

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.

December 12 2019

By William M. McCool Deputy
WILLIAM M. McCOOL, Clerk

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

UNITED STATES OF AMERICA,
Plaintiff,

v.

DENYS IARMAK,
aka "Denys Olegovich Iarmak,"
aka "Denys Yarmak,"
aka "Denis Jarmak,"
aka "GakTus,"
aka "denis.jarmak,"

Defendant.

NO. **CR19-257 RAJ**
INDICTMENT

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. 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
21 cybercriminals.

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.

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

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

COUNT 1

(Conspiracy to Commit Wire and Bank Fraud)

I. OFFENSE

11. The allegations set forth in Paragraphs 1 through 10 and 21 through 25 of this Indictment are re-alleged and incorporated as if fully set forth herein.

12. Beginning at a time unknown, but no later than September 2015, and continuing through on or after December 12, 2019, at Seattle, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, 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 willfully devise and execute and attempt to execute, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises; and in executing and attempting to execute this scheme and artifice, to knowingly cause to be transmitted in interstate and foreign commerce, by means of wire communication, certain signs, signals and sounds as further described below, in violation of Title 18, United States Code, Section 1343;

b. to knowingly and willfully devise and execute and attempt to execute, a scheme and artifice to defraud financial institutions, as defined by Title 18,

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. The defendant, and others known and unknown to the Grand Jury, were
7 part of a financially motivated cybercriminal conspiracy known variously as FIN7, the
8 Carbanak Group, and the Navigator Group (referred to herein as "FIN7"). FIN7 consists
9 of a group of criminal actors engaged in a sophisticated malware campaign targeting the
10 computer systems of businesses, primarily in the restaurant, gaming, and hospitality
11 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
17 purposes of establishing persistence, and stealing money and property, including payment
18 card (e.g., credit and debit) track data, financial information, and proprietary and non-
19 public information. The objectives of the conspiracy further included using and selling
20 the 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, the 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 has targeted hundreds of victim companies and brands, including, but
23 not limited to, the following representative victims:

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

1 ii. “Victim-2” referenced herein is a public corporation
2 headquartered in Seattle, within the Western District of Washington, with operations
3 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 a U.S.-based pizza parlor
8 chain with hundreds of locations predominantly in the Western United States, including
9 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 an automotive retail and
15 repair chain with hundreds of locations in the United States, including in the Western
16 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), Google Docs, or
3 Rich Text File (.rtf) document with embedded malware. FIN7 used a variety of malware
4 delivery mechanisms in its phishing attachments including, but not limited to,
5 weaponized Microsoft Word macros, malicious Object Linking and Embedding (OLE)
6 objects, malicious visual basic scripts or JavaScript, and malicious embedded shortcut
7 files (LNK files). In some instances, the phishing email or attached file contained a link
8 to malware hosted on servers controlled by FIN7. The phishing email, through false
9 representations and pretenses, fraudulently induced the victim company employee to
10 open the attachment or click on the link to activate the malware. For example, when
11 targeting a hotel chain, the purported sender of the phishing email might falsely claim to
12 be interested in making a hotel reservation. By way of further example, when targeting a
13 restaurant chain, the purported sender of the phishing email might falsely claim to be
14 interested in placing a catering order or making a complaint about prior food service at
15 the restaurant.

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

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

1 order, or customer complaint could be found in the file attached to the previously
2 delivered email, to induce the employee at the victim company to read the phishing
3 email, open the attached file, and activate the malware.

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

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

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

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

18 l. Once a victim company's computers were incorporated into the
19 FIN7 botnet and remotely controlled by FIN7's malware, the group used this remote
20 control and access to, among other things, install and manage additional malware,
21 conduct surveillance, map and navigate the compromised computer network, compromise
22 additional computers, exfiltrate files, and send and receive data. For instance, FIN7 often
23 conducted surveillance on the victim's computer network by, among other things,
24 capturing screen shots and videos of victim computer workstations that provided the
25 conspirators with additional information about the victim company computer network
26 and non-public credentials for both generic company accounts and for actual company
27 employees.
28

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

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

13 o. For example, between approximately March 24, 2017, and April 18,
14 2017, FIN7 harvested payment card data from point-of-sale devices at certain Victim-3
15 restaurant locations, including dozens of locations in the Western District of Washington.

