UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 20-
	:	
HOOMAN HEIDARIAN,	:	18 U.S.C. § 371
a/k/a "neo" and	:	18 U.S.C. § 1028A
MEHDI FARHADI,	:	18 U.S.C. § 1029
a/k/a "Mehdi Mahdavi"	:	18 U.S.C. § 1030
	:	18 U.S.C. § 1349
	:	18 U.S.C. § 2

I N D I C T M E N T

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

Count One
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers and Access Devices)

Overview

1. Since at least approximately 2010, defendants HOOMAN HEIDARIAN and MEHDI FARHADI (collectively, "Defendants") operated from Iran to conduct coordinated cyber-intrusions and hacking campaigns into computer systems in the United States and around the world. Defendants targeted universities, defense contractors, foreign policy organizations, non-governmental organizations (NGOs), non-profits, and countries and individuals identified as rivals or adversaries to Iran, including Saudi Arabia and Israel.

2. Defendants' scheme was often politically motivated and sometimes at the behest of Iran. The stolen data was typically highly protected and extremely sensitive, and included confidential communications pertaining to

national security, unpublished scientific research, protected non-military nuclear information, sensitive human rights activist information, and foreign policy intelligence. Defendants targeted non-military nuclear information during a time of sensitive international negotiations involving sanctions against Iran for nuclear activity and leading up to the Joint Comprehensive Plan of Action, the agreement between Iran and China, France, Russia, United Kingdom, and the United States on the Iranian nuclear program reached on July 14, 2015.

3. Defendants carefully selected their victims, stealing data from victim networks to use, disseminate, create intelligence dossiers, and sell on the black market. The stolen data included personal identifying information of individual users of victim networks, such as access credentials, names, addresses, phone numbers, social security numbers, and birth dates. In many instances, upon gaining access to computer systems, the defendants vandalized websites using the pseudonym "Sejeal" and posted messages that appeared to signal the purported demise of Iran's internal opposition, foreign adversaries, and countries identified as rivals to Iran, including Saudi Arabia and Israel.

4. Defendants created presentations showcasing their hacking techniques, insider access, and tailored methods for future operations against victim networks. After the theft of victim data, Defendants shared, priced and marketed for sale clusters of data to customers, including Iran. Some of this

information was related to Iran's state-sponsored surveillance efforts of dissidents, human rights activists, and opposition leaders.

5. At all times relevant to this Indictment:

Relevant Individuals and Entities

a. Defendant HOOMAN HEIDARIAN, a/k/a "neo," was an Iranian national who resided in Hamedan, Iran, and had extensive experience in social engineering, data interception, web application hacking, botnet management and denial of service attacks. Defendant HEIDARIAN claimed responsibility for carrying out over 1,000 destructive and disruptive hacks against computer sites that purportedly opposed the Government of the Islamic Republic of Iran ("GOI") and engaged in intrusions to extract information from foreign networks. Defendant HEIDARIAN claimed that some of these malicious activities were conducted at the behest of, or ultimately for the benefit of, Iran. In the course of describing his hacking activities during the time period of the conspiracy, defendant HEIDARIAN highlighted himself as an Iranian, a Shia hacker, and openly declared a strong opposition to Arabs, Sunni Muslims, Saudi Arabia, and Israel, among other perceived enemies of Iran.

b. Defendant MEHDI FARHADI, a/k/a "Mehdi Mahdavi," was an Iranian national, who resided in Hamedan, Iran, and was a prolific computer hacker who engaged in destructive and disruptive hacks against computer sites on a freelance and contract basis. Defendant FARHADI regularly partnered with, and often directed, defendant HEIDARIAN to target

specific victim entities. During the course of the conspiracy, defendant FARHADI compromised at least approximately 50 victim accounts and procured Internet infrastructure for carrying out hacking operations.

c. Victim-1 was a U.S. public research university located in Newark, New Jersey, that specialized in health sciences.

d. Victim-2 was a telecommunications provider located in Israel that provided mobile phone services.

