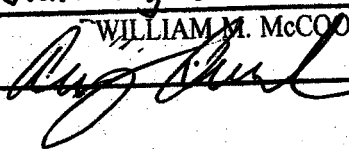


Exhibit 4

Superseding Indictment (Dkt. #7), *United States v. Fedorov*, CR18-004RSM

Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

January 25 20 18
WILLIAM M. McCOOL, Clerk
By  Deputy

UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,

NO. CR18-004RSM

SUPERSEDING INDICTMENT

v.

DMYTRO VALERIEVICH FEDOROV,
aka "hotdima,"
Defendant.

The Grand Jury charges that:

DEFINITIONS

1. **IP Address:** An Internet Protocol address (or simply "IP address") is a unique numeric address used by devices, such as computers, on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 104.250.138.210). Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

1 2. **Server:** A server is a computer that provides services for other computers
2 connected to it via a network or the Internet. The computers that use the server's services
3 are sometimes called "clients." Servers can be physically located anywhere with a
4 network connection that may be reached by the clients; for example, it is not uncommon
5 for a server to be located hundreds (or even thousands) of miles away from the client
6 computers. A server may be either a physical or virtual machine. A physical server is a
7 piece of computer hardware configured as a server with its own power source, central
8 processing unit/s and associated software. A virtual server is typically one of many
9 servers that operate on a single physical server. Each virtual server shares the hardware
10 resources of the physical server but the data residing on each virtual server is segregated
11 from the data on other virtual servers that reside on the same physical machine.

12 3. **Malware:** Malware is malicious computer code running on a computer.
13 Relative to the owner/authorized user of that computer, malware is computer code that is
14 running on the system that is unauthorized and present on the system without the user's
15 consent. Malware can be designed to do a variety of things, including logging every
16 keystroke on a computer, stealing financial information or "user credentials" (passwords
17 or usernames), or commanding that computer to become part of a network of "robot" or
18 "bot" computers known as a "botnet." In addition, malware can be used to transmit data
19 from the infected computer to another destination on the Internet, as identified by an IP
20 address. Often times, these destination IP addresses are computers controlled by cyber
21 criminals.

22 4. **The Carbanak malware:** "Carbanak" is the name given by computer
23 security researchers to a particular malicious software (malware) program. Carbanak has
24 been used to remotely access computers without authorization. The Carbanak malware
25 allows an attacker to spy on another person's computer and remotely control the
26 computer. Carbanak can record videos of the victim's computer screen and send the
27 recordings back to the attacker. It can also let the attacker use the victim computer to
28

1 | attack other computers, and to steal files from the victim computer, and install other
2 | malware. All of this can be done without the legitimate user's knowledge or permission.

3 | 5. **Bot:** A "bot" computer is a computer that has been infected with some kind
4 | of malicious software or code and is thereafter subject to control by someone other than
5 | the true owner. The true owner of the infected computer usually remains able to use the
6 | computer as he did before it was infected, although speed or performance may be
7 | compromised.

8 | 6. **Botnet:** A "botnet" is a network of compromised computers known as
9 | "bots" that are under the control of a cybercriminal or "bot herder." The bots are
10 | harnessed by the bot herder through the surreptitious installation of malware that provides
11 | the bot herder with remote access to, and control of, the compromised computers. A
12 | botnet may be used en masse, in a coordinated fashion, to deliver a variety of Internet-
13 | based attacks, including DDoS attacks, brute force password attacks, the transmission of
14 | spam emails, the transmission of phishing emails, and hosting communication networks
15 | for cybercriminals (e.g., acting as a proxy server for email communications).

16 | 7. **Phishing:** Phishing is a criminal scheme in which the perpetrators use
17 | mass email messages and/or fake websites to trick people into providing information such
18 | as network credentials (e.g., usernames and passwords) that may later be used to gain
19 | access to a victim's systems. Phishing schemes often utilize social engineering
20 | techniques similar to traditional con-artist techniques in order to trick victims into
21 | believing they are providing their information to a trusted vendor, customer, or other
22 | acquaintance. Phishing emails are also often used to trick a victim into clicking on
23 | documents or links that contain malicious software that will compromise the victim's
24 | computer system.

25 | 8. **Spear Phishing:** Spear phishing is a targeted form of phishing directed
26 | towards a specific individual, organization or business. Although often intended to steal
27 | data for malicious purposes, cybercriminals may also use spear phishing schemes to
28 | install malware on a targeted user's computer.

1 United States Code, Section 20, and to obtain moneys, funds, and credits under the
2 custody and control of the financial institutions by means of materially false and
3 fraudulent pretenses, representations, and promises, in violation of Title 18, United States
4 Code, Section 1344(1) and (2).

5 **II. OBJECTIVES OF THE CONSPIRACY**

6 13. Defendant DMYTRO VALERIEVICH FEDOROV, and others known and
7 unknown to the Grand Jury, were part of a financially motivated cybercriminal
8 conspiracy known variously as FIN7, the Carbanak Group, and the Navigator Group
9 (referred to herein as "FIN7"). FIN7 consists of a group of criminal actors engaged in a
10 sophisticated malware campaign targeting the computer systems of businesses, primarily
11 in the restaurant, gaming, and hospitality industries, among others.

12 14. The objectives of the conspiracy included hacking into protected computer
13 networks using malicious software (hereinafter, "malware") designed to provide the
14 conspirators with unauthorized access to, and control of, victim computer systems. The
15 objectives of the conspiracy further included conducting surveillance of victim computer
16 networks, and installing additional malware on victim computer networks for the purpose
17 of establishing persistence, stealing money and property, including payment card (e.g.,
18 credit and debit) track data, financial information, and proprietary and non-public
19 information. The objectives of the conspiracy further included using and selling the
20 stolen data and information for financial gain in a variety of ways, including, but not
21 limited to, using stolen payment card data to conduct fraudulent transactions across the
22 United States and in foreign countries.