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

19 q. The payment card data were offered for sale to allow purchasers to
20 falsely represent themselves as authorized users of the stolen payment cards and to use
21 the stolen payment card information to purchase goods and services in fraudulent
22 transactions throughout the United States and the world, resulting in millions of dollars in
23 losses to, and thereby affecting, merchants and banks, including financial institutions, as
24 defined in Title 18, United States Code, Section 20. For example, on or about March 10,
25 2017, stolen payment card data related to accounts held at Victim-5, a financial
26 institution headquartered in the Western District of Washington, compromised through
27 the computer network intrusion of a victim company, was used to make unauthorized
28 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 operated as a structured enterprise with a hierarchical
5 command structure under which dozens of members with diverse skillsets could
6 coordinate their malicious activity. Members of the scheme included, but were not
7 limited to:

8 i. Fedir Hladyr, a systems administrator who, among other
9 things, maintained servers and communication channels used by the organization. Fedir
10 Hladyr played a leading managerial role by delegating tasks and by providing instruction
11 to other members of the scheme.

12 ii. Dmytro Fedorov, a high-level "pen-tester" who supervised
13 other hackers specifically tasked with breaching the security of victims' computer
14 systems without the victims' knowledge or consent.

15 iii. Andrii Kolpakov, a high-level "pen-tester" who supervised
16 other hackers responsible for breaching the security of victims' computer systems
17 without the victims' knowledge or consent.

18 iv. DENYS IARMAK, a "pen-tester" who was tasked with
19 breaching the security of victims' computer systems without the victims' knowledge or
20 consent.

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

26 u. For example, in Jabber communications with other FIN7 members,
27 Dmytro Fedorov, referenced using malware in connection with several specific victim
28 companies, discussed using the administrative control panels to receive data from

1 compromised computers, and identified several pen-testers working at his direction. By
2 way of further example, in a Jabber communication sent on or about October 26, 2017,
3 DENIS IARMAK provided Fedir Hladyr with internal system information that had been
4 stolen from a victim company, a U.S.-based restaurant chain.

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

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

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

24 y. FIN7 conspirators frequently used the project management software
25 JIRA, hosted on private virtual servers in various countries, to coordinate their malicious
26 activity and to manage the assorted network intrusions. JIRA is a project management
27 and issue-tracking program used by software development teams. FIN7 members
28 typically created a “project” on the virtual JIRA server and then associated “issues” with

1 the project, each issue akin to an issue directory or folder, for a victim company, which
2 they used to collaborate and share details of the intrusion, to post victim company
3 intelligence, such as network mapping information, and to store and share exfiltrated
4 data.

5 z. For example, on about September 7, 2016, Fedir Hladyr created an
6 "issue" for Victim-6, to which FIN7 conspirators including Andreii Kolpakov posted files
7 containing internal credentials for the victim company's computer network.

8 aa. By way of further example, on multiple occasions in January 2017,
9 Dmytro Fedorov and another FIN7 member posted to the FIN7 "issue" created for
10 Victim-7, information about the victim company's internal network and uploaded
11 exfiltrated data, including stolen employee credentials. Similarly, on or about April 5,
12 2017, Dmytro Fedorov created an "issue" for another victim company, Victim-9, and
13 uploaded stolen user credentials from the victim company. DENIS IARMAK had access
14 to approximately 25 JIRA issues on one FIN7 server, and approximately 20 JIRA issues
15 on another FIN7 server.

16 bb. FIN7 conspirators knew that the scheme would involve the use of
17 wires in both interstate and foreign commerce to accomplish the objectives of the
18 scheme. For example, each defendant and his FIN7 co-conspirators knew that execution
19 of the scheme necessarily caused the transmission of wire communications between the
20 United States and one or more servers controlled by FIN7 located in foreign countries.

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

22
23 **COUNTS 2 - 15**

24 **(Wire Fraud)**

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

I. SCHEME AND ARTIFICE TO DEFRAUD

17. Beginning at a time unknown, but no later than September 2015, and continuing through on or after December 12, 2019, at Seattle, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises.

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

II. MANNER AND MEANS OF SCHEME TO DEFRAUD

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

III. EXECUTION OF SCHEME TO DEFRAUD

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

Count	Date(s)	Victim/Location	Wire Communication
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
3	August 8, 2016	Victim-1 Pierce County	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
4	August 8, 2016	Victim-1 Pierce County	Electronic communication between a server located outside the State of Washington, and Victim-1's computer system, located within the State of Washington
5	February 21, 2017	Victim-2 Seattle	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
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

Count	Date(s)	Victim/Location	Wire Communication
			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 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 December 12, 2019, at Seattle, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, 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 cause 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 Indictment.

