot in my pocket, and can be one of your best chances in this rally.

The user of these recipient email accounts did not reply to Actor Account 1's email.

83. Between on or about July 20, 2024, and on or about July 30, 2024, the Conspirators, obtained a means of authentication via a two-factor authentication social engineering scheme to access, without authorization, a personal email account with a U.S.-based email provider that belonged to U.S. Victim 12. The Conspirators used IRGC infrastructure, including the FDI 117 IP, to access the account, and maintained access to U.S. Victim 12's account until on or about August 13, 2024.

84. On or about June 27, 2024, the Conspirators created at least three email accounts with a U.S.-based email provider using IRGC infrastructure.

85. Between on or about July 22, 2024, and on or about August 12, 2024, the Conspirators used the email accounts described in paragraph 84 to distribute campaign material regarding U.S. Presidential Campaign 1's potential vice-presidential candidates, stolen from U.S. Victim 11, to multiple members of the media, in an attempt to induce the media to publish the material. In one instance, for example, the Conspirators' email stated "I think this information is worth a good [U.S. news publication] piece with your narration. Let me know your thoughts."

86. On or about July 22, 2024, the Conspirators used one of the email accounts described in paragraph 84 to send an email to a U.S.-based reporter ("Reporter 1"). In the text of the email, the Conspirators informed Reporter 1 that U.S. Victim 11 had communicated with U.S. Victim 14 about an article that Reporter 1 was allegedly intending to write. The Conspirators exchanged several emails with Reporter 1, and in at least two of those emails, the Conspirators directly quoted private emails sent by U.S. Victim 14 to U.S. Victim 11 about the proposed article.

87. Between on or about July 22, 2024, and on or about August 12, 2024, the Conspirators used tools available to Persona Account 1 to translate the content of emails (from

Farsi to English and English to Farsi) that related to their email exchanges with Reporter 1, as described in paragraph 86. The Conspirators used IRGC infrastructure, including the FDI 117 IP, to access Persona Account 1 through on or about August 2024.

88. Between on or about August 13, 2024, and on or about August 15, 2024, the Conspirators, while logged into Persona Account 1, reviewed news coverage of their activities identified in paragraphs 73 to 87.

89. Starting on or about August 31, 2024, the Conspirators created an additional email account with a U.S.-based email provider and used that email account to distribute campaign material belonging to U.S. Presidential Campaign 1, stolen from U.S. Victim 11, to multiple members of the media. The Conspirators claimed to be the same person who had previously leaked campaign material belonging to U.S. Presidential Campaign 1 between on or about July 22, 2024, and on or about August 12, 2024, as described in paragraph 85. Some of the campaign material distributed from the new email account contained the same vice-presidential candidate information that the Conspirators distributed to Reporter 1 and other members of the media between July 22, 2024, and August 12, 2024.

(**Conspiracy**, in violation of Title 18, United States Code, Sections 371, 1028(a)(7), 1028A, 1029(a)(2), 1030(a)(2)(C), (a)(4), and (c)(2)(B)(ii) and (iii), 1343, 1349, and 3559(g))

COUNT TWO
(Conspiracy to Provide Material Support to a Designated Foreign Terrorist Organization)

90. Paragraphs 1 through 15 are re-alleged here.

91. Beginning in or around January 2020, and continuing at least until in or around September 2024, within the District of Columbia and elsewhere, and begun and committed outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, the defendants, MASOUD JALILI, SEYYED ALI AGHAMIRI, YASAR BALAGHI, and others known and unknown to the Grand Jury, did knowingly conspire to provide material support and resources, as defined in Title 18, United States Code, Section 2339A(b), including personnel (to include themselves), expert advice and assistance to include computer hacking expertise, facilities, services, and tangible and intangible property, to a foreign terrorist organization: to wit, the IRGC, which at all relevant times had been designated by the Secretary of State as a foreign terrorist organization, knowing that the IRGC was a designated foreign terrorist organization and that the IRGC had engaged in, and was engaging in, terrorist activity and terrorism, and the offense occurred in part within the United States, and the offense occurred in and affected interstate and foreign commerce.

(**Conspiracy**, in violation of Title 18, United States Code, Section 2339B(a)(1))

COUNTS THREE THROUGH TEN
(Wire Fraud)

92. Paragraphs 1 through 89 are re-alleged here.

93. On or about the dates listed below, in the District of Columbia and elsewhere, and begun and committed outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, the defendants, MASOUD JALILI, SEYYED ALI AGHAMIRI, YASAR BALAGHI, and others known and unknown to the Grand Jury, for the purpose of

executing the scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and by concealment of material facts, and attempting to do so, did transmit, direct, and cause to be transmitted, by means of wire communications in interstate and foreign commerce between Iran, the United States, the District of Columbia and elsewhere, writings, signs, and signals—to wit, electronic connections between computers, servers, or other electronic infrastructure controlled by the Conspirators and computers, devices, or electronic accounts belonging to, or controlled by, the following persons identified in Count One, for the purpose of obtaining proprietary and valuable information from said victims, and did aid, abet, counsel, command, induce, or procure others to do so, and knowingly falsely registered and knowingly used domains in the course of the offenses:

COUNT	VICTIM	DATES
THREE	U.S. Victim 1	Between on or about December 21, 2021, and continuing through on or about October 26, 2022
FOUR	U.A.E. Victim 2	Between on or about October 4, 2022, and continuing through on or about November 1, 2022
FIVE	U.S. Victim 4	On or about August 23, 2022
SIX	U.S. Victim 5	Between on or about August 29, 2022, and continuing through October 5, 2022
SEVEN	U.S. Victim 6	Between on or about December 20, 2022, and continuing through on or about January 23, 2023
EIGHT	U.S. Victim 10	Between on or about May 24, 2024, and continuing through on or about June 20, 2024
NINE	U.S. Victim 11	Between on or about July 20, 2024, and continuing through on or about July 30, 2024

TEN	U.S. Victim 12	Between on or about June 12, 2024, and continuing through on or about August 11, 2024

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343, 3559(g), and 2)

COUNTS ELEVEN THROUGH EIGHTEEN
(Aggravated Identity Theft)

94. Paragraphs 1 through 89 are re-alleged here.

95. On or about the dates listed below, in the District of Columbia and elsewhere, and begun and committed outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, during and in relation to the crimes of Wire Fraud, in violation of Title 18, United States Code, Section 1343, the crime of Obtaining Information by Access to Protected Computers, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (a)(4), the crime of Fraud Involving the Use of Authentication Features, in violation of Title 18, United States Code, Section 1028(a)(7), and the crime of Access Device Fraud, in violation of Title 18, United States Code, Section 1029(a)(2), the defendants, MASOUD JALILI, SEYYED ALI AGHAMIRI, YASAR BALAGHI, and other conspirators known and unknown to the grand jury did knowingly transfer, possess, and use without lawful authority on or about the dates specified below, a means of identification of another person, login credentials, passport numbers and images, and personal identifying information, knowing that said means of identification belonged to the following actual persons, and did aid, abet, counsel, command, induce, or procure others to do so, said login credentials belonging to the following persons identified in Counts Eleven through Eighteen:

COUNT	PERSON	DATES
ELEVEN	U.S. Victim 1	Between on or about December 21, 2021, and continuing through on or about October 26, 2022
TWELVE	U.A.E. Victim 2	Between on or about October 4, 2022, and continuing through on or about November 1, 2022
THIRTEEN	U.S. Victim 4	On or about August 23, 2022
FOURTEEN	U.S. Victim 5	Between on or about August 29, 2022, and continuing through on or about October 5, 2022
FIFTEEN	U.S. Victim 6	Between on or about December 20, 2022, and continuing through on or about January 23, 2023
SIXTEEN	U.S. Victim 10	Between on or about May 24, 2024, and continuing through on or about June 20, 2024
SEVENTEEN	U.S. Victim 11	Between on or about July 20, 2024, and continuing through on or about July 30, 2024
EIGHTEEN	U.S. Victim 12	Between on or about June 12, 2024, and continuing through on or about August 11, 2024

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), and (5), and 2)

FORFEITURE ALLEGATION

96. Upon conviction of any offense alleged in Count One, the defendants shall forfeit to the United States any property, real or personal, constituting or derived from, any proceeds that the defendants obtained, directly or indirectly, as a result of any violation of or conspiracy to violate Title 18, United States Code, Sections 1030(a)(2)(C), (a)(4), and (c)(2)(B)(ii), (iii), and any personal property that was used or intended to be used to commit or to facilitate the commission of such violation, pursuant to Title 18, United States Code, Sections 1030(i)(1)(A)-(B) and 982(a)(2)(B); any property constituting, or derived from, proceeds the defendants obtained directly or indirectly, as the result of any violation of or conspiracy to violate Title 18, United States Code, Section 1028(a)(7), and any personal property used or intended to be used to commit the offense, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1028(b)(5); any property constituting, or derived from, proceeds the defendants obtained directly or indirectly, as the result of any violation of or conspiracy to violate Title 18, United States Code, Section 1029(a)(2), and any personal property used or intended to be used to commit the offense, pursuant to Title 18, United States Code, Section 982(a)(2)(B) and Title 18, United States Code, Section 1029(c)(1)(C); and any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of or a conspiracy to violate Title 18, United States Code, Section 1343, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

97. Upon conviction of the offense alleged in Count Two of this Indictment, the defendants shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of Title 18, United States Code, Section 2339B,

pursuant to Title 18, United States Code, Section 981(a)(1)(G) and Title 28, United States Code, Section 2461(c), and any personal property that was used or intended to be used to commit or to facilitate the commission of such violation, pursuant to Title 18, United States Code, Section 981(a)(1)(G) and Title 28, United States Code, Section 2461(c).

98. Upon conviction of any offenses alleged in Counts Three through Ten of this Indictment, the defendants shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of Title 18, United States Code, Section 1343, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

MONEY JUDGMENT

99. In the event of conviction, the United States may seek a money judgment.

SUBSTITUTE ASSETS

100. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(**Criminal Forfeiture**, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 981(a)(1)(G), 982(a)(2)(B), 1028(b)(5), 1029(c)(1)(C), 1030(i)(1)(A)-(B), Title 28, United Sates Code, Section 2461(c), and Title 21, United States Code, Section 853(p))

A TRUE BILL

_____
Foreperson

MATTHEW M. GRAVES
ATTORNEY FOR THE UNITED STATES
IN AND FOR THE DISTRICT OF COLUMBIA