23 **III. MANNER AND MEANS OF THE CONSPIRACY**

24 15. The manner and means used to accomplish the conspiracy included the
25 following:

26 a. FIN7 developed and employed various malware designed to
27 infiltrate, compromise, and gain control of the computer systems of victim companies
28 operating in the United States and elsewhere, including within the Western District of

1 Washington. FIN7 established and operated an infrastructure of servers, located in
2 various countries, through which FIN7 members coordinated activity to further the
3 scheme. This infrastructure included, but was not limited to, the use of command and
4 control servers, accessed through custom botnet control panels, that communicated with
5 and controlled compromised computer systems of victim companies.

6 b. FIN7 created a front company doing business as Combi Security to
7 facilitate the malware scheme by seeking to make the scheme's illegal conduct appear
8 legitimate. Combi Security purports to operate as a computer security pen-testing
9 company based in Moscow, Russia and Haifa, Israel. As part of advertisements and
10 public internet pages for Combi Security, FIN7 portrayed Combi Security as a legitimate
11 penetration testing enterprise that hired itself out to businesses for the purpose of testing
12 their computer security systems.

13 c. Under the guise of a legitimate computer security company, FIN7,
14 doing business as Combi Security, recruited individuals with computer programming
15 skills, falsely claiming that the prospective employees would be engaged in legitimate
16 pen-testing of client computer networks. In truth and in fact, as Defendant and his FIN7
17 co-conspirators well knew, Combi Security was a front company used to hire and deploy
18 hackers who were given tasks in furtherance of the FIN7 conspiracy.

19 d. FIN7 targeted victims in the Western District of Washington, and
20 elsewhere, using phishing techniques to distribute malware designed to gain unauthorized
21 access to, take control of, and exfiltrate data from the computer systems of various
22 businesses. FIN7's targeted victims include more than 120 identified companies, with
23 thousands of individual locations of operation throughout the United States, including,
24 but not limited to, the following representative victim companies:

25 i. "Victim-1" referenced herein is the Emerald Queen Hotel and
26 Casino (EQC), a hotel and casino owned and operated by a federally recognized Native
27 American Tribe with locations in Pierce County, within the Western District of
28 Washington.

1 ii. “Victim-2” referenced herein is [REDACTED], a
2 public corporation headquartered in Seattle, within the Western District of Washington,
3 with operations throughout the United States and elsewhere.

4 iii. “Victim-3” referenced herein is Chipotle Mexican Grill, a
5 U.S.-based restaurant chain with thousands of locations in the United States, including in
6 the Western District of Washington, and in Canada and multiple European countries.

7 iv. “Victim-4” referenced herein is [REDACTED], a U.S.-
8 based pizza parlor chain with hundreds of locations predominantly in the Western United
9 States, including in the Western District of Washington.

10 v. “Victim-5” referenced herein is BECU, a U.S.-based
11 federally insured credit union headquartered in the Western District of Washington.

12 vi. “Victim-6” referenced herein is Jason’s Deli, a U.S.-based
13 casual delicatessen restaurant chain with hundreds of locations in the United States.

14 vii. “Victim-7” referenced herein is [REDACTED], an automotive
15 retail and repair chain with hundreds of locations in the United States, including in the
16 Western District of Washington.

17 viii. “Victim-8” referenced herein is Red Robin Gourmet Burgers
18 and Brews (Red Robin), a U.S.-based casual dining restaurant chain, founded in the
19 Western District of Washington, with hundreds of locations in the United States,
20 including in the Western District of Washington.

21 ix. “Victim-9” referenced herein is Sonic Drive-in (Sonic), a
22 U.S.-based drive-in fast-food chain with thousands of locations in the United States,
23 including in the Western District of Washington.

24 x. “Victim-10” referenced herein is Taco John’s, a U.S.-based
25 fast-food restaurant chain with hundreds of locations in the United States, including in the
26 Western District of Washington.

27 e. FIN7 typically initiated its attacks by delivering, directly and
28 through intermediaries, a phishing email with an attached malicious file, using wires in

1 interstate and foreign commerce, to an employee of the targeted victim company. The
2 attached malicious file usually was a Microsoft Word (.doc or .docx) or Rich Text File
3 (.rtf) document with embedded malware. FIN7 used a variety of malware delivery
4 mechanisms in its phishing attachments including, but not limited to, weaponized
5 Microsoft Word macros, malicious Object Linking and Embedding (OLE) objects,
6 malicious visual basic scripts or JavaScript, and malicious embedded shortcut files (LNK
7 files). In some instances, the phishing email or attached file contained a link to malware
8 hosted on servers controlled by FIN7. The phishing email, through false representations
9 and pretenses, fraudulently induced the victim company employee to open the attachment
10 or click on the link to activate the malware. For example, when targeting a hotel chain,
11 the purported sender of the phishing email might falsely claim to be interested in making
12 a hotel reservation. By way of further example, when targeting a restaurant chain, the
13 purported sender of the phishing email might falsely claim to be interested in placing a
14 catering order or making a complaint about prior food service at the restaurant.

15 f. In certain phishing attacks, FIN7, directly and through
16 intermediaries, sent phishing emails to personnel at victim companies who had unique
17 access to internal proprietary and non-public company information, including, but not
18 limited to, employees involved with making filings with the United States Securities and
19 Exchange Commission ("SEC"). These emails used an email address that spoofed an
20 email address associated with the SEC's electronic filing system, and induced the
21 recipients to activate the malware contained in the emails' attachments.

22 g. In many of the FIN7 attacks, a FIN7 member, or someone hired by
23 FIN7 specifically for such purpose, would also call the victim company, using wires in
24 interstate or foreign commerce, to legitimize the phishing email and convince the victim
25 company employee to open the attached document using social engineering techniques.
26 For example, when targeting a hotel chain or a restaurant chain, a conspirator would
27 make a follow-up call falsely claiming that the details of a reservation request, catering
28 order, or customer complaint could be found in the file attached to the previously

1 delivered email, to induce the employee at the victim company to read the phishing
2 email, open the attached file, and activate the malware.