8 **IV. OVERT ACTS**

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

13 **Representative Channels of Communication**

14 *Virtual Servers*

15 a. As part of its command and control infrastructure, FIN7 used a
 16 number of physical servers in different countries to host virtual communication servers.
 17 In addition to other channels of communication, FIN7 members used virtual HipChat,
 18 JIRA, and Jabber servers to collaborate and coordinate their attacks.

19 **Hip Chat**

20 i. FIN7 utilized a virtual HipChat Server for a variety of
 21 purposes, including, but not limited to, interviewing prospective members, collaborating
 22 on attacks against victim companies, and sharing malware and exfiltrated data. Among
 23 other communications made in furtherance of the conspiracy:

24 1. In 2016, Fedir Hladyr created a private HipChat room
 25 for communications with a leader of the conspiracy and subsequently uploaded data
 26 stolen from victim companies.

27 2. On or about March 14, 2016, Fedir Hladyr uploaded an
 28 archive to his private HipChat room with a leader of the conspiracy that contained

1 numerous data files containing payment card numbers stolen from a victim company that
2 had publicly reported a security breach involving the loss of tens of thousands of payment
3 cards.

4 3. On or about February 1, 2016, a member of the
5 conspiracy uploaded a file named "track_dumper_micros" to a HipChat room.

6 4. On or about February 6, 2016, in a HipChat room
7 titled "collection" that was accessed by Fedir Hladyr, and others, a FIN7 member
8 uploaded a file named "tracksDecodingPHP."

9 5. On or about March 7, 2017, a FIN7 member uploaded
10 files containing VBS script-based malware code into a HipChat room.

11 6. On or about April 8, 2016, Fedir Hladyr created a
12 HipChat room called "My_Files," to which he had exclusive access, and to which he later
13 uploaded data for approximately 100 stolen payment cards and network maps of internal
14 network infrastructures.

15 7. On or about July 19, 2016, Fedir Hladyr posted in a
16 HipChat room, files related to a victim company, including multiple screenshots from one
17 or more compromised computers that showed, among other things, internal company
18 information and an administrator password.

19 8. On or about March 6, 2017, in a HipChat room, a
20 FIN7 member described FIN7's misuse of Google services to harvest information from
21 victim computers, disseminate malware, and perform additional malicious activities.

22 JIRA

23 ii. As explained in Paragraph 15.y, FIN7 used virtual JIRA
24 servers to coordinate their malicious activity and to exchange files. Among other
25 communications made in furtherance of the conspiracy:

26 1. On or about January 17, 2017, a FIN7 member created
27 an issue and uploaded PowerShell scripts design to capture and exfiltrate non-public
28 network information from victim computers.

2. On or about February 20, 2017, a FIN7 member created an issue in which he outlined how to use Meterpreter to allow FIN7 to access and control a victim computer.

3. On or about March 3, 2017, a FIN7 member created an issue regarding a malicious PowerShell script designed to steal passwords from victim companies while avoiding detection by anti-virus software.

4. On or about March 3, 2017, DENYS IARMAK updated a JIRA issue he had created for a specific victim company and uploaded data he had stolen from that U.S. company.

Jabber

iii. FIN7 maintained a virtual Jabber server through which members could communicate privately. Among other Jabber communications made in furtherance of the conspiracy:

1. On or about April 14, 2016, a FIN7 member informed Andrii Kolpakov that Fedir Hladyr and another individual were the “main” directors of the group.

2. On or about August 1, 2016, a FIN7 member directed Dmytro Fedorov to target victim machines that ran MICROS point-of-sale software.

3. On or about December 7, 2016, a FIN7 member directed another member of the conspiracy to develop the ability to misuse Google services to launch malicious JavaScript scripts.

4. On or about January 12, 2017, a FIN7 member introduced himself to a new FIN7 recruit, explained how the member's salary would be paid, and indicated that Andrii Kolpakov would be his supervisor.

5. On or about March 2, 2017, a FIN7 member provided technical guidance to Dmytro Fedorov regarding a botnet control panel and asked Dmytro Fedorov to identify hackers who were under Dmytro Fedorov's supervision.

1 6. On or about February 6 and 7, 2017, a FIN7 member
2 and Fedir Hladyr discussed one of the malware programs that FIN7 used to dump credit
3 cards from victims' networks and saved the stolen credit card dumps into a particular file.

4 7. On or about April 28, 2017, DENYS IARMAK and
5 Dmytro Fedorov discussed the creation and use of phishing emails.

