

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 *[Signature]* Deputy

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

UNITED STATES OF AMERICA,
Plaintiff,

NO. CR17-276RSL

SUPERSEDING INDICTMENT

v.

FEDIR OLEKSIYOVYCH HLADYR,
aka "Fedor Gladyr,"
aka "Fedir Oleksiyovych Gladyr,"
aka "Gladyr Fedir Oleksiyovych,"
aka "Gladyr Fedor Oleksiyovich,"
aka "Fedor,"
aka "das,"
aka "Fyodor,"
aka "AronaXus,"

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

1 from its source to its destination. Most Internet service providers control a range of IP
2 addresses.

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

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

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

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

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

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

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

26 | **8. Spear Phishing:** Spear phishing is a targeted form of phishing directed
27 | towards a specific individual, organization or business. Although often intended to steal
28 |

1 data for malicious purposes, cybercriminals may also use spear phishing schemes to
2 install malware on a targeted user's computer.

3 **9. Social Engineering:** Social engineering is a skill developed over time by
4 people who seek to acquire protected information through manipulation of social
5 relationships. People who are skilled in social engineering can convince key individuals
6 to divulge protected information or access credentials that the social engineer deems
7 valuable to the achievement of his or her aims.

8 **10. Pen-Testing:** Penetration testing, or pen-testing, is the practice of testing a
9 computer system, network or computer application to find vulnerabilities that an attacker
10 may exploit.

11 **COUNT 1**

12 **(Conspiracy to Commit Wire and Bank Fraud)**

13 **I. OFFENSE**

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

16 **12.** Beginning at a time unknown, but no later than September 2015, and
17 continuing through on or after January 10, 2018, at Seattle, within the Western District of
18 Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, aka "Fedor Gladyr,"
19 aka "Fedir Oleksiyovych Gladyr," "Gladyr Fedir Oleksiyovych," aka "Gladyr Fedor
20 Oleksiyovich," aka "Fedor," aka "das," aka "Fyodor," aka "AronaXus," and others
21 known and unknown to the Grand Jury, did knowingly and willfully combine, conspire,
22 confederate and agree together to commit offenses against the United States, to wit:

23 a. to knowingly and willfully devise and execute and attempt to
24 execute, a scheme and artifice to defraud, and for obtaining money and property by
25 means of materially false and fraudulent pretenses, representations, and promises; and in
26 executing and attempting to execute this scheme and artifice, to knowingly cause to be
27 transmitted in interstate and foreign commerce, by means of wire communication, certain
28

1 signs, signals and sounds as further described below, in violation of Title 18, United
2 States Code, Section 1343;

3 b. to knowingly and willfully devise and execute and attempt to
4 execute, a scheme and artifice to defraud financial institutions, as defined by Title 18,
5 United States Code, Section 20, and to obtain moneys, funds, and credits under the
6 custody and control of the financial institutions by means of materially false and
7 fraudulent pretenses, representations, and promises, in violation of Title 18, United States
8 Code, Section 1344(1) and (2).

9 II. OBJECTIVES OF THE CONSPIRACY

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

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

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

2 15. The manner and means used to accomplish the conspiracy included the
3 following:

4 a. FIN7 developed and employed various malware designed to
5 infiltrate, compromise, and gain control of the computer systems of victim companies
6 operating in the United States and elsewhere, including within the Western District of
7 Washington. FIN7 established and operated an infrastructure of servers, located in
8 various countries, through which FIN7 members coordinated activity to further the
9 scheme. This infrastructure included, but was not limited to, the use of command and
10 control servers, accessed through custom botnet control panels, that communicated with
11 and controlled compromised computer systems of victim companies.

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

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

25 d. FIN7 targeted victims in the Western District of Washington, and
26 elsewhere, using phishing techniques to distribute malware designed to gain unauthorized
27 access to, take control of, and exfiltrate data from the computer systems of various
28 businesses. FIN7's targeted victims include more than 120 identified companies, with

1 thousands of individual locations of operation throughout the United States, including,
2 but not limited to, the following representative victim companies:

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

7 ii. "Victim-2" referenced herein is [REDACTED], a
8 public corporation headquartered in Seattle, within the Western District of Washington,
9 with operations throughout the United States and elsewhere.