3 h. If the recipient activated the phishing email attachment or clicked on
4 the link, the recipient would unwittingly activate the malware, and the computer on
5 which it was opened would become infected and connect to one or more command and
6 control servers controlled by FIN7 to report details of the newly infected computer and
7 download additional malware. The command and control infrastructure relied upon
8 various servers in multiple countries, including, but not limited to, the United States,
9 typically leased using false information, such as alias names and fictitious information.

10 i. FIN7 typically would install additional malware, including the
11 Carbanak malware, to connect to additional FIN7 command and control servers to
12 establish remote control of the victim computer.

13 j. Once a victim's computer was compromised, FIN7 would
14 incorporate the compromised machine or "bot" into a botnet.

15 k. FIN7 designed and used a custom botnet control panel to manage
16 and issue commands to the compromised machines.

17 l. Once a victim company's computers were incorporated into the
18 FIN7 botnet and remotely controlled by FIN7's malware, the group used this remote
19 control and access to, among other things, install and manage additional malware,
20 conduct surveillance, map and navigate the compromised computer network, compromise
21 additional computers, exfiltrate files, and send and receive data. For instance, FIN7 often
22 conducted surveillance on the victim's computer network by, among other things,
23 capturing screen shots and videos of victim computer workstations that provided the
24 conspirators with additional information about the victim company computer network
25 and non-public credentials for both generic company accounts and for actual company
26 employees.

27 m. FIN7 used its access to the victim's computer network and
28 information gleaned from surveillance of the victim's computer systems to install

1 additional malware designed to target and extract particular information and property of
2 value, including payment card data and proprietary and non-public information. For
3 instance, FIN7 often utilized various “off-the-shelf” software and custom malware, and a
4 combination thereof, to extract and transfer data to a “loot” folder on one or more servers
5 controlled by FIN7.

6 n. FIN7 frequently targeted victim companies with customers who use
7 payment cards while making legitimate point-of-sale purchases, such as victim
8 companies in the restaurant, gaming, and hospitality industries. In those cases, FIN7
9 configured malware to extract, copy, and compile the payment card data, and then to
10 transmit the data from the victim computer systems to servers controlled by FIN7.

11 o. For example, between approximately March 24, 2017, and April 18,
12 2017, FIN7 harvested payment card data from point-of-sale devices at certain Victim-3
13 restaurant locations, including dozens of locations in the Western District of Washington.

14 p. FIN7 stole millions of payment card numbers, many of which have
15 been offered for sale through vending sites, including, but not limited to, Joker’s Stash,
16 thereby attempting to generate millions of dollars of illicit profits.

17 q. The payment card data were offered for sale to allow purchasers to
18 falsely represent themselves as authorized users of the stolen payment cards and to use
19 the stolen payment card information to purchase goods and services in fraudulent
20 transactions throughout the United States and the world, including over the Internet,
21 resulting in millions of dollars in losses to, and thereby affecting, merchants and banks,
22 including financial institutions, as defined in Title 18, United States Code, Section 20.
23 For example, on or about March 10, 2017, stolen payment card data related to accounts
24 held at Victim-5, a financial institution headquartered in the Western District of
25 Washington, compromised through the computer network intrusion of a victim company,
26 was used to make unauthorized purchases at a merchant in Puyallup, Washington.

1 r. FIN7 members employed various techniques to conceal their
2 identities, including simultaneously utilizing various leased servers, that had been leased
3 using false subscriber information, in multiple countries.

4 s. FIN7 member, co-conspirator F.H., served as a high-level systems
5 administrator for FIN7 who maintained servers and communication channels used by the
6 organization. For example, FIN7 members requested co-conspirator F.H. to grant them
7 access to servers used by FIN7 to facilitate the malware scheme. Co-conspirator F.H.
8 also played a management role in the scheme by delegating tasks and by providing
9 instruction to other members of the scheme.

10 t. FIN7 members typically communicated with one another and others
11 through private communication channels to further their malicious activity. Among other
12 channels, FIN7 conspirators communicated using Jabber, an instant messaging service
13 that allows members to communicate across multiple platforms and that supports end-to-
14 end encryption.

15 u. For example, in Jabber communications with other FIN7 members,
16 DMYTRO VALERIEVICH FEDOROV, using his alias "hotdima," referenced using
17 malware in connection with several specific victim companies, discussed using the
18 administrative control panels to receive data from compromised computers, and
19 identified several pen-testers working at his direction.

20 v. FIN7 members often communicated through a private HipChat
21 server. HipChat is a group chat, instant messaging, and file-sharing program. FIN7
22 members used its HipChat server to collaborate on malware and victim business
23 intrusions, to interview potential recruits, and to upload and share exfiltrated data, such as
24 stolen payment card data. As a system administrator, co-conspirator F.H. created
25 HipChat user accounts for FIN7 members that allowed them to access the server.

26 w. Co-conspirator F.H. also created and participated in multiple
27 HipChat "rooms" with other FIN7 members and participated in the uploading and
28 organization of stolen payment card data and malware. For example, on or about March

1 14, 2016, co-conspirator F.H. uploaded an archive that contained numerous data files
2 created by malware designed to steal data from point-of-sale systems that process
3 payment cards. The files contained payment card numbers stolen from a victim company
4 that had publicly reported a security breach that resulted in the compromise of tens of
5 thousands of payment cards. By way of further example, co-conspirator F.H. also set up
6 and used a HipChat room titled "MyFile", in which he was the only participant, and to
7 which he uploaded malware used by FIN7 and stolen payment card information.

8 x. FIN7 conspirators used numerous email accounts hosted by a variety
9 of providers in the United States and elsewhere, which they often registered using false
10 subscriber information.

