UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA -v.- GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," Defendants.	**SEALED INDICTMENT** S2 18 Cr. 94 (JMF)

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

The Grand Jury charges:

OVERVIEW

1. At all times relevant to this Indictment, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a

"Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants (the "Mabna Defendants"), all of whom were nationals of the Islamic Republic of Iran ("Iran") living and working within Iran, were leaders, contractors, associates, hackers for hire, and affiliates of the Mabna Institute, an Iran-based company that conducted massive, coordinated cyber intrusions into computer systems belonging to at least approximately 144 United States-based universities, including two universities based in the Southern District of New York ("University-1" and "University-2"). In addition, the Mabna Defendants conducted coordinated cyber intrusions into computer systems belonging to at least 178 universities located in 22 foreign countries, including Australia, Canada, China, Denmark, Finland, Germany, Ireland, Israel, Italy, Japan, Malaysia, Netherlands, Norway, Poland, Saudi Arabia, Singapore, South Korea, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. The Mabna Defendants conducted this activity at the behest of the government of Iran, specifically the Islamic Revolutionary Guard Corps ("IRGC"), which is one of several

entities within the Government of Iran responsible for gathering intelligence.

2. Since at least approximately 2013, the Mabna Defendants compromised thousands of accounts belonging to professors at victim universities and targeted academic data and intellectual property for theft, which, during the course of the conspiracy, cost the affected United States-based universities at least approximately $3.4 billion dollars to procure and access. The stolen data, as well as access to compromised university accounts, was used to benefit the IRGC and other Iranian customers, including Iran-based universities.

3. At the same time that the members of the conspiracy were targeting, compromising, and stealing data from universities around the world, they also compromised the computer systems of at least five U.S. federal and state government agencies, at least 42 private sector companies, and at least two non-governmental organizations ("NGOs").

4. Home Box Office, Inc. ("HBO"), a media and entertainment company headquartered in New York, New York, was one of the victims of the Mabna Institute's hacking campaign which targeted private sector companies. BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, was separately charged in United States v. Behzad Mesri, 17 Cr. 689 (AJN), with hacking into

HBO's computer systems, stealing proprietary data, and then attempting to extort HBO for approximately $6 million worth of Bitcoin, a form of digital currency. SAEID HOUSHAR, MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, were also directly involved in the hack of HBO's systems along with MESRI. The defendants stored proprietary data stolen from HBO on computer network infrastructure, which was controlled by members of the conspiracy and used to store proprietary data that had been stolen from university and private sector victims of the Mabna Institute.

MEANS AND METHODS OF THE CONSPIRACY

University Hacking Campaign

5. In conducting their hacking attacks of university victims, members of the conspiracy organized their activities into various phases, generally summarized as follows:

a. First, members of the conspiracy conducted online reconnaissance of university professors, including to determine these professors' research interests and the academic articles they had published.

b. Second, customized spearphishing emails were created. Spearphishing emails are emails sent to a target

seeking to induce action that would allow the sender to obtain unauthorized access to the recipient victim's computer system. This can be accomplished in a number of ways, including, but not limited to, tricking the target into unwittingly providing his or her account login credentials to allow the attacker to remotely log into, and obtain unauthorized access to, the victim's online accounts. The spearphishing emails created by the conspiracy purported to be sent from professors at one university, and were directed to victim professors at another university. In general, those spearphishing emails indicated that the sender had read an article the victim professor had recently published, and expressed an interest in several other articles. The sender provided links to those additional articles. If the victim professor clicked on certain links, he or she would be directed to a malicious Internet domain named to appear confusingly similar to the authentic domain of the recipient professor's university. The malicious domain contained a webpage designed to appear to be the login webpage for the victim professor's university. It was the conspirators' intent that the victim professor would be led to believe that he or she had inadvertently been logged out of his or her university's computer system prompting the victim professor for his or her login credentials, i.e., the username and password

for his or her university account. If a professor then entered his or her login credentials, those credentials were then logged and captured by the hackers.

c. Third, the members of the conspiracy used stolen account credentials and obtained unauthorized access to victim professor accounts, through which they then exfiltrated, or transferred to themselves, academic data and documents from the systems of compromised universities, including, among other things, academic journals, theses, dissertations and electronic books. The defendants targeted data across all fields of research and academic disciplines, including science and technology, engineering, social sciences, medical and other professional fields. At least approximately 31.5 terabytes of academic data and intellectual property from compromised universities was stolen and exfiltrated to servers under the control of members of the conspiracy located in countries outside the United States.

6. Over the course of this hacking conspiracy, the defendants and their co-conspirators targeted over 100,000 professor accounts worldwide with spearphishing messages, approximately half of which targeted professors at United States-based universities. As a result of those spearphishing attacks, the conspiracy successfully compromised at least

approximately 8,000 accounts worldwide, of which at least approximately 3,768 belonged to professors at United States-based victim universities.

