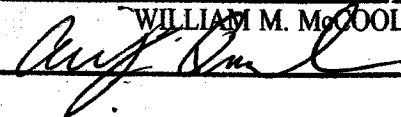


Exhibit 5

Indictment (Dkt. #1), *United States v. Kolpakov*, CR18-159RSM

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.

June 21 20 18
WILLIAM M. McCOOL, Clerk
By  Deputy

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

UNITED STATES OF AMERICA,
Plaintiff,

NO. **CR18-159 JLR**
INDICTMENT

v.

ANDRII KOLPAKOV,
aka "Andrey Kolpakov,"
aka "Andriy Kolpakov,"
aka "Andre Kolpakov,"
aka "Andrew Kolpakov,"
aka "santisimo,"
aka "santisimoz,"
aka "AndreyKS,"
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. 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.

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

7 **II. OBJECTIVES OF THE CONSPIRACY**

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

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

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

26 15. The manner and means used to accomplish the conspiracy included the
27 following:
28

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

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

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

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

27 i. "Victim-1" referenced herein is the Emerald Queen Hotel and
28 Casino (EQC), a hotel and casino owned and operated by a federally recognized Native

1 American Tribe with locations in Pierce County, within the Western District of
2 Washington.

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

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

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

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

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

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

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

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

26 x. "Victim-10" referenced herein is Taco John's, a U.S.-based
27 fast-food restaurant chain with hundreds of locations in the United States, including in the
28 Western District of Washington.

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

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

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

1 | make a follow-up call falsely claiming that the details of a reservation request, catering
2 | order, or customer complaint could be found in the file attached to the previously
3 | delivered email, to induce the employee at the victim company to read the phishing
4 | email, open the attached file, and activate the malware.

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

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

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

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

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

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 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. Key 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
16 supervised other hackers responsible for breaching the security of victims’ computer
17 systems without the victims’ knowledge or consent.

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,
24 co-conspirator Dmytro Fedorov, using his alias “hotdima,” referenced using malware in
25 connection with several specific victim companies, discussed using the administrative
26 control panels to receive data from compromised computers, and identified several pen-
27 testers working at his direction.

28

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, co-conspirator Fedir Hladyr created
6 HipChat user accounts for FIN7 members that allowed them to access the server.

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

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

21 y. FIN7 conspirators frequently used the project management software
22 JIRA, hosted on private virtual servers in various countries, to coordinate their malicious
23 activity and to manage the assorted network intrusions. JIRA is a project management
24 and issue-tracking program used by software development teams. FIN7 members
25 typically created a “project” on the virtual JIRA server and then associated “issues” with
26 the project, each issue akin to an issue directory or folder, for a victim company, which
27 they used to collaborate and share details of the intrusion, to post victim company
28

1 intelligence, such as network mapping information, and to store and share exfiltrated
2 data.

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

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

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

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

19
20 **COUNTS 2 - 15**

21 **(Wire Fraud)**

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

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

25 17. Beginning at a time unknown, but no later than September 2015, and
26 continuing through on or after June 20, 2018, at Seattle, within the Western District of
27 Washington, and elsewhere, the defendant, ANDRII KOLPAKOV, aka "Andrey
28 Kolpakov," "Andriy Kolpakov," "Andre Kolpakov," "Andrew Kolpakov," "santisimo,"

1 “santisimoz,” and “AndreyKS,” and others known and unknown to the Grand Jury,
 2 devised and intended to devise a scheme and artifice to defraud and to obtain money and
 3 property by means of materially false and fraudulent pretenses, representations and
 4 promises.

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

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

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

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

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

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

1 **I. OFFENSE**

2 22. Beginning at a time unknown, but no later than September 2015, and
3 continuing through on or after June 20, 2018, at Seattle, within the Western District of
4 Washington, and elsewhere, the defendant, ANDRII KOLPAKOV, aka "Andrey
5 Kolpakov," "Andriy Kolpakov," "Andre Kolpakov," "Andrew Kolpakov," "santisimo,"
6 "santisimoz," and "AndreyKS," and others known and unknown to the Grand Jury, did
7 knowingly and willfully combine, conspire, confederate and agree together to commit
8 offenses against the United States, to wit:

9 a. to knowingly and with intent to defraud, access a protected computer
10 without authorization and exceed authorized access to a protected computer, and by
11 means of such conduct further the intended fraud and obtain anything of value exceeding
12 \$5,000.00 in any 1-year period, in violation of Title 18, United States Code, Sections
13 1030(a)(4) and (c)(3)(A); and

14 b. to knowingly cause the transmission of a program, information,
15 code, and command, and as a result of such conduct, intentionally cause damage without
16 authorization to a protected computer, and cause loss to one or more persons during a 1-
17 year period aggregating at least \$5,000.00 in value and damage affecting 10 or more
18 protected computers during a 1-year period, in violation of Title 18, United States Code,
19 Sections 1030(a)(5)(A) and (c)(4)(B)(i).