10 iii. "Victim-3" referenced herein is Chipotle Mexican Grill, a
11 U.S.-based restaurant chain with thousands of locations in the United States, including in
12 the Western District of Washington, and in Canada and multiple European countries.

13 iv. "Victim-4" referenced herein is [REDACTED], a U.S.-
14 based pizza parlor chain with hundreds of locations predominantly in the Western United
15 States, including in the Western District of Washington.

16 v. "Victim-5" referenced herein is BECU, a U.S.-based
17 federally insured credit union headquartered in the Western District of Washington.

18 vi. "Victim-6" referenced herein is Jason's Deli, a U.S.-based
19 casual delicatessen restaurant chain with hundreds of locations in the United States.

20 vii. "Victim-7" referenced herein is [REDACTED], an automotive
21 retail and repair chain with hundreds of locations in the United States, including in the
22 Western District of Washington.

23 viii. "Victim-8" referenced herein is Red Robin Gourmet Burgers
24 and Brews (Red Robin), a U.S.-based casual dining restaurant chain, founded in the
25 Western District of Washington, with hundreds of locations in the United States,
26 including in the Western District of Washington.

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

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

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

23 f. In certain phishing attacks, FIN7, directly and through
24 intermediaries, sent phishing emails to personnel at victim companies who had unique
25 access to internal proprietary and non-public company information, including, but not
26 limited to, employees involved with making filings with the United States Securities and
27 Exchange Commission (“SEC”). These emails used an email address that spoofed an
28

1 | email address associated with the SEC's electronic filing system, and induced the
2 | recipients to activate the malware contained in the emails' attachments.

3 | g. In many of the FIN7 attacks, a FIN7 member, or someone hired by
4 | FIN7 specifically for such purpose, would also call the victim company, using wires in
5 | interstate or foreign commerce, to legitimize the phishing email and convince the victim
6 | company employee to open the attached document using social engineering techniques.
7 | For example, when targeting a hotel chain or a restaurant chain, a conspirator would
8 | make a follow-up call falsely claiming that the details of a reservation request, catering
9 | order, or customer complaint could be found in the file attached to the previously
10 | delivered email, to induce the employee at the victim company to read the phishing
11 | email, open the attached file, and activate the malware.

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

19 | i. FIN7 typically would install additional malware, including the
20 | Carbanak malware, to connect to additional FIN7 command and control servers to
21 | establish remote control of the victim computer.

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

24 | k. FIN7 designed and used a custom botnet control panel to manage
25 | and issue commands to the compromised machines.

26 | l. Once a victim company's computers were incorporated into the
27 | FIN7 botnet and remotely controlled by FIN7's malware, the group used this remote
28 | control and access to, among other things, install and manage additional malware,

1 conduct surveillance, map and navigate the compromised computer network, compromise
2 additional computers, exfiltrate files, and send and receive data. For instance, FIN7 often
3 conducted surveillance on the victim's computer network by, among other things,
4 capturing screen shots and videos of victim computer workstations that provided the
5 conspirators with additional information about the victim company computer network
6 and non-public credentials for both generic company accounts and for actual company
7 employees.

8 m. FIN7 used its access to the victim's computer network and
9 information gleaned from surveillance of the victim's computer systems to install
10 additional malware designed to target and extract particular information and property of
11 value, including payment card data and proprietary and non-public information. For
12 instance, FIN7 often utilized various "off-the-shelf" software and custom malware, and a
13 combination thereof, to extract and transfer data to a "loot" folder on one or more servers
14 controlled by FIN7.

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

20 o. For example, between approximately March 24, 2017, and April 18,
21 2017, FIN7 harvested payment card data from point-of-sale devices at certain Victim-3
22 restaurant locations, including dozens of locations in the Western District of Washington.