7. The exfiltrated data and the stolen login credentials of university professors were obtained for the benefit of the IRGC, and were also sold within Iran, including through two websites, Megapaper.ir ("Megapaper") and Gigapaper.ir ("Gigapaper"). Megapaper was operated by Falinoos Company ("Falinoos"), a company controlled by ABDOLLAH KARIMA, a/k/a "Vahid Karima," the defendant, and Gigapaper was affiliated with KARIMA. Megapaper sold stolen academic resources to customers within Iran, including Iran-based public universities and institutions, and Gigapaper sold a service to customers within Iran whereby purchasing customers could use compromised university professor accounts to directly access the online library systems of particular United States-based and foreign universities.

Private Sector Hacking Victims

8. In addition to targeting and compromising universities, members of the conspiracy targeted and compromised employee email accounts for at least approximately 42 United States-based private companies, and at least approximately eleven private companies based in Germany, Italy, Switzerland,

Sweden, and the United Kingdom, and exfiltrated entire email mailboxes from compromised employees' accounts. Among the United States-based private sector victims were the following:

a. Three academic publishers;

b. Four media and entertainment companies, including HBO;

c. One law firm;

d. Eleven technology companies;

e. Five consulting firms;

f. Four marketing firms;

g. Two banking and/or investment firms;

h. Two online car sales companies;

i. One healthcare company;

j. One employee benefits company;

k. One industrial machinery company;

l. One biotechnology company;

m. One food and beverage company;

n. One stock images company;

o. Two defense contractors;

p. One energy company; and

q. One non-profit lobbying firm.

9. In order to compromise accounts of private sector victims, members of the conspiracy used a technique known as

"password spraying," whereby they first collected lists of names and email accounts associated with the intended victim company through open source Internet searches. Then, they attempted to gain access to those accounts with commonly-used passwords, such as frequently used default passwords, in order to attempt to obtain unauthorized access to as many accounts as possible. Once they obtained access to the victim accounts, members of the conspiracy, among other things, exfiltrated entire email mailboxes from the victims. In addition, in many cases, the defendants established automated forwarding rules for compromised accounts that would prospectively forward new outgoing and incoming email messages from the compromised accounts to email accounts controlled by the conspiracy.

U.S. Government and NGO Hacking Victims

10. In the same time period as the university and private sector hacking campaigns described above, the Mabna Institute also conducted a computer hacking campaign against various governmental and non-governmental organizations within the United States. During the course of that campaign, employee login credentials were stolen by members of the conspiracy through password spraying. Among the victims were the following, all based in the United States:

a. United States Department of Labor;

b. Federal Energy Regulatory Commission;

c. State of Hawaii;

d. State of Indiana;

e. State of Indiana Department of Education;

f. United Nations; and

g. United Nations Children's Fund.

RELEVANT PERSONS AND ENTITIES

11. At all times relevant to this Indictment, the Mabna Institute was an organization founded in or about 2013, and was set up in order to assist Iranian universities, as well as scientific and research organizations, to obtain access to non-Iranian scientific resources. The Mabna Institute contracted with Iranian governmental and private entities to conduct hacking activities on their behalf. The Mabna Institute conducted the university spearphishing campaign specifically on behalf of the IRGC. The Mabna Institute logo appears below.

12. At all times relevant to this Indictment, GHOLAMREZA RAFATNEJAD, the defendant, was a founding member of the Mabna Institute. Among other things, RAFATNEJAD organized the Mabna Institute hacking campaign which targeted universities, sent and received compromised credentials belonging to victim professors to and from co-conspirators, organized stolen professor credentials, and controlled malicious domains that were used to target university victims. RAFATNEJAD had the contact with the IRGC that funded certain aspects of the Mabna Institute hacking campaign that targeted universities.

13. At all times relevant to this Indictment, EHSAN MOHAMMADI, the defendant, was a founding member of the Mabna Institute, and served as the Mabna Institute's Managing Director. Along with GHOLAMREZA RAFATNEJAD, the defendant, MOHAMMADI also helped organize the Mabna Institute campaign which targeted universities, and received compromised credentials to victim professors' accounts from co-conspirators. MOHAMMADI was also responsible for managing the finances of the Mabna Institute, including with respect to the Mabna Institute's computer hacking and exploitation operations.

14. At certain times relevant to this Indictment, ABDOLLAH KARIMA, a/k/a "Vahid Karima," the defendant, was an Iran-based businessman who owned and operated Falinoos, a

company operating in Iran that sold access to academic materials. Through Falinoos, KARIMA entered into contracts with multiple Iranian public universities to sell them access to academic materials that had been stolen from U.S. and foreign universities through computer intrusions. KARIMA contracted with the Mabna Institute to direct certain of the hacking activities described in this Indictment, and sold academic materials that had been stolen through the computer intrusions targeting United States-based and foreign universities through various websites operated by Falinoos, including Megapaper, and exchanged stolen professor credentials with the operators of the Gigapaper website. KARIMA was regularly provided with compromised login credentials for professors at various victim universities from other members of the conspiracy.