e. Victim-3 was a U.S. educational organization located in New Jersey.

f. Victim-4 was an international organization that promoted the non-military use of nuclear technology, the safeguarding of nuclear materials, and international nuclear security standards. Victim-4 had an office in New York.

g. Victim-5 was a U.S. defense contractor that specialized in aerial vehicles technology, aircraft launch systems, and other products for government and private customers. Victim-5 was headquartered in California.

h. Victim-6 was an aerospace company located in Saudi Arabia.

i. Victim-7 was a U.S. non-profit, non-partisan policy institution that conducted research and analysis on matters of cyber intelligence, international security, and military forces. Victim-7 was headquartered in Washington, D.C., and also had locations in approximately 50 countries around the world.

j. Victim-8 was a U.S. private research university located in Washington, D.C.

k. Victim-9 is a non-profit college located in Israel.

l. Victim-10 was a governmental agency whose responsibilities included regulating media and managing communications. Victim-10 was located in Saudi Arabia.

m. Victim-11 was a governmental agency that provided communications infrastructure and data center services, gathered data on communications platforms linked to terror groups or their supporters, and blocked online activity and websites linked to terror groups or extremists. Victim-11 was located in Afghanistan.

n. Victim-12 was an international non-profit NGO that promoted and safeguarded human rights in Iran. Victim-12 broadcast and disseminated information regarding political prisoners and human rights violations allegedly conducted by, or on behalf of, Iran. Victim-12 was headquartered in Virginia.

o. Victim-13 was a company that provided communications services such as Voice over Internet Protocol ("VoIP") and cloud products to customers around the world, including Iran. Victim-13 was based in the U.K.

p. NJ Victims-1 through -5 were individuals who resided in New Jersey.

Relevant Terms

q. A “botnet" was a collection of computers infected with malware and controlled by a hacker. A “Denial of Service Attack” involved using computers, commonly a botnet, to flood a victim website with repeated requests for information or data, which could effectively cripple the website by overloading it with too much information simultaneously.

r. The “Domain Name System” or “DNS” was a naming system for computers, services, or other resources connected to the Internet and associates various information with domain names assigned to each of the participating entities.

s. An “IP address” was a unique address assigned to a particular internet connection. Computers attached to the Internet used an internet connection which was assigned an IP address so that Internet traffic sent from and directed to that computer could be directed properly from its source to its destination.

t. A “key logger” was software that recorded the action of the keys struck on a keyboard, typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data could then be retrieved by the person operating the key logger.

u. “Malware” was malicious computer software intended to cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, usually unbeknownst to

that person. A “remote access Trojan” or “RAT” was a type of malware the created a back door for administrative control over the target computer.

v. “Session hijacking” was the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system

w. “Spamming” was the use of messaging systems to send an unsolicited message to large numbers of recipients

x. “Structured Query Language” or “SQL” was a computer programming language designed to retrieve and manage data in computer databases. A “SQL Injection Attack” was a method of hacking into and gaining unauthorized access to computers connected to the Internet using a series of SQL instructions.

y. A “server” was a type of computer or device on a network that managed network resources. A “Virtual Private Server,” or “VPS,” was a virtual server that a user perceived as a single physical server, even though it was installed on a physical server potentially running multiple operating systems.

z. A “Virtual Private Network” or “VPN” was a software service that extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

The Conspiracy

6. From in or about January 2010 through on or about January 1, 2017, in the District of New Jersey, and elsewhere, the defendants,