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

26 q. The payment card data were offered for sale to allow purchasers to
27 falsely represent themselves as authorized users of the stolen payment cards and to use
28 the stolen payment card information to purchase goods and services in fraudulent

1 transactions throughout the United States and the world, including over the Internet,
2 resulting in millions of dollars in losses to, and thereby affecting, merchants and banks,
3 including financial institutions, as defined in Title 18, United States Code, Section 20.
4 For example, on or about March 10, 2017, stolen payment card data related to accounts
5 held at Victim-5, a financial institution headquartered in the Western District of
6 Washington, compromised through the computer network intrusion of a victim company,
7 was used to make unauthorized purchases at a merchant in Puyallup, Washington.

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

11 s. FEDIR OLEKSIYOVYCH HLADYR served as a high-level
12 systems administrator for FIN7 who maintained servers and communication channels
13 used by the organization. For example, FIN7 members requested FEDIR
14 OLEKSIYOVYCH HLADYR to grant them access to servers used by FIN7 to facilitate
15 the malware scheme. FEDIR OLEKSIYOVYCH HLADYR also played a management
16 role in the scheme by delegating tasks and by providing instruction to other members of
17 the scheme.

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

23 u. For example, in Jabber communications with other FIN7 members, a
24 co-conspirator, D.F., using his alias "hotdima," referenced using malware in connection
25 with several specific victim companies, discussed using the administrative control panels
26 to receive data from compromised computers, and identified several pen-testers working
27 at his direction.

1 v. FIN7 members often communicated through a private HipChat
2 server. HipChat is a group chat, instant messaging, and file-sharing program. FIN7
3 members used its HipChat server to collaborate on malware and victim business
4 intrusions, to interview potential recruits, and to upload and share exfiltrated data, such as
5 stolen payment card data. As a system administrator, FEDIR OLEKSIYOVYCH
6 HLADYR created HipChat user accounts for FIN7 members that allowed them to access
7 the server.

8 w. FEDIR OLEKSIYOVYCH HLADYR also created and participated
9 in multiple HipChat “rooms” with other FIN7 members and participated in the uploading
10 and organization of stolen payment card data and malware. For example, on or about
11 March 14, 2016, FEDIR OLEKSIYOVYCH HLADYR uploaded an archive that
12 contained numerous data files created by malware designed to steal data from point-of-
13 sale systems that process payment cards. The files contained payment card numbers
14 stolen from a victim company that had publicly reported a security breach that resulted in
15 the compromise of tens of thousands of payment cards. By way of further example,
16 FEDIR OLEKSIYOVYCH HLADYR also set up and used a HipChat room titled
17 “MyFile”, in which he was the only participant, and to which he uploaded malware used
18 by FIN7 and stolen payment card information.

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

22 y. FIN7 conspirators frequently used the project management software
23 JIRA, hosted on private virtual servers in various countries, to coordinate their malicious
24 activity and to manage the assorted network intrusions. FIN7 members typically created
25 a “project” and then associated “issues” with the project, each issue akin to an issue
26 directory or folder, for a victim company, which they used to collaborate and share
27 details of the intrusion, to post victim company intelligence, such as network mapping
28 information, and to store and share exfiltrated data.

1 z. For example, on about September 7, 2016, FEDIR
2 OLEKSIYOVYCH HLADYR created an "issue" for Victim-6, to which FIN7
3 conspirators posted files containing internal credentials for the victim company's
4 computer network.

5 aa. By way of further example, on multiple occasions in January 2017,
6 co-conspirator D.F. and others posted to the FIN7 "issue" created for Victim-7,
7 information about the victim company's internal network and uploaded exfiltrated data,
8 including stolen employee credentials. Similarly, on or about April 5, 2017, co-
9 conspirator D.F. created an "issue" for another victim company, Victim-9, and uploaded
10 stolen user credentials from the victim company.