11 y. FIN7 conspirators frequently used the project management software
12 JIRA, hosted on private virtual servers in various countries, to coordinate their malicious
13 activity and to manage the assorted network intrusions. FIN7 members typically created
14 a "project" and then associated "issues" with the project, each issue akin to an issue
15 directory or folder, for a victim company, which they used to collaborate and share
16 details of the intrusion, to post victim company intelligence, such as network mapping
17 information, and to store and share exfiltrated data.

18 z. For example, on about September 7, 2016, co-conspirator F.H.
19 created an "issue" for Victim-6, to which FIN7 conspirators posted files containing
20 internal credentials for the victim company's computer network.

21 aa. By way of further example, on multiple occasions in January 2017,
22 DMYTRO VALERIEVICH FEDOROV and others posted to the FIN7 "issue" created
23 for Victim-7, information about the victim company's internal network and uploaded
24 exfiltrated data, including stolen employee credentials. Similarly, on or about April 5,
25 2017, DMYTRO VALERIEVICH FEDOROV created an "issue" for another victim
26 company, Victim-9, and uploaded stolen user credentials from the victim company.

27 bb. FIN7 conspirators knew that the scheme would involve the use of
28 wires in both interstate and foreign commerce to accomplish the objectives of the

1 | scheme. For example, the Defendant and his FIN7 co-conspirators knew that execution
2 | of the scheme necessarily caused the transmission of wire communications between the
3 | United States and one or more servers controlled by FIN7 located in foreign countries.

4 | All in violation of Title 18, United States Code, Section 1349.

5 | **COUNTS 2 - 15**

6 | **(Wire Fraud)**

7 | 16. The allegations set forth in Paragraphs 1 through 15 of this Superseding
8 | Indictment are re-alleged and incorporated as if fully set forth herein.

9 | **I. SCHEME AND ARTIFICE TO DEFRAUD**

10 | 17. Beginning at a time unknown, but no later than September 2015, and
11 | continuing through on or after January 17, 2018, at Seattle, within the Western District of
12 | Washington, and elsewhere, DMYTRO VALERIEVICH FEDOROV, and others known
13 | and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to
14 | defraud and to obtain money and property by means of materially false and fraudulent
15 | pretenses, representations and promises.

16 | 18. The essence of the scheme and artifice to defraud was to obtain
17 | unauthorized access into, and control of, the computer networks of victims through deceit
18 | and materially false and fraudulent pretenses and representations, through the installation
19 | and use of malware designed to facilitate, among other things, the installation of
20 | additional malware, the sending and receiving of data, and the surveillance of the
21 | victims' computer networks. The object of the scheme and artifice to defraud was to
22 | steal money and property of value, including payment card data and proprietary and non-
23 | public information, which was, and could have been, sold and used for financial gain.

24 | **II. MANNER AND MEANS OF SCHEME TO DEFRAUD**

25 | 19. The manner and means of the scheme and artifice to defraud are set forth in
26 | Paragraph 15 of Count 1 of this Superseding Indictment.

1 **III. EXECUTION OF SCHEME TO DEFRAUD**

2 20. On or about the dates set forth below, within the Western District of
 3 Washington, and elsewhere, DMYTRO VALERIEVICH FEDOROV, and others known
 4 and unknown to the Grand Jury, having devised a scheme and artifice to defraud, and to
 5 obtain money and property by means of materially false and fraudulent pretenses,
 6 representations, and promises, did knowingly transmit and cause to be transmitted
 7 writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme,
 8 by means of wire communication in interstate and foreign commerce, including the
 9 following transmissions:

10			
11	2	August 8, 2016	Victim-1 Pierce County
12			Email from just_etravel@yahoo.com, which traveled through a server located outside the State of Washington, to a Victim-1 employee, located within the State of Washington
13	3	August 8, 2016	Victim-1 Pierce County
14			Email from frankjohnson@revital- travel.com, which traveled through a server located outside the State of Washington, to a Victim-1 employee, located within the State of Washington
15	4	August 8, 2016	Victim-1 Pierce County
16			Electronic communication between a server located outside the State of Washington, and Victim-1's computer system, located within the State of Washington
17	5	February 21, 2017	Victim-2 Seattle
18			Email purporting to be from a government account, which traveled through a server located outside the State of Washington, to a Victim-2 employee, located within the State of Washington
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			

6	February 23, 2017	Victim-2 Seattle	Electronic communication between a server located outside the State of Washington, and Victim-2's computer system, located within the State of Washington
7	March 24, 2017	Victim-3 4120 196 th St SW, Suite 150, Lynnwood	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
8	March 25, 2017	Victim-3 1415 Broadway, Seattle	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
9	March 25, 2017	Victim-3 800 156 th Ave NE, Bellevue	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
10	March 25, 2017	Victim-3 4 Bellis Fair Pkwy, Bellingham	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
11	March 25, 2017	Victim-3 775 NW Gilman Blvd, Suite A, Issaquah	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
12	March 27, 2017	Victim-3 515 SE Everett Mall Way, Suite B, Everett	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
13	April 11, 2017	Victim-3 22704 SE 4th St, Suite 210, Sammamish	Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington

14	April 11, 2017	Victim-4 Renton	Email from oliver_palmer@yahoo.com, which traveled through a server located outside the State of Washington, to a Victim-4 employee, located within the State of Washington
15	March 10, 2017	Victim-5 Puyallup	Electronic communication between a merchant, located within the State of Washington, and a payment processor server, located outside the State of Washington

All in violation of Title 18, United States Code, Section 1343.