HOOMAN HEIDARIAN,
a/k/a "neo," and
MEHDI FARHADI,
a/k/a "Mehdi Mahdavi,"

who will first be brought to the District of New Jersey, did knowingly and intentionally conspire and agree with each other and others to commit offenses against the United States, that is:

a. to access computers without authorization and exceed authorized access to computers, and thereby obtain information from protected computers, for the purpose of commercial advantage and private financial gain, and the value of the information obtained would and did exceed $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i) and (iii);

b. to knowingly and with intent to defraud access to a protected computer without authorization and by means of such conduct further the intended fraud and obtain something of value, including the use of the computer, and the value of such use was more than $5,000 within a 1-year time period, contrary to Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A);

c. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct,

intentionally cause damage without authorization to a protected computer, thus causing loss to persons during a 1-year period from Defendants' course of conduct affecting protected computers aggregating at least $5,000 in value, and damage affecting 10 or more protected computers during a 1-year period, contrary to Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(VI), and (c)(4)(B); and

d. to knowingly, with intent to defraud, possess fifteen or more devices which are counterfeit and unauthorized access devices contrary to Title 18, United States Code, Section 1029(a)(3).

Goal of the Conspiracy

7. The goal of the conspiracy was for Defendants, acting from inside Iran, to hack into victim computers and networks to: (a) steal intellectual property and other data; (b) sell such stolen data to customers, including Iran; (c) use proceeds from the sale of stolen data to accumulate personal wealth and to invest in future hacking activities; and (d) destroy and deface websites to intimidate perceived enemies of Iran and help Iran project influence around the world.

Manner and Means of the Conspiracy

8. It was part of the conspiracy that:

a. Defendants conducted online reconnaissance to carefully select their victims, gathering data and intelligence to determine their areas of expertise, and assessing victim computer networks in preparation for

launching cyber-attacks. This reconnaissance phase included network scanning to discern the victims' IP address range, accessible hosts, router locations, network mapping, and DNS records, all to assess the vulnerability of the victims' computer networks. Defendants often used information obtained at this stage in latter phases of their hacking activities to complete a picture of processes, organizational structure, and potential soft spots of victim networks.

b. Defendants gained and maintained unauthorized access to victim networks using various tools, including: (i) session hijacking; (ii) SQL injection; and (iii) malware installations.

c. Defendants used key loggers and RATs to maintain access and monitor the actions of users of the victim networks.

d. Defendants developed a botnet tool, which facilitated the spread of malware, Denial of Service attacks, and spamming to victim networks.

e. Defendants stole hundreds of terabytes of data from their victims, including confidential work product, intellectual property, and personal identifying information, such as access credentials, names, addresses, phone numbers, social security numbers, and birth dates.

f. Defendants replaced the publicly available contents of websites with political and other ideological content, thereby defacing websites, for the apparent purpose of projecting Iranian influence and threatening perceived enemies of Iran. The defacements featured, among other things,

images of burning Israeli flags and threats forecasting the death or demise of citizens in the United States, Israel, and elsewhere.

g. Defendants and their co-conspirators leveraged unauthorized access to victim networks or accounts to establish automated forwarding rules for compromised victim accounts, whereby new outgoing and incoming emails were automatically forwarded from the compromised accounts to accounts controlled by Defendants.

h. Defendants, using the pseudonym "Sejeal," regularly posted evidence of their network intrusions and defacements on other publicly available websites. In some cases, Defendants notified various media outlets to ensure coverage of certain of their hacking attacks, to gain recognition in the hacking community for their work, leverage that status to exchange hacking best-practice tips with other cyber hackers, and increase their profile to promote future contract work. Defendants regularly used the website Zone-H.org ("Zone-H"), a forum used by cyber criminals to post evidence of their network intrusions and website defacements. Between 2010 and 2017, Zone-H listed over 106,232 website defacements by the pseudonym "Sejeal," obtaining a top world ranking according to Zone-H for hacking intrusions.

i. Defendants marketed the data they stole, seeking to sell it to interested buyers on the black market. In some cases, Defendants summarized the information stolen from victims in finished reports that were often provided to prospective customers seeking hacked data. Defendants maintained price

lists in Iranian rials or U.S. dollars that outlined market values for victim network access and previously stolen victim data.

j. Defendants attempted to hide their true identities and locations by using aliases and VPS services. Defendants used compromised credit cards stolen from hacking activities to purchase VPS on private computer networks owned by third parties, and used these networks to conduct cyber operations. By using VPS, Defendants and their co-conspirators obfuscated their true IP addresses, location, and identities in order steal data from the victims.