6 8. On or about May 31, 2017, a FIN7 member and Fedir
7 Hladyr discussed the possible detection of FIN7 malware installed on point-of-sale (POS)
8 terminals at a U.S.-based casual seafood restaurant chain.

9 9. On or about June 22, 2017, DENYS IARMAK
10 informed Dmytro Fedorov that one of FIN7's malware tools had been "burned" because
11 it was detectable by antivirus software.

12 10. On July 24, 2017, DENYS IARMAK exchanged
13 stolen victim information with Fedir Hladyr.

14 11. Between on or about August 7, 2017 and August 29,
15 2017, a FIN7 member and Fedir Hladyr discussed compromising point-of-sale systems
16 and intrusions related to known U.S. victim companies, including a franchise
17 management company that operates servers for a nation-wide restaurant chain.

18 12. On or about August 15, 2017, a FIN7 member and
19 Fedir Hladyr discussed the dissemination of phishing emails.

20 13. On or about October 19, 2017, Fedir Hladyr sent a
21 FIN7 member victim payment card information and the recipient confirmed that the
22 payment cards were valid.

23 14. On or about October 26, 2017, DENYS IARMAK
24 provided Fedir Hladyr information about a computer belonging to a victim, a U.S.
25 restaurant chain that was breached by FIN7.

26 *Email Communications*

27 b. FIN7 members also communicated regularly by email. Among other
28 communications made in furtherance of the conspiracy:

1 i. On or about September 29, 2015, a FIN7 member sent an
2 email containing code for a VBS script.

3 ii. On or about May 25, 2016, a FIN7 member sent a phishing
4 email to another member of FIN7.

5 iii. On or about September 13, 2016, a FIN7 member sent an
6 email with an attachment containing a malicious PHP script to another FIN7 member.

7 iv. On or about November 1, 2016, a FIN7 member sent an email
8 with the text of a phishing email and an attached Microsoft Word document containing
9 malware.

10 v. On or about November 1, 2016, Fedir Hladyr sent an email to
11 a FIN7 member with access information for FIN7's private Jabber server.

12 vi. On or about April 13, 2017, DENIS IARMAK sent another
13 FIN7 member an email related to his efforts to use commercial antivirus software to test
14 whether FIN7's malware tools would be detected by the antivirus software.

15 vii. On or about September 20, 2017, a FIN7 member emailed
16 malware to another member of the conspiracy that contained a malicious script designed
17 to take screenshots of victims' computers.

18 **Victim-1**

19 c. 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-1, a hotel and casino in the Western
22 District of Washington. For instance,

23 i. On or about August 8, 2016, the conspiracy, directly and
24 through intermediaries, used the account just_etravel@yahoo.com to send a phishing
25 email, with the subject "order," to an employee of Victim-1 located in Tacoma,
26 Washington, with an attached Microsoft Word document that contained malware. The
27 email contained materially false representations designed to induce the targeted employee
28 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 **Victim-2**

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

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

25 ii. From on or about February 21, 2017, to approximately
26 March 3, 2017, the conspiracy illegally accessed and had communications with the
27 computer systems of Victim-2 located in Seattle, Washington. For instance, between
28 about February 23, 2017, and February 24, 2017, the victim computer made outgoing

1 connections to and transferred internal data, without authorization, to an IP address
2 located in a foreign country.

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

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

11 **Victim-3**

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

20 **Victim-4**

21 f. 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 one or more locations of Victim-4, a pizza
24 parlor chain with hundreds of locations, including in Washington. For instance,

25 i. On or about April 11, 2017, the conspiracy, directly and
26 through intermediaries, used the account oliver_palmer@yahoo.com, to send a phishing
27 email, with the subject "claim," to an employee of a Victim-4 located in Renton,
28 Washington, with an attached Rich Text Format (.rtf) document that contained malware.

1 The email falsely purported to convey a customer complaint and contained additional
2 materially false representations designed to induce the targeted employee to enable the
3 malware, and compromise the computer system.

4 ii. On or about April 11, 2017, the conspiracy, directly and
5 through intermediaries, used the account oliver_palmer@yahoo.com, to send a phishing
6 email, with the subject "claim," to an employee of a Victim-4 located in Vancouver,
7 Washington, with an attached Rich Text Format (.rtf) document that contained malware.

8 The email falsely purported to convey a customer complaint and contained additional
9 materially false representations designed to induce the targeted employee to enable the
10 malware, and compromise the computer system.