20 **II. OBJECTIVES OF THE CONSPIRACY**

21 23. The objectives of the conspiracy included hacking into protected computer
22 networks using malware designed to provide the conspirators with unauthorized access
23 to, and control of, victim computer systems. The objectives of the conspiracy further
24 included conducting surveillance of victim computer networks and installing additional
25 malware on the victim computer networks for the purposes of establishing persistence,
26 and stealing payment card track data, financial information, and proprietary, private, and
27 non-public information, with the intention of using and selling such stolen items, either
28 directly or indirectly, for financial gain. The objectives of the conspiracy further

1 included installing malware that would integrate victim computers into a botnet that
2 allowed the conspiracy to control, alter, and damage compromised computers.

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

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

6 **IV. OVERT ACTS**

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

11 a. As part of its command and control infrastructure, FIN7 used a
12 number of physical servers in different countries to host virtual communication servers.
13 In addition to other channels of communication, FIN7 members used virtual HipChat,
14 JIRA, Mumble, and Jabber servers to collaborate and coordinate their attacks.

15 b. For example, FIN7 maintained a virtual Jabber server through which
16 members could communicate privately. Among other Jabber communications made in
17 furtherance of the conspiracy:

18 i. On or about April 14, 2016, a FIN7 member informed
19 ANDRII KOLPAKOV that a particular individual and Fedir Hladyr were the “main”
20 directors of the group.

21 ii. On or about April 15, 2016, a FIN7 member informed
22 ANDRII KOLPAKOV that a particular individual was the “chief manager.”

23 iii. On or about January 12, 2017, a FIN7 member introduced
24 himself to a new FIN7 recruit, explained how the member’s salary would be paid, and
25 indicated that ANDRII KOLPAKOV would be his supervisor.

26 iv. On or about May 29, 2017, ANDRII KOLPAKOV informed
27 Dmytro Fedorov that KOLPAKOV had successfully located point-of-sale data and
28 accounting technology on a victim company’s network.

1 v. On or about September 18, 2017, ANDRII KOLPAKOV and
2 Dmytro Fedorov discussed the file types used in phishing emails, and KOLPAKOV
3 informed Fedorov of the development of an enhanced malware file that can activate
4 without being double-clicked upon by the phishing email recipient.

5 **Victim-1**

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

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

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

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

Victim-6

1
2 d. The conspiracy compromised, illegally accessed, had unauthorized
3 communications with, and exfiltrated proprietary, private, and non-public victim data and
4 information from the computer systems of Victim-6, a restaurant chain with locations in
5 multiple states. For instance,

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

12 ii. On or about September 7, 2016, co-conspirator Fedir Hladyr
13 created an “issue” on the conspiracy’s private JIRA server specifically related to Victim-
14 6, to which ANDRII KOLPAKOV subsequently uploaded comments and stolen
15 information pertaining to Victim-6’s network structure and administrative credentials.

Victim-7

16
17 e. 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-7, an automotive retail and repair chain
20 with hundreds of locations in multiple states, including Washington. For instance,

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

25 ii. On or about January 20, 2017, a FIN7 member posted
26 exfiltrated data, including multiple usernames and passwords with the title “Server
27 Passwords,” to the Victim-7 JIRA “issue.”
28

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

4 iii. On or about March 31, 2017, a FIN7 member posted a link to
5 the point-of-sale software management solution used by Victim-8, and a username and
6 password to the Victim-8 JIRA “issue.” The software management tool allows a
7 company to manage point-of-sale systems at multiple locations. The FIN7 member also
8 uploaded several screenshots presumably from one or more victim computers at Victim-
9 8, which showed, among other things, the user logged into Victim-8’s account for the
10 software management tool.

11 iv. On or about April 6, 2017, a FIN7 member uploaded to the
12 Victim-8 JIRA “issue” a file containing hundreds of usernames and passwords for
13 approximately 798 Victim-8 locations, including 37 locations located in the State of
14 Washington. The file included network information, telephone communications, and
15 locations of alarm panels within restaurants.

16 v. On or about April 7, 2017, a FIN7 member uploaded to the
17 Victim-8 JIRA “issue” a similar file containing numerous usernames and passwords for
18 Victim-8 locations.

19 vi. On or about May 5, 2017, a FIN7 member uploaded to the
20 Victim-8 JIRA “issue” a file containing file directories on a compromised computer.

21 vii. On or about May 8, 2017, a FIN7 member uploaded to the
22 Victim-8 JIRA “issue” exfiltrated files related to a password management system from a
23 compromised computer, which contained the credentials, usernames, and passwords of a
24 particular employee.

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

Victim-9

1
2 i. The conspiracy compromised, illegally accessed, had unauthorized
3 communications with, and exfiltrated proprietary, private, and non-public victim data and
4 information from the computer systems of one or more locations of Victim-9, a fast-food
5 restaurant chain with thousands of locations throughout the United States, including
6 Washington. For instance,

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

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

Victim-4

18
19 j. 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 one or more locations of Victim-4, a pizza
22 parlor chain with hundreds of locations, including in Washington. For instance,

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

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

8 iii. From on or about June 12, 2017, to a date unknown, the
9 conspiracy illegally accessed and had communications with the computer systems of the
10 Victim-10 located in Iowa. For instance, the conspiracy transferred, without
11 authorization, proprietary, private, and non-public victim data and information, including
12 usernames and passwords, to a JIRA server managed by FIN7, located in a foreign
13 country. On or about June 14, 2017, a FIN7 member uploaded a variety of information
14 including recommendations for attack vectors FIN7 members could use to access Victim-
15 10’s internal network.