"Sejeal" Defacements and Destructive Cyber Actions

9. It was further part of the conspiracy that from in or about January 2010 through in or about January 1, 2017, Defendants conducted sustained defacements and threatening text message dissemination campaigns against perceived adversaries of Iran, always bearing attribution to "Sejeal", as set forth below:

Victim-1: Public Research University in Newark, New Jersey

a. On or about March 17, 2013, Defendants unlawfully gained access Victim-1's computer system by exploiting security vulnerabilities associated with a version of a Content Management System (CMS) plugin used on the victim website.

b. Defendant modified the contents of the website to display the text "Sejeal," and to display imagery of a burning Israeli flag. The following is a screenshot of the defacement of the Victim-1 website:

Victim-2: Israeli Telecommunications Provider

c. On or about April 25, 2015, Defendants, using the pseudonym "Sejeal," gained unauthorized access to a large database of Israel-based cellular phone numbers by compromising Victim-2, an Israeli telecommunications company. Defendants subsequently compromised a UK-based technology company specializing in bulk text messaging and used this unauthorized access to spam approximately 2.5 million Israeli customers with the short messaging service (SMS) text message "Sejeal is Coming Soon! In memory of the martyrs of Yemen."

d. Following the bulk message threat dissemination, Defendants sent each other descriptions of how the hacked numbers were

obtained, and how messages were sent leveraging the unauthorized access of the U.K.-based text messaging service. Defendants tracked the media coverage and social media dissemination of this SMS hack and sent each other various screen shots, including the following:

Victim-3: Educational organization in New Jersey

e. From on or about July 4, 2011 through on or about December 25, 2012, Defendants gained unauthorized access to a network owned by Victim-3, a N.J.-based educational organization, and defaced a website by modifying the contents of the website to display the text "Sejeal" and "Death to…….Iranian Martyrs," with imagery of a burning Israeli flag used as a backdrop.

SEJEAL Identity Thefts

10. It was further part of the conspiracy that from on or about July 4, 2011 through on or about December 25, 2012, Defendants used their

unauthorized access to Victim-3's networks to steal the personal information, including account usernames and passwords, of at least 26 individuals affiliated with Victim-3. Defendants then used the stolen victim information to steal financial information for personal gain, often using email accounts that were created using false identifier information ("Fraudulent Email Accounts"). For example, Defendants fraudulently purchased computer security software and VPN services with personally identifiable information obtained from the Victim-3 intrusion, combining compromised New Jersey credit card information with fake addresses to evade detection. Defendants then used the software and VPN services to improve their operational security in subsequent intrusion methods.

Nuclear and Military Data Theft

11. It was further part of the conspiracy that between on or about, January 2010, and on or about January 1, 2017, Defendants conducted intrusions to gain unauthorized access to non-Iranian nuclear and military technology information as set forth below:

Victim-4: International Organization in New York

a. From in or about January 2013 through in or about January 2015, Defendants targeted and gained unauthorized access to Victim-4's servers. Defendants targeted network servers and compromised numerous victim accounts. Defendants exchanged login credentials, including usernames and passwords, for compromised Victim-4 accounts.

b. Defendants' intrusions and data theft for Victim-4 were conducted during a time of sensitive international negotiations involving sanctions against Iran for nuclear activity, leading up to the Joint Comprehensive Plan of Action, the agreement between Iran and China, France, Russia, United Kingdom, and the United States on the Iranian nuclear program reached on July 14, 2015.

c. Following the Victim-4 attack, Defendants described the hacking techniques used to gain unauthorized access to the network in a document labeled "Pentest Report" and shared the document with other conspirators. A photo of the cover page of the report is provided below:

d. The report used exfitrated graphics to showcase the unauthorized access to the network and generate interest from conspirators or prospective black market buyers, and it sought conspirator input on the nature of the stolen materials.