15. At all times relevant to this Indictment, MOSTAFA SADEGHI, the defendant, was a prolific Iran-based computer hacker who was an affiliate of the Mabna Institute. SADEGHI personally compromised over approximately 1,000 victim professor accounts through the course of the spearphishing campaign. SADEGHI exchanged credentials for compromised professor accounts with GHOLAMREZA RAFATNEJAD and ABDOLLAH KARIMA, a/k/a "Vahid Karima," the defendants, and provided training to RAFATNEJAD on computer hacking techniques, specifically focused on

compromising university-based accounts. SADEGHI was also involved in the operation of, and maintained a financial interest in, the Megapaper website.

16. At certain times relevant to this Indictment, SEYED ALI MIRKARIMI, the defendant, was an Iran-based hacker and contractor for the Mabna Institute. MIRKARIMI participated in a wide range of Mabna Institute hacking projects, including the spearphishing campaign that targeted universities and hacking efforts that targeted private sector companies, government organizations, and NGOs. MIRKARIMI was involved in many aspects and phases of the hacking activity, including, but not limited to, crafting and testing spearphishing emails, registering malicious domains that were used to target victim universities, compiling targeting lists, and organizing stolen credentials.

17. At certain times relevant to this Indictment, MOHAMMED REZA SABAHI, the defendant, was an Iran-based contractor for the Mabna Institute. MOHAMMAD REZA SABAHI helped carry out the spearphishing campaign, which targeted universities by, among other things, conducting online reconnaissance of victim university systems, creating targeting lists of victim professors, and cataloging academic databases at victim universities that were targeted by the hacking campaign.

18. At certain times relevant to this Indictment, ROOZBEH SABAHI, the defendant, was an Iran-based contractor for the Mabna Institute. ROOZBEH SABAHI helped carry out the various hacking activities of the Mabna Institute by, among other things, organizing stolen credentials obtained by Mabna Institute hackers, including credentials for accounts belonging to victim professors, and accounts belonging to employees of private sector, government, and NGO victims of the Mabna Institute.

19. At certain times relevant to this Indictment, ABUZAR GOHARI MOQADAM, the defendant, was an Iran-based professor and affiliate of the Mabna Institute who exchanged credentials for compromised accounts with Mabna Institute founders GHOLAMREZA RAFATNEJAD and EHSAN MOHAMMADI, the defendants.

20. At certain times relevant to this Indictment, SAJJAD TAHMASEBI, the defendant, was an Iran-based contractor for the Mabna Institute. TAHMASEBI helped facilitate the spearphishing campaign which targeted universities by, among other things, conducting online network surveillance of victim university computer systems, and maintaining lists of credentials stolen from victim professors.

21. At certain times relevant to this Indictment, SAEID HOUSHYAR, the defendant, was an Iran-based hacker and contractor for the Mabna Institute. HOUSHYAR was also a member of Iran's internal cyber police known as FATA. HOUSHYAR helped facilitate the spearphishing campaign which targeted universities by, among other things, registering and managing malicious domains that were used to target victim universities. HOUSHYAR provided hacking tools to the Mabna Institute, and also registered and managed computer network infrastructure used by the Mabna Institute to hack and obtain unauthorized access to private sector companies.

22. At certain times relevant to this Indictment, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, was an Iran-based hacker and contractor for the Mabna Institute. MESRI was a self-professed expert in computer hacking techniques, and worked on behalf of the Iranian military to conduct computer network attacks that targeted military systems, nuclear software systems, and Israeli infrastructure. At certain times relevant to this Indictment, MESRI was a member of an Iran-based hacking group called the Turk Black Hat Security team. MESRI participated in a wide range of Mabna Institute hacking projects, including the spearphishing campaign that targeted universities and hacking efforts that targeted private sector

companies, government organizations, and NGOs. MESRI was involved in many aspects and phases of the Mabna Institute hacking activity, including, but not limited to, obtaining unauthorized access to computer servers belonging to victims, managing computer network infrastructure used to facilitate hacks and store stolen information, and exchanging login credentials for compromised accounts with other co-conspirators.

23. At certain times relevant to this Indictment, MANOUCHEHR HASHEMLOO, the defendant, was an Iran-based hacker and contractor for the Mabna Institute. HASHEMLOO was also a member of FATA, and conducted extensive cybersecurity work for the Iranian Government, including, but not limited to, work on behalf of the IRGC, FATA, and a website project for the Supreme Leader of Iran. HASHEMLOO participated in a wide range of Mabna Institute hacking projects, including the spearphishing campaign that targeted universities and hacking efforts that targeted private sector companies. HASHEMLOO was involved in procuring and managing computer network infrastructure used in furtherance of the Mabna Institute hacking activity, including servers used to send spearphishing messages to victim professors, servers used to obtain unauthorized access to private sector victims, and malicious domains used to target victim universities.