COUNT 16

(Conspiracy to Commit Computer Hacking)

21. The allegations set forth in Paragraphs 1 through 20 of this Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

I. OFFENSE

22. Beginning at a time unknown, but no later than September 2015, and continuing through on or after January 17, 2018, at Seattle, within the Western District of Washington, and elsewhere, DMYTRO VALERIEVICH FEDOROV, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree together to commit offenses against the United States, to wit:

a. to knowingly and with intent to defraud, access a protected computer without authorization and exceed authorized access to a protected computer, and by means of such conduct further the intended fraud and obtain anything of value exceeding \$5,000.00 in any 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A); and

b. 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, and the offense caused loss to one or more persons during a 1-year period aggregating at least \$5,000.00 in value and damage affecting 10 or

1 | more protected computers during a 1-year period, in violation of Title 18, United States
2 | Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

3 | **II. OBJECTIVES OF THE CONSPIRACY**

4 | 23. The objectives of the conspiracy included hacking into protected computer
5 | networks using malware designed to provide the conspirators with unauthorized access
6 | to, and control of, victim computer systems. The objectives of the conspiracy further
7 | included conducting surveillance of victim computer networks and installing additional
8 | malware on the victim computer networks for the purposes of establishing persistence,
9 | and stealing payment card track data, financial information, and proprietary, private, and
10 | non-public information, with the intention of using and selling such stolen items, either
11 | directly or indirectly, for financial gain. The objectives of the conspiracy further
12 | included installing malware that would integrate victim computers into a botnet that
13 | allowed the conspiracy to control, alter, and damage compromised computers.

14 | **III. MANNER AND MEANS OF THE CONSPIRACY**

15 | 24. The manner and means used to accomplish the conspiracy are set forth in
16 | Paragraph 15 of Count 1 of this Superseding Indictment.

17 | **IV. OVERT ACTS**

18 | 25. In furtherance of the conspiracy, and to achieve the objects thereof,
19 | DMYTRO VALERIEVICH FEDOROV, and others known and unknown to the Grand
20 | Jury, did commit and cause to be committed, the following overt acts, among others, in
21 | the Western District of Washington and elsewhere:

22 | a. Co-conspirator F.H. served as a high-level systems administrator for
23 | FIN7 who maintained servers and communication channels used by the organization,
24 | including administrating HipChat rooms and the uploading and organization of stolen
25 | payment card data and malware. For example,

26 | i. On or about March 14, 2016, co-conspirator F.H. uploaded to
27 | a HipChat room shared with another FIN7 member an archive that contained numerous
28 | data files containing payment card numbers stolen from a victim company that had

1 publicly reported a security breach that resulted in the loss of tens of thousands of
2 payment cards.

3 ii. On or about April 8, 2016, co-conspirator F.H. created a
4 HipChat room called "My_Files," to which he had exclusive access, and later uploaded
5 data for approximately 100 stolen payment cards.

6 iii. On or about July 19, 2016, co-conspirator F.H. posted in a
7 HipChat room accessible to other FIN7 members, files related to a victim company,
8 including multiple screenshots from one or more victim company computers that showed,
9 among other things, internal company information and an administrator password.

10 iv. On or about November 22, 2016, co-conspirator F.H.
11 uploaded to his "My_Files" HipChat room a file containing data for stolen payment
12 cards.

13 b. DMYTRO VALERIEVICH FEDOROV served as a high-level "pen-
14 tester" (i.e., one tasked with finding vulnerabilities that an attacker may exploit) who
15 managed other pen-testers responsible for breaching the security of victims' computer
16 systems. For example,

17 i. DMYTRO VALERIEVICH FEDOROV created and
18 managed "issues" on FIN7's private JIRA server relating to intrusions of multiple victim
19 companies, including, but not limited to, Victim-7 and Victim-9, to which FIN7 members
20 shared and stored intrusion information and exfiltrated data.

21 ii. Using FIN7's private Jabber server, DMYTRO
22 VALERIEVICH FEDOROV communicated under the alias "hotdima" with other FIN7
23 members regarding his hacking efforts, and his payment for such efforts.

24 iii. DMYTRO VALERIEVICH FEDOROV accessed and
25 controlled compromised computer systems through custom control panels.

26 c. The conspiracy compromised, illegally accessed, had unauthorized
27 communications with, and exfiltrated proprietary, private, and non-public victim data and
28

1 information from the computer systems of the Victim-1, a hotel and casino in the
2 Western District of Washington. For instance,

3 i. On or about August 8, 2016, the conspiracy, directly and
4 through intermediaries, used the account just_etravel@yahoo.com to send a phishing
5 email, with the subject "order," to an employee of Victim-1 located in Tacoma,
6 Washington, with an attached Microsoft Word document that contained malware. The
7 email contained materially false representations designed to induce the targeted employee
8 to open enable the malware, and compromise the computer system.

9 ii. On or about August 8, 2016, the conspiracy, directly and
10 through intermediaries, used the account frankjohnson@revital-travel.com to send a
11 phishing email, with the subject "order," to an employee of Victim-1 located in Tacoma,
12 Washington, with an attached Microsoft Word document that contained malware. The
13 email contained materially false representations designed to induce the targeted employee
14 to enable the malware, and compromise the computer system.

15 iii. Under the control of the conspiracy's malware, a
16 compromised computer of Victim-1 communicated with a command and control server
17 located in a foreign country. For instance, from August 8, 2016, to August 9, 2016, and
18 from August 24, 2016 to August 31, 2016, a compromised Victim-1 computer logged
19 approximately 3,639 communications with various URLs all starting with "revital-
20 travel.com" at an IP address hosted in Russia.

21 d. The conspiracy compromised, illegally accessed, had unauthorized
22 communications with, and exfiltrated proprietary, private, and non-public victim data and
23 information from the computer systems of Victim-6, a restaurant chain with locations in
24 multiple states. For instance,

25 i. On or about August 25, 2016, the conspiracy, directly and
26 through intermediaries, used the account revital.travel@yahoo.com to send a phishing
27 email to an employee of Victim-6, with an attached Microsoft Word document that
28 contained malware. The email contained materially false representations designed to

1 induce the targeted employee to enable the malware, and compromise the computer
2 system.

3 ii. On or about September 7, 2016, co-conspirator F.H. created
4 an "issue" on the conspiracy's private JIRA server specifically related to Victim-6. One
5 or more FIN7 members posted files containing internal credentials for the Victim-6
6 computer network.