11 bb. FIN7 conspirators knew that the scheme would involve the use of
12 wires in both interstate and foreign commerce to accomplish the objectives of the
13 scheme. For example, the Defendant and his FIN7 co-conspirators knew that execution
14 of the scheme necessarily caused the transmission of wire communications between the
15 United States and one or more servers controlled by FIN7 located in foreign countries.

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

17 **COUNTS 2 - 15**

18 **(Wire Fraud)**

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

21 **I. SCHEME AND ARTIFICE TO DEFRAUD**

22 17. Beginning at a time unknown, but no later than September 2015, and
23 continuing through on or after January 10, 2018, at Seattle, within the Western District of
24 Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, and others known
25 and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to
26 defraud and to obtain money and property by means of materially false and fraudulent
27 pretenses, representations and promises.

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

9 **II. MANNER AND MEANS OF SCHEME TO DEFRAUD**

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

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

13 20. On or about the dates set forth below, within the Western District of
 14 Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, and others known
 15 and unknown to the Grand Jury, having devised a scheme and artifice to defraud, and to
 16 obtain money and property by means of materially false and fraudulent pretenses,
 17 representations, and promises, did knowingly transmit and cause to be transmitted
 18 writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme,
 19 by means of wire communication in interstate and foreign commerce, including the
 20 following transmissions:

Count	Date	Victim	Description
2	August 8, 2016	Victim-1 Pierce County	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

1			
2			
3	3	August 8, 2016	Victim-1 Pierce County
4			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
5			
6	4	August 8, 2016	Victim-1 Pierce County
7			Electronic communication between a server located outside the State of Washington, and Victim-1's computer system, located within the State of Washington
8			
9	5	February 21, 2017	Victim-2 Seattle
10			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
11			
12	6	February 23, 2017	Victim-2 Seattle
13			Electronic communication between a server located outside the State of Washington, and Victim-2's computer system, located within the State of Washington
14			
15	7	March 24, 2017	Victim-3 4120 196 th St SW, Suite 150, Lynnwood
16			Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
17			
18	8	March 25, 2017	Victim-3 1415 Broadway, Seattle
19			Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
20			
21	9	March 25, 2017	Victim-3 800 156 th Ave NE, Bellevue
22			Electronic communication between a server, located outside the State of Washington, and Victim-3's computer system, located within the State of Washington
23			
24			
25			
26			
27			
28			

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 10, 2018, at Seattle, within the Western District of Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, 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 more protected computers during a 1-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

II. OBJECTIVES OF THE CONSPIRACY

23. The objectives of the conspiracy included hacking into protected computer networks using malware designed to provide the conspirators with unauthorized access to, and control of, victim computer systems. The objectives of the conspiracy further included conducting surveillance of victim computer networks and installing additional malware on the victim computer networks for the purposes of establishing persistence, and stealing payment card track data, financial information, and proprietary, private, and

1 non-public information, with the intention of using and selling such stolen items, either
2 directly or indirectly, for financial gain. The objectives of the conspiracy further
3 included installing malware that would integrate victim computers into a botnet that
4 allowed the conspiracy to control, alter, and damage compromised computers.

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

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

8 **IV. OVERT ACTS**

9 25. In furtherance of the conspiracy, and to achieve the objects thereof, FEDIR
10 OLEKSIYOVYCH HLADYR, and others known and unknown to the Grand Jury, did
11 commit and cause to be committed, the following overt acts, among others, in the
12 Western District of Washington and elsewhere:

13 a. FEDIR OLEKSIYOVYCH HLADYR served as a high-level
14 systems administrator for FIN7 who maintained servers and communication channels
15 used by the organization, including administrating HipChat rooms and the uploading and
16 organization of stolen payment card data and malware. For example,

17 i. On or about March 14, 2016, FEDIR OLEKSIYOVYCH
18 HLADYR uploaded to a HipChat room shared with another FIN7 member an archive that
19 contained numerous data files containing payment card numbers stolen from a victim
20 company that had publicly reported a security breach that resulted in the loss of tens of
21 thousands of payment cards.