24. At certain times relevant to this Indictment, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," the defendant, was an Iran-based hacker and contractor for the Mabna Institute. FAYAZ participated in the Mabna Institute's efforts to hack into private sector companies through password spray attacks. FAYAZ specifically managed computer servers that were used to conduct password spray attacks, obtained unauthorized access to compromised employee accounts at victim companies, and accessed servers containing data stolen from private sector victims of the Mabna Institute.

25. At certain times relevant to this Indictment, AMIR BARATI, the defendant, was an Iran-based hacker and contractor for the Mabna Institute. BARATI participated in a wide range of Mabna Institute hacking projects, including the spearphishing campaign that targeted universities and hacking efforts that targeted private sector companies. With respect to the Mabna Instiute hacking campaign that targeted universities, BARATI was involved in tracking the progress of the campaign, and exchanged login credentials for compromised professor accounts with other co-conspirators. With respect to private sector victims of the Mabna Institute, BARATI was involved in creating targeting lists, conducting computer network

reconnaissance, crafting spearphishing messages, and receiving credentials for compromised employee accounts.

26. At certain times relevant to this Indictment, SABER SHAHBAZI BALLOJEH, the defendant, was an Iran-based hacker and contractor for the Mabna Institute. BALLOJEH participated in the Mabna Institute's efforts to hack into private sector companies, including by conducting password spray attacks, obtaining unauthorized access to victim system, and exfiltrating emails from compromised email accounts.

27. At certain times relevant to this Indictment, ARMAN KAHZADIAN, the defendant, was an Iran-based hacker and contractor for the Mabna Institute. KAHZADIAN participated in a wide range of Mabna Institute hacking projects, including the spearphishing campaign that targeted universities and hacking efforts that targeted private sector companies. KAHZADIAN participated in the Mabna Institute hacking campaign that targeted universities by conducting computer network reconnaissance of victim university systems, and exchanging login credentials for compromised accounts with other co-conspirators. With respect to private sector victims of the Mabna Institute, KAHZADIAN conducted online computer network reconnaissance of victim systems and obtained unauthorized access to, and exfiltrated emails from, compromised accounts.

28. At certain times relevant to this Indictment, MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendant, was an Iran-based hacker who conspired with certain of the Mabna Defendants to conduct computer intrusions against private sector companies and governmental entities, using the same password spray techniques that were developed and deployed as part of the Mabna Institute's hacking activities. Among other things, GALEKUHI procured, controlled, and directed infrastructure that was used in such password spray attacks.

STATUTORY ALLEGATIONS

29. From at least in or about 2013 through at least in or about December 2017, in the Southern District of New York and elsewhere, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit offenses against the United States, to wit, computer intrusion, in violation of Title 18, United States Code,

Sections 1030(a)(2), 1030(c)(2)(B)(i), 1030(c)(2)(B)(iii), 1030(a)(5)(A), 1030(a)(6), 1030(c)(2)(A), 1030(c)(4)(A)(i)(I), and 1030(c)(4)(B)(i).

30. It was a part and an object of the conspiracy that GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, and others known and unknown, would and did intentionally access computers without authorization, and exceed authorized access, and thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and the value of the information obtained would and did exceed $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2), 1030(c)(2)(B)(i), and 1030(c)(2)(B)(iii).

31. It was further a part and an object of the conspiracy that GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI

MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage, without authorization, to a protected computer, which would and did cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least $5,000 to one and more persons during any one year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), 1030(c)(4)(B)(i), and 2.

32. It was further a part and an object of the conspiracy that GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, and others known and unknown, knowingly and with the intent to

defraud, would and did traffic in passwords and similar information through which computers may be accessed without authorization, in transactions affecting interstate and foreign commerce, and involving computers used by and for the Government of the United States, in violation of Title 18, United States Code, Sections 1030(a)(6) and 1030(c)(2)(A).

Overt Acts

33. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about October 2013, MOSTAFA SADEGHI, the defendant, transmitted credentials for compromised email accounts at multiple universities to ABDOLLAH KARIMA, a/k/a "Vahid Karima," the defendant.

b. In or about May 2014, SEYED ALI MIRKARIMI, the defendant, transmitted information to GHOLAMREZA REFATNEJAD, the defendant, regarding malicious domains registered and used by the conspiracy used to spearphish professors at victim universities.

c. In or about May 2014, MOSTAFA SADEGHI, the defendant, transmitted credentials for compromised email accounts at multiple universities to RAFATNEJAD.

d. In or about January 2015, MANOUCHEHR HASHEMLOO, the defendant, leased computer network infrastructure while knowing that it would be used by members of the conspiracy to send spearphishing messages to victim professors.

e. In or about March 2015, RAFATNEJAD, transmitted credentials for compromised email accounts at multiple universities, including for University-1, to multiple co-conspirators, including EHSAN MOHAMMADI, the defendant.