Victim-5: U.S. Defense Contractor in California

e. From in or about August 2015 through in or about December 2016, Defendants gained unauthorized access to servers within Victim-5's network, including those that hosted documents and data pertaining to personal information of company employees and researchers. Defendants compromised numerous victim accounts in the course of this intrusion. Defendants exchanged login credentials (i.e., usernames and passwords) for compromised accounts, and described computer hacking techniques used to gain unauthorized access to the network.

Victim-6: Aerospace Company in Saudi Arabia

f. On or about May 22, 2015, defendant HEIDARIAN provided defendant FARHADI with a report that summarized a computer intrusion into the network of Victim-6, an aerospace company located in Saudi Arabia. The report included screenshots of portions of the internal network that demonstrated remote access allowing the actors to delete or upload files to the network and a summary of various types of aircraft. The screenshots included a directory with over twenty resumes, a screenshot of a computer program providing access into the company's network that enumerated directories, and a database with Saudi citizens' personally identifiable information ("PII"), to include 15,756 records consisting of individuals' names, emails, dates of birth, national ID numbers and mobile phone numbers.

International Policy, Research and Foreign Government Data Theft

12. It was further part of the conspiracy that between in or about January 2010 through on or about January 1, 2017, Defendants conducted intrusions to steal data pertaining to policy and academic research, as set forth below:

Victim-7: U.S. Policy Institution in Washington, D.C.

a. From in or about May 2014 through in or about October 2015, Defendants gained unauthorized access to Victim-7's network, and obtained information for numerous individual accounts.

b. Defendants used their unauthorized access to Victim-7's network to maintain access to some of the compromised individual accounts. This unauthorized access allowed Defendants to appear to the victim servers as if the intruder had previously obtained valid access to the associated user's account, obviating the need to enter a username and password for that account.

c. Defendants discussed between themselves how to gain unauthorized access to other areas of Victim-7's network to further exploit network vulnerabilities. On or about October 12, 2015, the defendants completed and shared a finished hacking report for Victim-7, which included over 2,905 individual usernames, corresponding passwords, and individual user subscriber information previously stolen from the Victim-7 network. Additionally, on or about May 15, 2016, defendant HEIDARIAN sent defendant

FARHADI a file containing instructions on how to navigate around the Victim-7 network.

Victim-8: Private Research University in Washington. D.C.

d. In or about August 2013, Defendants gained unauthorized access into a website owned by Victim-8. Thereafter, Defendants stole university files, documents, and databases containing the names of professors, scientific journals, and student information. Defendants also downloaded malicious files and software tools onto the victim computer network to gain and maintain further unauthorized access to university systems and to conceal the extent of such unauthorized access.

e. In or about August 2013, Defendants offered for sale on the black market approximately 45 gigabytes of data stolen from Victim-8.

Victim-9: Non-Profit College in Israel

f. In or about August 2015, Defendants gained unauthorized access to Victim-9's network. Defendants accessed files, documents and a database that included information on names of professors, the college's administrative letters and scientific journals. Defendants stole more than 10,000 files.

Victim-10 – Governmental Agency in Saudi Arabia

g. On or about October 21, 2015, Defendant HEIDARIAN saved a screenshot that demonstrated unauthorized access to a Microsoft Exchange server within the network of Victim-10. The screenshot showed the group

mailbox for the website, and enumerated approximately 6,706 objects, including entries for individual employees, their emails, and organizational units. Another screenshot in the same folder showed an image of directories for Exchange Database and so-called MDBdata, which are files containing database queries, tables, and other information used to link to and store data from server files and applications. Another screenshot was entitled "shell" and showed remote access to the .gov.sa domain.

Victim-11: Governmental Agency in Afghanistan

h. On or about August 4, 2015, Defendants gained unauthorized access to corporate email communications for Victim-11. Defendants stole emails, and used their unauthorized access to review internal Afghanistan government communications at all levels of government. The compromised emails included log-in credentials for domains related to the Office of the Afghani President, usernames and passwords for multiple Afghani university domains, and reservation details for international delegations visiting Afghanistan.