7 e. The conspiracy compromised, illegally accessed, had unauthorized
8 communications with, and exfiltrated proprietary, private, and non-public victim data and
9 information from the computer systems of Victim-7, an automotive retail and repair chain
10 with hundreds of locations in multiple states, including Washington. For instance,

11 i. On or about January 18, 2017, a FIN7 member created an
12 "issue" on the conspiracy's private JIRA server specifically related to Victim-7. That
13 FIN7 member and DMYTRO VALERIEVICH FEDOROV posted results from several
14 network mapping tools used on Victim-7's internal network.

15 ii. On or about January 20, 2017, a FIN7 member posted
16 exfiltrated data, including multiple usernames and passwords with the title "Server
17 Passwords," to the Victim-7 JIRA "issue."

18 iii. On or about January 23, and January 24, 2017, DMYTRO
19 VALERIEVICH FEDOROV posted information about Victim-7's internal network and
20 uploaded a file containing multiple IP addresses and information about Victim-7's
21 servers to the Victim-7 JIRA "issue."

22 iv. On or about January 27, 2017, DMYTRO VALERIEVICH
23 FEDOROV uploaded to the Victim-7 JIRA "issue" a file containing over 1,000
24 usernames and passwords for generic company accounts and employee accounts. The
25 potentially compromised accounts related to approximately 700 Victim-7 locations
26 throughout the United States, including approximately 12 locations located in the state of
27 Washington.

28

1 f. The conspiracy compromised, illegally accessed, had unauthorized
2 communications with, and exfiltrated proprietary, private, and non-public victim data and
3 information from the computer systems of Victim-2, a corporation headquartered in
4 Seattle, Washington. For instance,

5 i. On or about February 21, 2017, the conspiracy, directly and
6 through intermediaries, used an account purporting to be filings@sec.gov (but actually
7 sent by secureserver.net) to send a phishing email to an employee of Victim-2 located in
8 Seattle, Washington, with an attached Microsoft Word document that contained malware.
9 The email falsely purported to relate to a corporate filing with the SEC and contained
10 materially false representations designed to induce the targeted employee to open the file,
11 enable the malware, and compromise the computer system.

12 ii. From on or about February 21, 2017, to approximately
13 March 3, 2017, the conspiracy illegally accessed and had communications with the
14 computer systems of Victim-2 located in Seattle, Washington. For instance, between
15 about February 23, 2017, and February 24, 2017, the victim computer made outgoing
16 connections to and transferred internal data, without authorization, to an IP address
17 located in a foreign country.

18 iii. On or about February 24, 2017, a FIN7 member posted to a
19 JIRA "issue" created for Victim-2, a screenshot from the targeted employee's computer
20 at Victim-2, which showed, among other things, an internal Victim-2 webpage available
21 only to employees with a valid user account.

22 iv. Similarly, a FIN7 member posted to the Victim-2 JIRA
23 "issue" a text file containing the usernames and passwords of the targeted Victim-2
24 employee, including his/her personal email account, LinkedIn account, and personal
25 investment and financial institution accounts.

26 g. The conspiracy compromised, illegally accessed, had unauthorized
27 communications with, and exfiltrated proprietary, private, and non-public victim data and
28 information from the computer systems of Victim-3, a restaurant chain with thousands of

1 | locations, including the State of Washington. From approximately March 24, 2017 to
2 | April 18, 2017, the conspiracy accessed computer systems of Victim-3 and implanted
3 | malware designed to harvest payment card data from cards used on point-of-sale devices
4 | at restaurant locations nationwide, including approximately 33 locations within the
5 | Western District of Washington.

6 | h. The conspiracy compromised, illegally accessed, had unauthorized
7 | communications with, and exfiltrated proprietary, private, and non-public victim data and
8 | information from the computer systems of Victim-8, a restaurant chain with hundreds of
9 | locations in multiple states, including Washington. For instance,

10 | i. On or about March 27, 2017, the conspiracy, directly and
11 | through intermediaries, used the account ray.donovan84@yahoo.com, to send a phishing
12 | email to a Victim-8 employee, with an attached Microsoft Word document that contained
13 | malware. The email falsely purported to convey a customer complaint and contained
14 | additional materially false representations designed to induce the targeted employee to
15 | enable the malware, and compromise the computer system.

16 | ii. On or about March 29, 2017, a FIN7 member created an
17 | “issue” on the conspiracy’s private JIRA server specifically related to Victim-8 and
18 | posted results from several network mapping tools used on Victim-8’s internal network.

19 | iii. On or about March 31, 2017, a FIN7 member posted a link to
20 | the point-of-sale software management solution used by Victim-8, and a username and
21 | password to the Victim-8 JIRA “issue.” The software management tool allows a
22 | company to manage point-of-sale systems at multiple locations. The FIN7 member also
23 | uploaded several screenshots presumably from one or more victim computers at Victim-
24 | 8, which showed, among other things, the user logged into Victim-8’s account for the
25 | software management tool.

26 | iv. On or about April 6, 2017, a FIN7 member uploaded to the
27 | Victim-8 JIRA “issue” a file containing hundreds of usernames and passwords for
28 | approximately 798 Victim-8 locations, including 37 locations located in the State of

1 | Washington. The file included network information, telephone communications, and
2 | locations of alarm panels within restaurants.

3 | v. On or about April 7, 2017, a FIN7 member uploaded to the
4 | Victim-8 JIRA "issue" a similar file containing numerous usernames and passwords for
5 | Victim-8 locations.

6 | vi. On or about May 5, 2017, a FIN7 member uploaded to the
7 | Victim-8 JIRA "issue" a file containing file directories on a compromised computer.

8 | vii. On or about May 8, 2017, a FIN7 member uploaded to the
9 | Victim-8 JIRA "issue" exfiltrated files related to a password management system from a
10 | compromised computer, which contained the credentials, usernames, and passwords of a
11 | particular employee.