22 ii. On or about April 8, 2016, FEDIR OLEKSIYOVYCH
23 HLADYR created a HipChat room called "My_Files," to which he had exclusive access,
24 and later uploaded data for approximately 100 stolen payment cards.

25 iii. On or about July 19, 2016, FEDIR OLEKSIYOVYCH
26 HLADYR posted in a HipChat room accessible to other FIN7 members, files related to a
27 victim company, including multiple screenshots from one or more victim company
28

1 computers that showed, among other things, internal company information and an
2 administrator password.

3 iv. On or about November 22, 2016, FEDIR OLEKSIYOVYCH
4 HLADYR uploaded to his "My_Files" HipChat room a file containing data for stolen
5 payment cards.

6 b. Co-conspirator D.F. served as a high-level "pen-tester" (i.e., one
7 tasked with finding vulnerabilities that an attacker may exploit) who managed other pen-
8 testers responsible for breaching the security of victims' computer systems. For example,

9 i. Co-conspirator D.F. created and managed "issues" on FIN7's
10 private JIRA server relating to intrusions of multiple victim companies, including, but not
11 limited to, Victim-7 and Victim-9, to which FIN7 members shared and stored intrusion
12 information and exfiltrated data.

13 ii. Using FIN7's private Jabber server, co-conspirator D.F.,
14 communicated under the alias "hotdima" with other FIN7 members regarding his hacking
15 efforts, and his payment for such efforts.

16 iii. Co-conspirator D.F. accessed and controlled compromised
17 computer systems through custom control panels.

18 c. The conspiracy compromised, illegally accessed, had unauthorized
19 communications with, and exfiltrated proprietary, private, and non-public victim data and
20 information from the computer systems of the Victim-1, a hotel and casino in the
21 Western District of Washington. For instance,

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

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

7 iii. Under the control of the conspiracy’s malware, a
8 compromised computer of Victim-1 communicated with a command and control server
9 located in a foreign country. For instance, from August 8, 2016, to August 9, 2016, and
10 from August 24, 2016 to August 31, 2016, a compromised Victim-1 computer logged
11 approximately 3,639 communications with various URLs all starting with “revital-
12 travel.com” at an IP address hosted in Russia.

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

17 i. On or about August 25, 2016, the conspiracy, directly and
18 through intermediaries, used the account revital.travel@yahoo.com to send a phishing
19 email to an employee of Victim-6, with an attached Microsoft Word document that
20 contained malware. The email contained materially false representations designed to
21 induce the targeted employee to enable the malware, and compromise the computer
22 system.

23 ii. On or about September 7, 2016, FEDIR OLEKSIYOVYCH
24 HLADYR created an “issue” on the conspiracy’s private JIRA server specifically related
25 to Victim-6. One or more FIN7 members posted files containing internal credentials for
26 the Victim-6 computer network.

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

1 information from the computer systems of Victim-7, an automotive retail and repair chain
2 with hundreds of locations in multiple states, including Washington. For instance,

3 i. On or about January 18, 2017, a FIN7 member created an
4 “issue” on the conspiracy’s private JIRA server specifically related to Victim-7. That
5 FIN7 member and co-conspirator D.F. posted results from several network mapping tools
6 used on Victim-7’s internal network.

7 ii. On or about January 20, 2017, a FIN7 member posted
8 exfiltrated data, including multiple usernames and passwords with the title “Server
9 Passwords,” to the Victim-7 JIRA “issue.”

10 iii. On or about January 23, and January 24, 2017, co-conspirator
11 D.F. posted information about Victim-7’s internal network and uploaded a file containing
12 multiple IP addresses and information about Victim-7’s servers to the Victim-7 JIRA
13 “issue.”