f. In or about June 2015, MIRKARIMI, transmitted credentials for compromised email accounts at multiple universities, including for University-1, to RAFATNEJAD.

g. In or about August 2014, MOHAMMAD REZA SABAHI, the defendant, sent targeting information designed to be used in spearphishing emails targeting professors at a victim university to RAFATNEJAD.

h. In or about August 2014, ROOZBEH SABAHI, the defendant, sent targeting information designed to be used in spearphishing emails targeting professors at multiple universities to MOHAMMAD REZA SABAHI.

i. In or about June 2015, ARMAN KAHZADIAN, the defendant, transmitted credentials for compromised email accounts at multiple universities to AMIR BARATI, the defendant.

j. In or about July 2015, KAHZADIAN transmitted credentials for compromised email accounts belonging to a private sector victim to BARATI.

k. In or about September 2015, ABUZAR GOHARI MOQADAM, the defendant, transmitted credentials for compromised email accounts at multiple universities, including for University-1, to MOHAMMADI.

l. In or about November 2015, ABDOLLAH KARIMA, a/k/a "Vahid Karima," the defendant, possessed credentials for a compromised email account belonging to a professor at University-1.

m. In or about November 2015, SAJJAD TAHMASEBI, the defendant, possessed credentials for compromised emails accounts at multiple universities.

n. In or about April 2016, MOHAMMAD REZA SABAHI conducted online reconnaissance of webmail portals for at least approximately 13 U.S.-based universities.

o. In or about September 2016, MIRKARIMI transmitted credentials for compromised email accounts from a university to BEHZAD MESRI, a/k/a "Skote Vahshat, the defendant.

p. In or about February 2017, TAHMASEBI conducted online reconnaissance of webmail portals for at least

approximately 13 U.S.-based universities, including University-1.

q. In or about April 2017, SAEID HOUSHYAR, the defendant, leased a server while knowing it would be used by members of the conspiracy to conduct password spray attacks against at least two U.S.-based private sector companies.

r. In or about June 2017, MESRI obtained unauthorized access to a compromised HBO employee account on multiple occasions.

s. In or about July 2017, SABER SHAHBAZI BALLOJEH, the defendant, possessed emails stolen from an employee account of a private sector victim.

t. In or about October 2017, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," leased computer network infrastructure while knowing it would be used by members of the conspiracy to conduct password spray attacks and obtain unauthorized access to servers belonging to a private sector victim.

u. In or about November 2017, BALLOJEH obtained unauthorized access to servers belonging to a private sector victim.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

34. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

35. From at least in or about 2013 through at least in or about December 2017, in the Southern District of New York and elsewhere, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

36. It was a part and object of the conspiracy that GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat,"

MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, FAYAZ, BARATI, BALLOJEH, and KAHZADIAN, obtained and used stolen login credentials of authorized users of victim computer networks to obtain unauthorized access to those networks and to steal data, which scheme involved the use of interstate wires, including remote spearphishing e-mails and interstate logins to victim servers.

(Title 18, United States Code, Section 1349.)

COUNT THREE
(Computer Fraud - Unauthorized Access for Private Financial Gain)

The Grand Jury further charges:

37. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

38. From at least in or about May 2014 through at least in or about April 2017, in the Southern District of New York and elsewhere, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, AMIR BARATI, and ARMAN KAHZADIAN, the defendants, willfully and intentionally accessed a computer without authorization and exceeded authorized access, and thereby would and did obtain information from a protected computer, for purposes of commercial advantage and private financial gain, the value of which exceeded $5,000, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, BARATI and KAHZADIAN conducted, and aided and abetted in conducting, computer intrusions to gain unauthorized access to the computer systems of University-1, and

obtained and sold academic resources stolen from University-1 as well as access to compromised University-1 professor accounts.

(Title 18, United States Code, Sections 1030(a)(2), (c)(2)(B)(i), (c)(2)(B)(iii) and 2.)

COUNT FOUR
(Wire Fraud)

The Grand Jury further charges:

39. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

40. From at least in or about May 2014 through in or about April 2017, in the Southern District of New York and elsewhere, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, AMIR BARATI, and ARMAN KAHZADIAN, the defendants, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose

of executing such scheme and artifice, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, BARATI and KAHZADIAN obtained University-1 professor login credentials through misrepresentations, including, by among other means, sending spearphishing messages to University-1 professors located in the Southern District New York, and directing University-1 professors to fake login pages, and then using and aiding and abetting others in using those login credentials to access University-1's computer systems without authorization, which scheme involved the use of interstate wires, including emails transmitted into and out of the Southern District of New York.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT FIVE

(Computer Fraud – Unauthorized Access for Private Financial Gain)

The Grand Jury further charges:

41. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

42. From at least in or about June 2014 through at least in or about November 2016, in the Southern District of New

York and elsewhere, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, AMIR BARATI, and ARMAN KAHZADIAN, the defendants, willfully and intentionally accessed a computer without authorization and exceeded authorized access, and thereby would and did obtain information from a protected computer, for purposes of commercial advantage and private financial gain, the value of which exceeded $5,000, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, BARATI and KAHZADIAN conducted, and aided and abetted in conducting, computer hacking attacks to gain unauthorized access to the computer systems of University-2, and obtained and sold academic resources stolen from University-2 as well as access to compromised University-2 professor accounts.