12 | viii. On or about May 15, 2017, a FIN7 member uploaded to the
13 | Victim-8 JIRA "issue" screenshots of a compromised computer that showed the
14 | employee accessing Victim-8's security infrastructure management software using that
15 | same employee's credentials.

16 | i. The conspiracy compromised, illegally accessed, had unauthorized
17 | communications with, and exfiltrated proprietary, private, and non-public victim data and
18 | information from the computer systems of one or more locations of Victim-9, a fast-food
19 | restaurant chain with thousands of locations throughout the United States, including
20 | Washington. For instance,

21 | i. On various dates, the conspiracy, directly and through
22 | intermediaries, sent phishing emails with an attached file that contained malware to
23 | multiple Victim-9 locations. For instance, on or about April 7, 2017, the conspiracy used
24 | the account oliver_palmer@yahoo.com to send a phishing email to a Victim-9 location in
25 | the State of Oregon. The email contained materially false representations designed to
26 | induce the targeted employee to open the file, enable the malware, and compromise the
27 | computer system.

1 ii. On or about April 5, 2017, DMYTRO VALERIEVICH
2 FEDOROV created an “issue” on the conspiracy’s private JIRA server specifically
3 related to Victim-9. One or more FIN7 members posted usernames and passwords for
4 Victim-9 locations, including a Victim-9 location in Vancouver, Washington.

5 j. The conspiracy compromised, illegally accessed, had unauthorized
6 communications with, and exfiltrated proprietary, private, and non-public victim data and
7 information from the computer systems of one or more locations of Victim-4, a pizza
8 parlor chain with hundreds of locations, including in Washington. For instance,

9 i. On or about April 11, 2017, the conspiracy, directly and
10 through intermediaries, used the account oliver_palmer@yahoo.com, to send a phishing
11 email, with the subject “claim,” to an employee of a Victim-4 located in Renton,
12 Washington, with an attached Rich Text Format (.rtf) document that contained malware.
13 The email falsely purported to convey a customer complaint and contained additional
14 materially false representations designed to induce the targeted employee to enable the
15 malware, and compromise the computer system.

16 ii. On or about April 11, 2017, the conspiracy, directly and
17 through intermediaries, used the account oliver_palmer@yahoo.com, to send a phishing
18 email, with the subject “claim,” to an employee of a Victim-4 located in Vancouver,
19 Washington, with an attached Rich Text Format (.rtf) document that contained malware.
20 The email falsely purported to convey a customer complaint and contained additional
21 materially false representations designed to induce the targeted employee to enable the
22 malware, and compromise the computer system.

23 iii. On or about May 25, 2017, the conspiracy, directly and
24 through intermediaries, used the account Adrian.1987clark@yahoo.com, to send a
25 phishing email, with the subject “takeout order,” to an employee of a Victim-4 located in
26 or around Spokane, Washington, with an attached Rich Text Format (.rtf) document that
27 contained malware. The email falsely stated that the sender had a large takeout order and
28

1 | contained additional materially false representations designed to induce the targeted
2 | employee to enable the malware, and compromise the computer system.

3 | k. The conspiracy compromised, illegally accessed, had unauthorized
4 | communications with, and exfiltrated proprietary, private, and non-public victim data and
5 | information from the computer systems of one or more locations of Victim-10, a fast-
6 | food restaurant chain with hundreds of locations in various states, including Washington.
7 | For instance,

8 | i. On or about May 24, 2017, a FIN7 member created an “issue”
9 | on the conspiracy’s private JIRA server specifically related to Victim-10. One or more
10 | FIN7 members posted information relating to the intrusion of computer systems and
11 | exfiltrated data, including files containing passwords and screenshots from one or more
12 | compromised computers.

13 | ii. On or about June 12, 2017, the conspiracy, directly and
14 | through intermediaries, used the account Adrian.1987clark@yahoo.com, to send a
15 | phishing email, with the subject “order.catering,” to an employee of a Victim-10 located
16 | in Iowa, with an attached Rich Text Format (.rtf) document that contained malware. The
17 | email falsely stated that the sender had a catering order for the following day and
18 | contained additional materially false representations designed to induce the employee to
19 | enable the malware, and compromise the computer system.

20 | iii. From on or about June 12, 2017, to a date unknown, the
21 | conspiracy illegally accessed and had communications with the computer systems of the
22 | Victim-10 located in Iowa. For instance, the conspiracy transferred, without
23 | authorization, the proprietary, private, and non-public victim data and information,
24 | including usernames and passwords, to a JIRA server managed by FIN7, located in a
25 | foreign country.

26 | All in violation of Title 18, United States Code, Section 371.
27 |
28 |

COUNTS 17 - 19**(Accessing a Protected Computer in Furtherance of Fraud)**

26. The allegations set forth in Paragraphs 1 through 25 of this Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

27. On or about the dates listed below, within the Western District of Washington, and elsewhere, DMYTRO VALERIEVICH FEDOROV, and others known and unknown to the Grand Jury, knowingly and with intent to defraud accessed a protected computer without authorization and in excess of authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, specifically, payment card data and proprietary and non-public information, whereby the object of the fraud and the thing obtained consisted of more than the use of the computers and the value of such use was more than \$5,000 in a 1-year period, as listed below:

17	August 8, 2016 through October 4, 2016	Victim-1
18	February 21, 2017 through March 3, 2017	Victim-2
19	March 24, 2017 through April 18, 2017	Victim-3

All in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A) and 2.

COUNTS 20 - 22**(Intentional Damage to a Protected Computer)**

28. The allegations set forth in Paragraphs 1 through 27 of this Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

29. On or about the dates listed below, within the Western District of Washington, and elsewhere, DMYTRO VALERIEVICH FEDOROV, and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, specifically, the protected computer system of the victim listed below, and the offense caused (i) loss to one or more

1 persons during a 1-year period aggregating at least \$5,000.00 in value and (ii) damage
 2 affecting 10 or more protected computers during a 1-year period:

3	20	August 8, 2016 through October 4, 2016	Victim-1
4	21	February 21, 2017 through March 3, 2017	Victim-2
5	22	March 24, 2017 through April 18, 2017	Victim-3

6 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b),
 7 1030(c)(4)(B), and 2.