14 iv. On or about January 27, 2017, co-conspirator D.F. uploaded
15 to the Victim-7 JIRA “issue” a file containing over 1,000 usernames and passwords for
16 generic company accounts and employee accounts. The potentially compromised
17 accounts related to approximately 700 Victim-7 locations throughout the United States,
18 including approximately 12 locations located in the state of Washington.

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

23 i. On or about February 21, 2017, the conspiracy, directly and
24 through intermediaries, used an account purporting to be filings@sec.gov (but actually
25 sent by secureserver.net) to send a phishing email to an employee of Victim-2 located in
26 Seattle, Washington, with an attached Microsoft Word document that contained malware.
27 The email falsely purported to relate to a corporate filing with the SEC and contained
28

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

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

9 | iii. On or about February 24, 2017, a FIN7 member posted to a
10 | JIRA “issue” created for Victim-2, a screenshot from the targeted employee’s computer
11 | at Victim-2, which showed, among other things, an internal Victim-2 webpage available
12 | only to employees with a valid user account.

13 | iv. Similarly, a FIN7 member posted to the Victim-2 JIRA
14 | “issue” a text file containing the usernames and passwords of the targeted Victim-2
15 | employee, including his/her personal email account, LinkedIn account, and personal
16 | investment and financial institution accounts.

17 | g. The conspiracy compromised, illegally accessed, had unauthorized
18 | communications with, and exfiltrated proprietary, private, and non-public victim data and
19 | information from the computer systems of Victim-3, a restaurant chain with thousands of
20 | locations, including the State of Washington. From approximately March 24, 2017 to
21 | April 18, 2017, the conspiracy accessed computer systems of Victim-3 and implanted
22 | malware designed to harvest payment card data from cards used on point-of-sale devices
23 | at restaurant locations nationwide, including approximately 33 locations within the
24 | Western District of Washington.

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

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

7 ii. On or about March 29, 2017, a FIN7 member created an
8 "issue" on the conspiracy's private JIRA server specifically related to Victim-8 and
9 posted results from several network mapping tools used on Victim-8's internal network.

10 iii. On or about March 31, 2017, a FIN7 member posted a link to
11 the point-of-sale software management solution used by Victim-8, and a username and
12 password to the Victim-8 JIRA "issue." The software management tool allows a
13 company to manage point-of-sale systems at multiple locations. The FIN7 member also
14 uploaded several screenshots presumably from one or more victim computers at Victim-
15 8, which showed, among other things, the user logged into Victim-8's account for the
16 software management tool.

17 iv. On or about April 6, 2017, a FIN7 member uploaded to the
18 Victim-8 JIRA "issue" a file containing hundreds of usernames and passwords for
19 approximately 798 Victim-8 locations, including 37 locations located in the State of
20 Washington. The file included network information, telephone communications, and
21 locations of alarm panels within restaurants.

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

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

27 vii. On or about May 8, 2017, a FIN7 member uploaded to the
28 Victim-8 JIRA "issue" exfiltrated files related to a password management system from a

1 | compromised computer, which contained the credentials, usernames, and passwords of a
2 | particular employee.

3 | viii. On or about May 15, 2017, a FIN7 member uploaded to the
4 | Victim-8 JIRA “issue” screenshots of a compromised computer that showed the
5 | employee accessing Victim-8’s security infrastructure management software using that
6 | same employee’s credentials.

7 | i. 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 one or more locations of Victim-9, a fast-food
10 | restaurant chain with thousands of locations throughout the United States, including
11 | Washington. For instance,

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

19 | ii. On or about April 5, 2017, co-conspirator D.F. created an
20 | “issue” on the conspiracy’s private JIRA server specifically related to Victim-9. One or
21 | more FIN7 members posted usernames and passwords for Victim-9 locations, including a
22 | Victim-9 location in Vancouver, Washington.

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

27 | i. On or about April 11, 2017, the conspiracy, directly and
28 | through intermediaries, used the account oliver_palmer@yahoo.com, to send a phishing

1 email, with the subject "claim," to an employee of a Victim-4 located in Renton,
2 Washington, with an attached Rich Text Format (.rtf) document that contained malware.
3 The email falsely purported to convey a customer complaint and contained additional
4 materially false representations designed to induce the targeted employee to enable the
5 malware, and compromise the computer system.