(Title 18, United States Code, Sections 1030(a)(2), (c)(2)(B)(i), (c)(2)(B)(iii) and 2.)

COUNT SIX
(Wire Fraud)

The Grand Jury further charges:

43. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

44. From at least in or about June 2014 through at least in or about November 2016, in the Southern District of New York and elsewhere, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, AMIR BARATI, and ARMAN KAHZADIAN, the defendants, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, BARATI and KAHZADIAN obtained University-2 professor login

credentials through misrepresentations, including, by among other means, sending spearphishing messages to University-2 professors located in the Southern District New York, and directing University-2 professors to fake login pages, and then using and aiding and abetting others in using those login credentials to access University-2's computer systems without authorization, which scheme involved the use of interstate wires, including emails transmitted into and out of the Southern District of New York.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT SEVEN

(Aggravated Identity Theft)

The Grand Jury further charges:

45. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

46. From at least in or about 2013 through at least in or about December 2017, in the Southern District of New York and elsewhere, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), and aided and abetted the same, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, FAYAZ, BARATI, BALLOJEH, and KAHZADIAN transferred, possessed, and used, and aided and

abetted the transfer, possession, and use of, the login credentials including usernames and passwords of various professors at United States universities and various employees at private sector companies and government institutions during and in relation to the wire fraud and computer fraud offenses charged in Counts One through Six of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b) and 2.)

COUNT EIGHT

(Computer Fraud - Unauthorized Access for Private Financial Gain)

The Grand Jury further charges:

47. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

HBO Intrusion

48. As discussed above, HBO was one of the numerous victims of Mabna Institute's hacking campaign which targeted private sector victims through password spray attacks.

49. Starting in at least in or about May 2017, hackers associated with the Mabna Institute, including SAEID HOUSHYAR, MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "bc.monster," SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, along with BEHZAD MESRI,

a/k/a "Skote Vahshat," began efforts to compromise computer systems belonging to HBO. First, the defendants conducted online reconnaissance of HBO's computer networks and employees. Among other things, MESRI and FAYAZ searched for access points to the network where employees and other authorized users could remotely access HBO's computer systems.

50. Between at least in or about May 2017 and in or about July 2017, the defendants successfully compromised multiple user accounts belonging to HBO employees and other authorized users, using password spray attacks, consistent with the tactics and procedures of the Mabna Institute. Over the course of several months, the defendants used that unauthorized access to steal confidential and proprietary information belonging to HBO which they then exfiltrated to computer servers, which were controlled by members of the conspiracy and also used to store proprietary data that had been stolen from universities and private sector victims of the Mabna Institute.

51. Through the course of the intrusions into HBO's systems, the defendants were responsible for stealing confidential and proprietary data belonging to HBO, including, but not limited to: (a) confidential video files containing unaired episodes of original HBO television programs, including episodes of Ballers, Barry, Room 104, Curb Your Enthusiasm, and

The Deuce; (b) scripts and plot summaries for unaired programming, including but not limited to episodes of Game of Thrones; (c) confidential cast and crew contact lists; (d) emails belonging to at least one HBO employee; (e) financial documents; and (f) online credentials for HBO social media accounts (collectively, the "Stolen Data").

STATUTORY ALLEGATIONS

52. From at least in or about May 2017 through at least in or about August 2017, in the Southern District of New York and elsewhere, SAEID HOUSHYAR, MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, who will first enter the United States in the Southern District of New York, willfully and intentionally accessed a computer without authorization and exceeded authorized access, and thereby obtained information from a protected computer, for purposes of commercial advantage and private financial gain, the value of which exceeded $5,000, and did aid and abet the same, to wit, HOUSHYAR, HASHEMLOO, FAYAZ, BALLOJEH and KAHZADIAN conducted, accessed without authorization HBO's computer networks, and stole proprietary data belonging to HBO and transferred the data to computer servers under their control.

(Title 18, United States Code, Sections 1030(a)(2), (c)(2)(B)(i), (c)(2)(B)(iii) and 2; Title 18, United States Code, Section 3238.)

COUNT NINE

(Wire Fraud)

The Grand Jury further charges:

53. The allegations contained in paragraphs 1 through 28 and 47 through 51 of this Indictment are repeated and realleged as if fully set forth herein.