8 COUNT 23

9 (Access Device Fraud)

10 30. The allegations set forth in Paragraphs 1 through 29 of this Superseding
 11 Indictment are re-alleged and incorporated as if fully set forth herein.

12 31. Beginning at a time unknown, and continuing through on or after
 13 January 17, 2018, within the Western District of Washington, and elsewhere, DMYTRO
 14 VALERIEVICH FEDOROV, and others known and unknown to the Grand Jury,
 15 knowingly and with intent to defraud, possessed fifteen or more counterfeit and
 16 unauthorized access devices, namely, payment card data, account numbers, and other
 17 means of account access that can be used, alone and in conjunction with another access
 18 device, to obtain money, goods, services, and any other thing of value, and that can be
 19 used to initiate a transfer of funds; said activity affecting interstate and foreign commerce

20 All in violation of Title 18, United States Code, Sections 1029(a)(3), 1029(b)(1),
 21 1029(c)(1)(A), and 2.

22 COUNT 24

23 (Aggravated Identity Theft)

24 32. The allegations set forth in Paragraphs 1 through 31 of this Superseding
 25 Indictment are re-alleged and incorporated as if fully set forth herein.

26 33. Beginning at a time unknown, but no earlier than on or about February 21,
 27 2017, and no later than March 3, 2017, and continuing through on or after November 21,
 28 2017, at Seattle, within the Western District of Washington, and elsewhere, DMYTRO

1 VALERIEVICH FEDOROV, and others known and unknown to the Grand Jury, did
2 knowingly transfer, possess, and use, without lawful authority, a means of identification
3 of another person, to wit: the name, username, and password of a real person, J.Q., an
4 employee of Victim-2, during and in relation to a felony violation enumerated in 18
5 U.S.C. § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18
6 U.S.C. § 1349, as charged in Count 1, and wire fraud, in violation of 18 U.S.C. § 1343, as
7 charged in Counts 5 and 6, knowing that the means of identification belonged to another
8 actual person.

9 All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

10 **COUNT 25**

11 **(Aggravated Identity Theft)**

12 34. The allegations set forth in Paragraphs 1 through 33 of this Superseding
13 Indictment are re-alleged and incorporated as if fully set forth herein.

14 35. Beginning at a time unknown, but no later than on or about May 8, 2017,
15 and continuing through on or after November 21, 2017, within the Western District of
16 Washington, and elsewhere, DMYTRO VALERIEVICH FEDOROV, and others known
17 and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful
18 authority, a means of identification of another person, to wit: the name, employee
19 credentials, username, and password of a real person, N.M., an employee of Victim-8,
20 during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is,
21 conspiracy to commit wire and bank fraud, in violation of 18 U.S.C. § 1349, as charged
22 in Count 1, knowing that the means of identification belonged to another actual person.

23 All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

24 **COUNT 26**

25 **(Aggravated Identity Theft)**

26 36. The allegations set forth in Paragraphs 1 through 35 of this Superseding
27 Indictment are re-alleged and incorporated as if fully set forth herein.

1 such offenses, including but not limited to a judgment for a sum of money representing
2 the property described in this paragraph.

3 40. The allegations contained in Count 23 of this Superseding Indictment are
4 hereby realleged and incorporated by reference for the purpose of alleging forfeitures
5 pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 1029(c)(1)(C), and
6 Title 28, United States Code, Section 2461(c). Upon conviction of the offense charged in
7 Count 23, the defendant, DMYTRO VALERIEVICH FEDOROV, shall forfeit to the
8 United States any property, real or personal, which constitutes or is derived from
9 proceeds traceable to such offense, and shall also forfeit any personal property used or
10 intended to be used to commit such offense, including but not limited to a judgment for a
11 sum of money representing the property described in this paragraph.

12 (Substitute Assets)

13 41. If any of the property described above, as a result of any act or omission of
14 the defendant:

- 15 a. cannot be located upon the exercise of due diligence;
- 16 b. has been transferred or sold to, or deposited with, a third party;
- 17 c. has been placed beyond the jurisdiction of the court;
- 18 d. has been substantially diminished in value; or
- 19 e. has been commingled with other property which cannot be divided
20 without difficulty,

21 //

22 //

1 the United States of America shall be entitled to forfeiture of substitute property pursuant
2 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
3 Code, Section 2461(c).


4 A TRUE BILL:

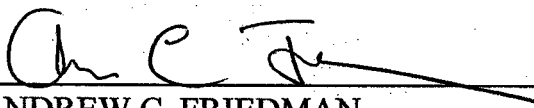
5 DATED:

1.25.18

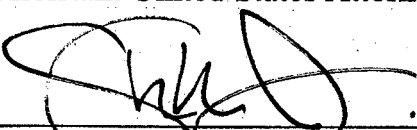
6
7 (Signature of Foreperson redacted pursuant to
8 policy of the Judicial Conference)

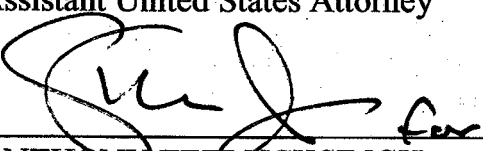
9 FOREPERSON

10 
11 ANNETTE L. HAYES
12 United States Attorney

13 
14 ANDREW C. FRIEDMAN
15 Assistant United States Attorney

16 
17 FRANCIS FRANZE-NAKAMURA
18 Assistant United States Attorney

19 
20 STEVEN MASADA
21 Assistant United States Attorney

22 
23 ANTHONY TEELUCKSINGH
24 Trial Attorney
25 Computer Crime and Intellectual Property Section
26
27
28