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

13 iii. On or about May 25, 2017, the conspiracy, directly and
14 through intermediaries, used the account Adrian.1987clark@yahoo.com, to send a
15 phishing email, with the subject "takeout order," to an employee of a Victim-4 located in
16 or around Spokane, Washington, with an attached Rich Text Format (.rtf) document that
17 contained malware. The email falsely stated that the sender had a large takeout order and
18 contained additional materially false representations designed to induce the targeted
19 employee to enable the malware, and compromise the computer system.

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

25 i. On or about May 24, 2017, a FIN7 member created an "issue"
26 on the conspiracy's private JIRA server specifically related to Victim-10. One or more
27 FIN7 members posted information relating to the intrusion of computer systems and
28

1 | exfiltrated data, including files containing passwords and screenshots from one or more
2 | compromised computers.

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

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

16 | All in violation of Title 18, United States Code, Section 371.

17 | **COUNTS 17 - 19**

18 | **(Accessing a Protected Computer in Furtherance of Fraud)**

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

21 | 27. On or about the dates listed below, within the Western District of
22 | Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, and others known
23 | and unknown to the Grand Jury, knowingly and with intent to defraud accessed a
24 | protected computer without authorization and in excess of authorized access, and by
25 | means of such conduct furthered the intended fraud and obtained something of value,
26 | specifically, payment card data and proprietary and non-public information, whereby the
27 | object of the fraud and the thing obtained consisted of more than the use of the computers
28 | 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, FEDIR OLEKSIYOVYCH HLADYR, 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 persons during a 1-year period aggregating at least \$5,000.00 in value and (ii) damage affecting 10 or more protected computers during a 1-year period:

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

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

//
//
//

COUNT 23

(Access Device Fraud)

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

31. Beginning at a time unknown, and continuing through on or after January 10, 2018, within the Western District of Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, and others known and unknown to the Grand Jury, knowingly and with intent to defraud, possessed fifteen or more counterfeit and unauthorized access devices, namely, payment card data, account numbers, and other means of account access that can be used, alone and in conjunction with another access device, to obtain money, goods, services, and any other thing of value, and that can be used to initiate a transfer of funds; said activity affecting interstate and foreign commerce

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

COUNT 24

(Aggravated Identity Theft)

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

33. Beginning at a time unknown, but no earlier than on or about February 21, 2017, and no later than March 3, 2017, and continuing through on or after November 21, 2017, at Seattle, within the Western District of Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, and others known and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit: the name, username, and password of a real person, J.Q., an employee of Victim-2, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18 U.S.C. § 1349, as charged in Count 1, and wire fraud, in violation of 18 U.S.C. § 1343, as

1 charged in Counts 5 and 6, knowing that the means of identification belonged to another
2 actual person.

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

4 **COUNT 25**

5 **(Aggravated Identity Theft)**

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

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

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

18 **COUNT 26**

19 **(Aggravated Identity Theft)**

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

22 37. Beginning at a time unknown, but no later than on or about January 27,
23 2017, and continuing through on or after November 21, 2017, within the Western District
24 of Washington, and elsewhere, FEDIR OLEKSIYOVYCH HLADYR, and others known
25 and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful
26 authority, a means of identification of another person, to wit: the name, username, and
27 password of real persons, B.C., C.H., E.L., J.M., A.P, R.O., T.T., and L.D., employees of
28 Victim-7, during and in relation to a felony violation enumerated in 18 U.S.C.

1 § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18 U.S.C.
2 § 1349, as charged in Count 1, knowing that the means of identification belonged to
3 another actual person.

