UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | |
| -v.- | : | SEALED INDICTMENT |
| GHOLAMREZA RAFATNEJAD,<br>EHSAN MOHAMMADI,<br>ABDOLLAH KARIMA,<br>a/k/a "Vahid Karima,"<br>MOSTAFA SADEGHI,<br>SEYED ALI MIRKARIMI,<br>MOHAMMED REZA SABAHI,<br>ROOZBEH SABAHI,<br>ABUZAR GOHARI MOQADAM, and<br>SAJJAD TAHMASEBI, | : | 18 Cr. _____ |
| Defendants. | : | |

18 CRIM 94

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, and SAJJAD TAHMASEBI, the 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 defendants conducted cyber intrusions into computer systems belonging to at least 176 universities located in 21 foreign countries, including Australia, Canada, China, Denmark, Finland, Germany, Ireland, Israel, Italy, Japan, Malaysia, Netherlands, Norway, Poland, Singapore, South Korea, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. The 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 members of the conspiracy 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 defendants 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 36 private sector companies, and at least two non-governmental organizations ("NGOs").

## MEANS AND METHODS OF THE CONSPIRACY

### University Hacking Campaign

4. 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.

5. 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 7,998 accounts worldwide, of which at least approximately 3,768 belonged to professors at United States-based victim universities.

6. 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

7. In addition to targeting and compromising universities, the Mabna Institute defendants targeted and compromised employee email accounts for at least approximately 36 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. Two media and entertainment companies;

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; and

n. One stock images company.

8. 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

9. 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

10. 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.


11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

## STATUTORY ALLEGATIONS

20. 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, and SAJJAD TAHMASEBI, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit computer intrusion offenses in violation of Title 18, United States Code, Sections 1030(a)(2), 1030(c)(2)(B)(i), 1030(c)(2)(B)(iii), 1030(a)(6) and 1030(c)(2)(A).

21. 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, and SAJJAD TAHMASEBI, 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).

22. 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, and SAJJAD TAHMASEBI, 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).

(Title 18, United States Code, Section 1030(b).)

COUNT TWO
**(Conspiracy to Commit Wire Fraud)**

The Grand Jury further charges:

23. The allegations contained in paragraphs 1 through 19 of this Indictment are repeated and realleged as if fully set forth herein.

24. 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, and SAJJAD TAHMASEBI, 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.

25. 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, and SAJJAD TAHMASEBI, 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.

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

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

The Grand Jury further charges:

26. The allegations contained in paragraphs 1 through 19 of this Indictment are repeated and realleged as if fully set forth herein.

27. 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, and SAJJAD TAHMASEBI, 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, and the value of which exceeded $5,000, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, GOHARI MOQADAM, and TAHMASEBI 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:

28. The allegations contained in paragraphs 1 through 19 of this Indictment are repeated and realleged as if fully set forth herein.

29. 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, and SAJJAD TAHMASEBI, 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, GOHARI MOQADAM, and TAHMASEBI obtained

University-1 professor login credentials through misrepresentations, including, by among other means, sending spearphishing messages 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.

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

## COUNT FIVE

**(Computer Fraud - Unauthorized Access for Private Financial Gain)**

The Grand Jury further charges:

30. The allegations contained in paragraphs 1 through 19 of this Indictment are repeated and realleged as if fully set forth herein.

31. 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, and SAJJAD TAHMASEBI, 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, and the value of which exceeded $5,000, to wit, RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, GOHARI MOQADAM, and TAHMASEBI 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:

32. The allegations contained in paragraphs 1 through 19 of this Indictment are repeated and realleged as if fully set forth herein.

33. 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, and SAJJAD TAHMASEBI, 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, GOHARI MOQADAM, and TAHMASEBI obtained University-2 professor login credentials through misrepresentations, including, by among other means, sending spearphishing messages 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.

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

## COUNT SEVEN
**(Aggravated Identity Theft)**

The Grand Jury further charges:

34. The allegations contained in paragraphs 1 through 19 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, and SAJJAD TAHMASEBI, 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, GOHARI MOQADAM, and TAHMASEBI 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 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.)

FORFEITURE ALLEGATION AS TO COUNTS ONE, THREE, AND FIVE

36. As a result of committing one or more of the offenses alleged in Counts One, Three, and Five 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, and SAJJAD TAHMASEBI, 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 defendant personally obtained.

FORFEITURE ALLEGATION AS TO COUNTS TWO, FOUR, AND SIX

37. As a result of committing the offenses alleged in Counts Two, Four, and Six 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, and SAJJAD TAHMASEBI, 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 defendant personally obtained.

Substitute Assets Provision

38. If any of the above-described forfeitable property, 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 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 defendant 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

Geoffrey Berman

GEOFFREY S. BERMAN
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, and
SAJJAD TAHMASEBI,

Defendants.

SEALED INDICTMENT

18 Cr. ___

(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), and 2.)

GEOFFREY S. BERMAN
United States Attorney.

TRUE BILL

[redacted]

FOREPERSON