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

18 **Victim-6**

19 g. 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-6, a restaurant chain with locations in
22 multiple states. For instance,

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

1 ii. On or about September 7, 2016, Fedir Hladyr created an
2 “issue” on the conspiracy’s private JIRA server specifically related to Victim-6, to which
3 Andrii Kolpakov subsequently uploaded comments and stolen information pertaining to
4 Victim-6’s network structure and administrative credentials.

5 iii. On or about May 29, 2017, a FIN7 member and Fedir Hladyr
6 discussed an issue with FIN7 command and control servers associated with the
7 compromise of Victim-6.

8 **Victim-7**

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

13 i. On or about January 18, 2017, a FIN7 member created an
14 “issue” on the conspiracy’s private JIRA server specifically related to Victim-7, to which
15 that individual and Dmytro Fedorov subsequently posted results from several network
16 mapping tools used on Victim-7’s internal network.

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

20 iii. On or about January 23, and January 24, 2017, Dmytro
21 Fedorov posted information about Victim-7’s internal network and uploaded a file
22 containing multiple IP addresses and information about Victim-7’s servers to the Victim-
23 7 JIRA “issue.”

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

1 On or about February 9, 2017, a FIN7 member created an “issue” on the
2 conspiracy’s private JIRA server specifically related to Victim-7, which was assigned to
3 DENYS IARMAK.

4 **Victim-8**

5 i. 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 Victim-8, a restaurant chain with hundreds of
8 locations in multiple states, including Washington. For instance,

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

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

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

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

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 ix. On or about May 16, 2017, a member of the conspiracy and
17 Fedir Hladyr discussed through Jabber a particular server used in the intrusion of
18 Victim-8.

19 **Victim-9**

20 j. 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-9, a fast-food
23 restaurant chain with thousands of locations throughout the United States, including
24 Washington. For instance,

25 i. The conspiracy, directly and through intermediaries, sent
26 phishing emails with an attached file that contained malware to multiple Victim-9
27 locations. For instance, on or about April 7, 2017, the conspiracy used the account
28 oliver_palmer@yahoo.com to send a phishing email to a Victim-9 location in the State of

1 Oregon. The email contained materially false representations designed to induce the
2 targeted employee to open the file, enable the malware, and compromise the computer
3 system.

4 ii. On or about April 5, 2017, Dmytro Fedorov created an
5 “issue” on the conspiracy’s private JIRA server specifically related to Victim-9 to which
6 one or more FIN7 members subsequently posted usernames and passwords for Victim-9
7 locations, including a Victim-9 location in Vancouver, Washington.

8 **Victim-10**

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

14 i. On or about May 24, 2017, a FIN7 member created an “issue”
15 on the conspiracy’s private JIRA server specifically related to Victim-10, to which other
16 FIN7 members subsequently posted information relating to the intrusion of computer
17 systems and exfiltrated data, including files containing passwords and screenshots from
18 one or more compromised computers.

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

26 iii. From on or about June 12, 2017, to a date unknown, the
27 conspiracy illegally accessed and had communications with the computer systems of
28 Victim-10 located in Iowa. For instance, the conspiracy transferred, without

1 authorization, proprietary, private, and non-public victim data and information, including
 2 usernames and passwords, to a JIRA server managed by FIN7, located in a foreign
 3 country.

4 iv. On or about June 13, 2017, , a FIN7 member created an
 5 “issue” on the conspiracy’s private JIRA server specifically related to Victim-10, which
 6 was assigned to DENYS IARMAK.

7 v. On or about June 14, 2017, a FIN7 member uploaded a
 8 variety of information including recommendations for attack vectors FIN7 members
 9 could use to access Victim-10’s internal network.

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

11 COUNTS 17 - 19

12 **(Accessing a Protected Computer in Furtherance of Fraud)**

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

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

Count	Dates	Victim
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

23 All in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b),
 24 1030(c)(3)(A) and 2.
 25
 26
 27
 28

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

28. The allegations set forth in Paragraphs 1 through 27 of this 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, the defendant, DENYS IARMAK, 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:

Count	Dates	Victim
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 Indictment are re-alleged and incorporated as if fully set forth herein.