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

5 **FORFEITURE ALLEGATION**

6 38. The allegations contained in Counts 1 through 15 of this Superseding
7 Indictment are hereby realleged and incorporated by reference for the purpose of alleging
8 forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28,
9 United States Code, Section 2461(c). Upon conviction of any of the offenses charged in
10 Counts 1 through 15, the defendant, FEDIR OLEKSIYOVYCH HLADYR, shall forfeit
11 to the United States any property, real or personal, which constitutes or is derived from
12 proceeds traceable to such offenses, including but not limited to a judgment for a sum of
13 money representing the property described in this paragraph.

14 39. The allegations contained in Counts 16 through 22 of this Superseding
15 Indictment are hereby realleged and incorporated by reference for the purpose of alleging
16 forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).
17 Upon conviction of any of the offenses charged in Counts 16 through 22, the defendant,
18 FEDIR OLEKSIYOVYCH HLADYR, shall forfeit to the United States any property
19 constituting, or derived from, proceeds the defendant obtained, directly or indirectly, as
20 the result of such offenses, and shall also forfeit the defendant's interest in any personal
21 property that was used or intended to be used to commit or to facilitate the commission of
22 such offenses, including but not limited to a judgment for a sum of money representing
23 the property described in this paragraph.

24 40. The allegations contained in Count 23 of this Superseding Indictment are
25 hereby realleged and incorporated by reference for the purpose of alleging forfeitures
26 pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 1029(c)(1)(C), and
27 Title 28, United States Code, Section 2461(c). Upon conviction of the offense charged in
28 Count 23, the defendant, FEDIR OLEKSIYOVYCH HLADYR, shall forfeit to the

1 United States any property, real or personal, which constitutes or is derived from
2 proceeds traceable to such offense, and shall also forfeit any personal property used or
3 intended to be used to commit such offense, including but not limited to a judgment for a
4 sum of money representing the property described in this paragraph.

5 *(Substitute Assets)*

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

- 8 a. cannot be located upon the exercise of due diligence;
- 9 b. has been transferred or sold to, or deposited with, a third party;
- 10 c. has been placed beyond the jurisdiction of the court;
- 11 d. has been substantially diminished in value; or
- 12 e. has been commingled with other property which cannot be divided
13 without difficulty,

14 //

15 //

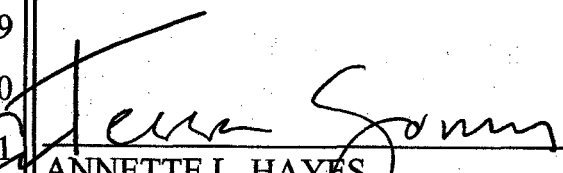
1 the United States of America shall be entitled to forfeiture of substitute property pursuant
2 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
3 Code, Section 2461(c).

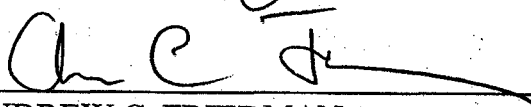
4 A TRUE BILL:

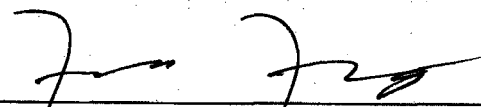
5 DATED: 1.25.18

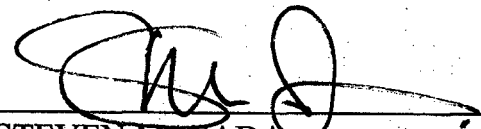
6
7 (Signature of Foreperson redacted pursuant to
8 policy of the Judicial Conference)

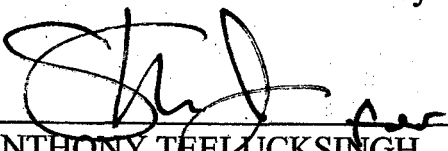
9 FOREPERSON

10
11 
12 ANNETTE L. HAYES
13 United States Attorney

14 
15 ANDREW C. FRIEDMAN
16 Assistant United States Attorney

17 
18 FRANCIS FRANZE-NAKAMURA
19 Assistant United States Attorney

20 
21 STEVEN MASADA
22 Assistant United States Attorney

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