54. From at least in or about May 2017 through at least in or about August 2017, in the Southern District of New York and elsewhere, SAEID HOUSHYAR, MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, who will first enter the United States in the Southern District of New York, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, and aided and abetted the same, to wit, HOUSHYAR, HASHEMLOO, FAYAZ, BALLOJEH and KAHZADIAN

obtained and used stolen login credentials of authorized users of HBO's computer network to obtain unauthorized access to that network and to steal proprietary data belonging to HBO, which scheme involved the use of interstate wires, including remote interstate logins to HBO servers.

(Title 18, United States Code, Sections 1343 and 2; Title 18, United States Code, Section 3238.)

COUNT TEN
(Aggravated Identity Theft)

The Grand Jury further charges:

55. The allegations contained in paragraphs 1 through 28 and 47 through 51 of this Indictment are repeated and realleged as if fully set forth herein.

56. From at least in or about May 2017 through at least in or about August 2017, in the Southern District of New York and elsewhere, SAEID HOUSHYAR, MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and ARMAN KAHZADIAN, the defendants, who will first enter the United States in the Southern District of New York, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), and aided and abetted the same, to wit, HOUSHYAR, HASHEMLOO, FAYAZ, BALLOJEH

and KAHZADIAN transferred, possessed, and used, and aided and abetted the transfer, possession, and use of, the usernames and passwords of various employees at HBO during and in relation to the wire fraud and computer fraud offenses charged in Counts Eight and Nine of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b) and 2; Title 18, United States Code, Section 3238.)

COUNT ELEVEN
(Conspiracy to Commit Computer Intrusions)

The Grand Jury further charges:

57. The allegations contained in paragraphs 1 through 28 and 47 through 51 of this Indictment are repeated and realleged as if fully set forth herein.

Fayaz, Ballojeh, and Galekuhi Computer Intrusion Conspiracy

58. Since at least approximately October 2018, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, have continued to conduct computer intrusions against numerous private sector companies and at least two governmental entities, using the same password spray techniques to compromise systems that were developed and deployed as part of the Mabna Institute's hacking activities against private sector companies, government agencies, and NGOs. In some cases, terabytes worth of victim proprietary data were

exfiltrated to online accounts under the control of one or more of the defendants. The victims of the intrusions conducted by FAYAZ, BALLOJEH, and GALEKUHI have suffered an excess of $20 million in costs to investigate and remediate the intrusions, and include, among others:

a. One COVID-19 vaccine developer;

b. One U.S.-based information technology company;

c. One U.S.-based data analytics company;

d. One U.S.-based media and entertainment company;

e. One U.S.-based social media company;

f. One U.S.-based information management company;

g. One U.S.-based technology staffing company;

h. Three U.S.-based defense contractors;

i. One U.S.-based public utility;

j. One U.S.-based energy company;

k. One U.S.-based city department of education;

l. One Australia-based shipping company; and

m. One major, worldwide airline.

59. KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, further sought to monetize stolen compromised credentials through their sale on various Internet "dark web" forums, under

various online pseudonyms used by FAYAZ, including "Achilles," "The Joker," and "b.c.monster." In addition to the victims described above, FAYAZ offered for sale credentials for compromised accounts for additional private sector companies and public systems located in the United States, the United Kingdom, Canada, Saudi Arabia, the United Arab Emirates, Kuwait, Italy, Norway, Netherlands, Greece, Sweden and Luxembourg.

STATUTORY ALLEGATIONS

60. From at least in or about October 2018 through at least in or about March 2022, in the Southern District of New York and elsewhere, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, and others known and unknown, who will first enter the United States in the Southern District of New York, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit offenses against the United States, to wit, computer intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2), 1030(c)(2)(B)(i), and 1030(c)(2)(B)(iii).

61. It was a part and an object of the conspiracy that KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI,

a/k/a "Mojtaba Ghaleh Koui," the defendants, and others known and unknown, would and did intentionally access computers without authorization, and exceed authorized access, and thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and the value of the information obtained would and did exceed $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2), 1030(c)(2)(B)(i), and 1030(c)(2)(B)(iii).

Overt Acts

62. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about November 2018, SABER SHAHBAZI BALLOJEH, the defendant, conducted a password spray attack against the servers of a U.S.-based information technology company.

b. In or about November 2018, KEYVAN FAYAZ a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," the defendant, sold stolen login credentials for a compromised account at a private company to another individual.

c. In or about December 2018, FAYAZ conducted a password spray attack against the servers of a private company.

d. In or about December 2020, MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendant, conducted a password spray attack against the servers of a COVID-19 vaccine developer.

(Title 18, United States Code, Section 371; Title 18, United States Code, Section 3238.)

COUNT TWELVE
(Computer Intrusion)

The Grand Jury further charges:

63. The allegations contained in paragraphs 1 through 28, 47 through 51, and 58 through 59 of this Indictment are repeated and realleged as if fully set forth herein.