International Dissident Surveillance

13. It was further part of the conspiracy that from in or about January 2010 through on or about January 1, 2017, Defendants stole information from victim computers and systems of human rights organizations and telecommunications companies, including data on perceived domestic and international enemies of Iran, as set forth below:

Victim-12: Human Rights Non-Governmental Organization in Virginia

a. From in or about January 2014 through in or about December 2014, Defendants gained unauthorized access to network servers in the United States for Victim-12. Defendants gained control of the main panel of the victim server, allowing full unauthorized access to the systems administrator pages, and the administrator's emails. Defendants compromised numerous victim accounts in the course of this intrusion.

b. Defendants planned to use the unauthorized access to the Victim-12 network to track the automated system and the individuals who visited and used the entity website. Defendants also exchanged login credentials (i.e., usernames and passwords), for compromised accounts.

Victim-13: Communications company in the United Kingdom

c. From in or about December 2014 through in or about January 2015, Defendants gained unauthorized access to the network of Victim-13. Defendants obtained unauthorized access to more than 35,000 subscriber records, including individual biodata, phone numbers, email accounts, and other databases. Defendants also gained access to recorded VoIP calls and SMS messages delivered to the United Kingdom, including callers and SMS users from within Iran.

Overt Acts

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

a. On or about March 17, 2013, in Newark, New Jersey, Defendants unlawfully gained access to the Victim-1 computer system and modified the contents of the website to display the text "Sejeal," and to display imagery of a burning Israeli flag.

b. On or about July 4, 2011, in the District of New Jersey, Defendants unlawfully gained access to a network owned by Victim-3 and defaced a website by modifying the contents of the website to display the text "Sejeal" and "Death to……Iranian Martyrs," with imagery of a burning Israeli flag used as a backdrop.

c. On or about June 21, 2013, defendant FARHADI accessed emails which had been forwarded to Employee A's fraudulent account.

d. On or about April 25, 2015, Defendants sent 2.5 million Israel-based cellular phone numbers previously obtained from hacking into Victim-2 computers a text message stating that "Sejeal is Coming Soon! In memory of the martyrs of Yemen."

e. On or about May 21, 2015, defendant HEIDARIAN emailed a co-conspirator numerous usernames and passwords stolen from Victim-7.

f. On or about August 4, 2015, Defendants gained unauthorized access to corporate email communications for Victim-11, a governmental agency in Afghanistan.

g. On or about May 15, 2016, defendant HEIDARIAN sent defendant FARHADI a file containing instructions on how to navigate around the Victim-7 network.

All in violation of Title 18, United States Code, Sections 371.

COUNT TWO

(Computer Fraud - Unauthorized Access to Protected Computers)

1. The allegations contained in paragraphs 1 through 5 and 7 through 14 of Count One in this Indictment are repeated and realleged as if fully set forth herein.

2. From at least in or about 2010 through at least in or about 2017, in the District of New Jersey and elsewhere, the defendants,

HOOMAN HEIDARIAN,
a/k/a "neo," and
MEHDI FARHADI,
a/k/a "Mehdi Mahdavi"

who will first be brought to the District of New Jersey, willfully and without authorization attempted to access and did access 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, HOOMAN HEIDARIAN and MEHDI FARHADI conducted, aided, and abetted in conducting, computer intrusions to gain unauthorized access to the computer systems of Victim-5 and obtained and sold stolen resources from Victim-5 as well as access to compromised Victim-5 employee accounts.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2) (B) (i) and (iii) and 2.

COUNT THREE
(Computer Fraud - Unauthorized Damage to Protected Computers)

1. The allegations contained in paragraphs 1 through 5 and 7 through 14 of Count One of this Indictment are repeated and realleged as if fully set forth herein.