31. Beginning at a time unknown, and continuing through on or after June 20, 2018, within the Western District of Washington, and elsewhere, the defendant, DENYS IARMAK, 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,

1 services, and any other thing of value, and that can be used to initiate a transfer of funds;
 2 said activity affecting interstate and foreign commerce

3 All in violation of Title 18, United States Code, Sections 1029(a)(3), 1029(b)(1),
 4 1029(c)(1)(A), and 2.

6 **COUNT 24**

7 **(Aggravated Identity Theft)**

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

10 33. Beginning at a time unknown, but no earlier than on or about February 21,
 11 2017, and no later than March 3, 2017, and continuing through on or after November 21,
 12 2017, at Seattle, within the Western District of Washington, and elsewhere, the
 13 defendant, DENYS IARMAK, and others known and unknown to the Grand Jury, did
 14 knowingly transfer, possess, and use, without lawful authority, a means of identification
 15 of another person, to wit: the name, username, and password of a real person, J.Q., an
 16 employee of Victim-2, during and in relation to a felony violation enumerated in 18
 17 U.S.C. § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18
 18 U.S.C. § 1349, as charged in Count 1, and wire fraud, in violation of 18 U.S.C. § 1343, as
 19 charged in Counts 5 and 6, knowing that the means of identification belonged to another
 20 actual person.

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

23 **COUNT 25**

24 **(Aggravated Identity Theft)**

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

27 35. Beginning at a time unknown, but no later than on or about May 8, 2017,
 28 and continuing through on or after November 21, 2017, within the Western District of

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

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

10 **COUNT 26**

11 **(Aggravated Identity Theft)**

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

14 37. Beginning at a time unknown, but no later than on or about January 27,
15 2017, and continuing through on or after November 21, 2017, within the Western District
16 of Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and
17 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, username, and
19 password of real persons, B.C., C.H., E.L., J.M., A.P, R.O., T.T., and L.D., employees of
20 Victim-7, during and in relation to a felony violation enumerated in 18 U.S.C.
21 § 1028A(c), that is, conspiracy to commit wire and bank fraud, in violation of 18 U.S.C.
22 § 1349, as charged in Count 1, knowing that the means of identification belonged to
23 another actual person.

24 All in violation of Title 18, United States Code, Sections 1028A(a) and 2.
25
26
27
28

FORFEITURE ALLEGATION

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

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

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

(Substitute Assets)

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

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

//

//

//

//

//

//

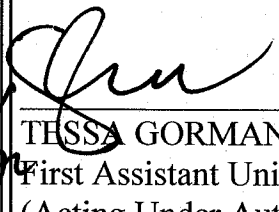
1 the United States of America shall be entitled to forfeiture of substitute property pursuant
2 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
3 Code, Section 2461(c).

4 A TRUE BILL:

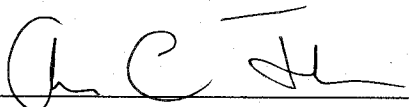
5 DATED: 12/12/19

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

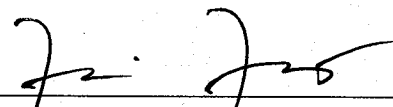
9 FOREPERSON

10 
11 _____
12 TESSA GORMAN

13 First Assistant United States Attorney
14 (Acting Under Authority Conferred by 28 U.S.C. § 515)

15 
16 _____
17 ANDREW C. FRIEDMAN

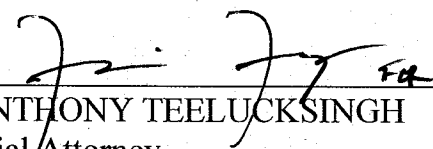
18 Assistant United States Attorney

19 
20 _____
21 FRANCIS FRANZE-NAKAMURA

22 Assistant United States Attorney

23 
24 _____
25 STEVEN MASADA

26 Assistant United States Attorney

27 
28 _____
29 ANTHONY TEELUCKSINGH

30 Trial Attorney
31 Computer Crime and Intellectual Property Section

DEFENDANT STATUS SHEET

(One for each defendant)

I. CASE STATUS

Name of Defendant: DENYS IARMAK

Has defendant had initial appearance in this case? ☐ Yes ☒ No

MJ

CR

II. CUSTODIAL STATUS

If defendant had initial appearance, please check one of the following:

☐ Continue Conditions of Release

☐ Continue Detention

☐ Temporary Detention, a detention hearing has been scheduled for

III. ARRAIGNMENT

☒ Warrant to Issue (If so, please complete *Defendant Arrest Warrant Info Sheet*)

☐ Summons to be Issued for Appearance on

Defendant's Address:

☐ Letter to Defense Counsel for Appearance on

Defense Attorney's Name and address:

The estimated trial time is 21 days.

(Revised March 2018)