64. From at least in or about October 2018 through at least in or about March 2022, in the Southern District of New York and elsewhere, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, and others known and unknown, would and did intentionally access computers without authorization, and exceed authorized access, and thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and the value of the information obtained would and did exceed $5,000, in violation of Title 18, United States

Code, Sections 1030(a)(2), 1030(c)(2)(B)(i), and 1030(c)(2)(B)(iii).

COUNT THIRTEEN
(Conspiracy to Commit Wire Fraud)

The Grand Jury further charges:

65. The allegations contained in paragraphs 1 through 28, 47 through 51, and 58 through 59 of this Indictment are repeated and realleged as if fully set forth herein.

66. From at least in or about October 2018 through at least in or about March 2022, in the Southern District of New York and elsewhere, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, and others known and unknown, who will first enter the United States in the Southern District of New York, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

67. It was a part and object of the conspiracy that KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for

obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, FAYAZ, BALLOJEH, and GALEKUHI obtained and used stolen login credentials of authorized users of victim computer networks, including those identified in paragraph 58, to obtain unauthorized access to that network and to steal proprietary data, which scheme involved the use of interstate wires, including remote interstate logins to victim servers.

(Title 18, United States Code, Section 1349; and Title 18, United States Code, Section 3238.)

COUNT FOURTEEN
(Aggravated Identity Theft)

The Grand Jury further charges:

68. The allegations contained in paragraphs 1 through 28, 47 through 51, and 58 through 59 of this Indictment are repeated and realleged as if fully set forth herein.

69. From at least in or about October 2018 through at least in or about March 2022, in the Southern District of New York and elsewhere, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The

Joker," a/k/a "b.c.monster," SABER SHAHBAZI BALLOJEH, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, who will first enter the United States in the Southern District of New York, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), and aided and abetted the same, to wit, FAYAZ, BALLOJEH, and GALEKUHI transferred, possessed, and used, and aided and abetted the transfer, possession, and use of, the usernames and passwords of various employees at private sector companies and one governmental entity during and in relation to the wire fraud and computer fraud offenses charged in Counts Eleven, Twelve, and Thirteen of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b) and 2; Title 18, United States Code, Section 3238.)

FORFEITURE ALLEGATION AS TO COUNTS ONE, THREE, FIVE, EIGHT, ELEVEN, AND TWELVE

70. As a result of committing one or more of the offenses alleged in Counts One, Three, Five, Eight, Eleven, and Twelve of this Indictment, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD

MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," AMIR BARATI, SABER SHAHBAZI BALLOJEH, ARMAN KAHZADIAN, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, shall forfeit to the United States, pursuant to Title 18, United States Section, Section 1030(i), any and all property, real or personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of said offenses, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses that the defendants personally obtained.

FORFEITURE ALLEGATION AS TO COUNTS TWO, FOUR, SIX, NINE, AND THIRTEEN

71. As a result of committing the offenses alleged in Counts Two, Four, Six, Nine, and Thirteen of this Indictment, GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, SAJJAD TAHMASEBI, SAEID HOUSHYAR, BEHZAD MESRI, a/k/a "Skote Vahshat," MANOUCHEHR HASHEMLOO, KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker," a/k/a "b.c.monster," AMIR BARATI, SABER SHAHBAZI

BALLOJEH, ARMAN KAHZADIAN, and MOJTABA GALEKUHI, a/k/a "Mojtaba Ghaleh Koui," the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any and all property, real and personal, which constitutes or is derived from proceeds traceable to the commission said offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses that the defendants personally obtained.

Substitute Assets Provision

72. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

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

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

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 which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981 & 1030;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)

[redacted]
FOREPERSON

Damian Williams /NWC
DAMIAN WILLIAMS
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

GHOLAMREZA RAFATNEJAD,
EHSAN MOHAMMADI,
ABDOLLAH KARIMA, a/k/a "Vahid Karima,"
MOSTAFA SADEGHI,
SEYED ALI MIRKARIMI,
MOHAMMED REZA SABAHI,
ROOZBEH SABAHI,
ABUZAR GOHARI MOQADAM,
SAJJAD TAHMASEBI,
SAEID HOUSHYAR,
BEHZAD MESRI, a/k/a "Skote Vahshat,"
MANOUCHEHR HASHEMLOO,
KEYVAN FAYAZ, a/k/a "Achilles," a/k/a "The Joker,"
a/k/a "b.c.monster,"
AMIR BARATI,
SABER SHAHBAZI BALLOJEH,
ARMAN KAHZADIAN, and
MOJTABA GALEKUHI, a/k/a "Mojtava Ghaleh Koui,"

Defendants.

SEALED INDICTMENT

S2 18 Cr. 94 (JMF)

(18 U.S.C. §§ 1030(b), 1030(a)(2), 1030(c)(2)(B)(i), (c)(2)(B)(iii), 1343, 1349, 1028A(a)(1), 1028A(b), 3238 and 2.)

DAMIAN WILLIAMS
United States Attorney.

TRUE BILL

[redacted]

FOREPERSON