2. From at least in or about 2010 through at least in or about 2017, in the District of New Jersey and elsewhere, the defendants,

HOOMAN HEIDARIAN,
a/k/a "neo," and
MEHDI FARHADI,
a/k/a "Mehdi Mahdavi"

who will first be brought to the District of New Jersey, knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, to wit, HOOMAN HEIDARIAN and MEHDI FARHADI conducted, aided, and abetted in conducting, computer intrusions to gain unauthorized access to the computer systems of Victim-7 and obtained and sold stolen resources from Victim-7 as well as access to compromised Victim-7 employee accounts, and the offense caused loss to persons during a 1-year period from Defendants' course of conduct affecting protected computers aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(a), and 2.

COUNT FOUR
(Conspiracy to Commit Wire Fraud)

1. The allegations contained in paragraphs 1 through 5 and 7 through 14 of Count One of this Indictment are realleged as if fully set forth herein.

2. From in or about 2010 through in or about 2017, in the District of New Jersey and elsewhere, the defendants,

HOOMAN HEIDARIAN,
a/k/a "neo," and
MEHDI FARHADI,
a/k/a "Mehdi Mahdavi,"

who will first be brought to the District of New Jersey, did knowingly and intentionally conspire and agree with each other and others to devise a scheme and artifice to defraud Victims-1 through -13, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

All in violation of Title 18, United States Code, Sections 1349.

COUNT FIVE
(Access Device Fraud)

1. The allegations contained in paragraphs 1 through 5 and 7 through 14 of Count One of this indictment are repeated and realleged as if fully set forth herein.

2. On or about October 12, 2015, in the District of New Jersey and elsewhere, the defendants,

HOOMAN HEIDARIAN,
a/k/a "neo," and
MEHDI FARHADI,
a/k/a "Mehdi Mahdavi,"

who will first be brought to the District of New Jersey, did knowingly, with intent to defraud, possess fifteen or more devices which are counterfeit and unauthorized access devices, as defined in Title 18, United States Code, Sections 1029(e)(1) and (3), namely usernames and passwords obtained from Victim-7.

In violation of Title 18, United States Code, Sections 1029(a)(3), and 2.

COUNTS SIX through TEN
(Aggravated Identity Theft)

1. The allegations contained in paragraphs 1 through 5 and 7 through 14 of Count One of this indictment are repeated and realleged as if fully set forth herein.

2. On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendants,

HOOMAN HEIDARIAN,
a/k/a "neo," and
MEHDI FARHADI,
a/k/a "Mehdi Mahdavi,"

during and in relation to the crime of conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, as more fully set forth in Count Four above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person as set forth below, each date constituting a separate count of the indictment.

Count	Approximate Date	Means of Identification
Six	October 12, 2015	username, password, email address, and home address of Individual-1 obtained from the network of Victim-7
Seven	October 12, 2015	username, password, email address, and home address of Individual-2 obtained from the network of Victim-7
Eight	October 12, 2015	username, password, email address, and home address of Individual-3 obtained from the network of Victim-7

Count	Approximate Date	Means of Identification
Nine	October 12, 2015	username, password, email address, and home address of Individual-4 obtained from the network of Victim-7
Ten	October 12, 2015	username, password, email address, and home address of Individual-5 obtained from the network of Victim-7

In violation of Title 18, United States Code, Sections 1028A(a)(3), 1028A(b), and 1028(d)(1), and 2.

FORFEITURE ALLEGATION

1. The allegations contained in this Indictment are hereby re-alleged and incorporated by reference for the purpose of noticing forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2), and Title 28, United States Code, Section 2461(c).

2. The United States hereby gives notice to the defendant, that upon his conviction of the offenses charged in this Indictment, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2), and Title 28, United States Code, Section 2461(c), which requires any person convicted of such offenses to forfeit any property constituting or derived from proceeds obtained directly or indirectly as a result of such offenses.

3. 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 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

A TRUE BILL

_____

FOREPERSON

Craig Carpenito

CRAIG CARPENITO
United States Attorney