16 All in violation of Title 18, United States Code, Section 371.
17

18 **COUNTS 17 - 19**

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

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

22 27. On or about the dates listed below, within the Western District of
23 Washington, and elsewhere, the defendant, ANDRII KOLPAKOV, aka “Andrey
24 Kolpakov,” “Andriy Kolpakov,” “Andre Kolpakov,” “Andrew Kolpakov,” “santisimo,”
25 “santisimoz,” and “AndreyKS,” and others known and unknown to the Grand Jury,
26 knowingly and with intent to defraud accessed a protected computer without
27 authorization and in excess of authorized access, and by means of such conduct furthered
28 the intended fraud and obtained something of value, specifically, payment card data and

1 proprietary and non-public information, whereby the object of the fraud and the thing
 2 obtained consisted of more than the use of the computers and the value of such use was
 3 more than \$5,000 in a 1-year period, as listed below:

4			
5	17	August 8, 2016 through October 4, 2016	Victim-1
6	18	February 21, 2017 through March 3, 2017	Victim-2
	19	March 24, 2017 through April 18, 2017	Victim-3

7 All in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b),
 8 1030(c)(3)(A) and 2.

10 COUNTS 20 - 22

11 (Intentional Damage to a Protected Computer)

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

14 29. On or about the dates listed below, within the Western District of
 15 Washington, and elsewhere, the defendant, ANDRII KOLPAKOV, aka "Andrey
 16 Kolpakov," "Andriy Kolpakov," "Andre Kolpakov," "Andrew Kolpakov," "santisimo,"
 17 "santisimoz," and "AndreyKS," and others known and unknown to the Grand Jury,
 18 knowingly caused the transmission of a program, information, code, and command, and
 19 as a result of such conduct, intentionally caused damage without authorization, to a
 20 protected computer, specifically, the protected computer system of the victim listed
 21 below, and the offense caused (i) loss to one or more persons during a 1-year period
 22 aggregating at least \$5,000.00 in value and (ii) damage affecting 10 or more protected
 23 computers during a 1-year period:

24			
25	20	August 8, 2016 through October 4, 2016	Victim-1
26	21	February 21, 2017 through March 3, 2017	Victim-2
27	22	March 24, 2017 through April 18, 2017	Victim-3

28 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, ANDRII KOLPAKOV, aka “Andrey Kolpakov,” “Andriy Kolpakov,” “Andre Kolpakov,” “Andrew Kolpakov,” “santisimo,” “santisimoz,” and “AndreyKS,” 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 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, the defendant, ANDRII KOLPAKOV, aka “Andrey Kolpakov,” “Andriy Kolpakov,” “Andre Kolpakov,” “Andrew Kolpakov,” “santisimo,” “santisimoz,” and “AndreyKS,” 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,

1 | username, and password of a real person, J.Q., an employee of Victim-2, during and in
2 | relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, conspiracy to
3 | commit wire and bank fraud, in violation of 18 U.S.C. § 1349, as charged in Count 1, and
4 | wire fraud, in violation of 18 U.S.C. § 1343, as charged in Counts 5 and 6, knowing that
5 | the means of identification belonged to another actual person.

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

7 |
8 | **COUNT 25**

9 | **(Aggravated Identity Theft)**

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

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

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

24 |
25 | **COUNT 26**

26 | **(Aggravated Identity Theft)**

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

1 37. Beginning at a time unknown, but no later than on or about January 27,
2 2017, and continuing through on or after November 21, 2017, within the Western District
3 of Washington, and elsewhere, the defendant, ANDRII KOLPAKOV, aka "Andrey
4 Kolpakov," "Andriy Kolpakov," "Andre Kolpakov," "Andrew Kolpakov," "santisimo,"
5 "santisimoz," and "AndreyKS," and others known and unknown to the Grand Jury, did
6 knowingly transfer, possess, and use, without lawful authority, a means of identification
7 of another person, to wit: the name, username, and password of real persons, B.C., C.H.,
8 E.L., J.M., A.P, R.O., T.T., and L.D., employees of Victim-7, during and in relation to a
9 felony violation enumerated in 18 U.S.C. § 1028A(c), that is, conspiracy to commit wire
10 and bank fraud, in violation of 18 U.S.C. § 1349, as charged in Count 1, knowing that the
11 means of identification belonged to another actual person.

12 All in violation of Title 18, United States Code, Sections 1028A(a) and 2.
13

14 **FORFEITURE ALLEGATION**

15 38. The allegations contained in Counts 1 through 15 of this Indictment are
16 hereby realleged and incorporated by reference for the purpose of alleging forfeitures
17 pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States
18 Code, Section 2461(c). Upon conviction of any of the offenses charged in Counts 1
19 through 15, the defendant, ANDRII KOLPAKOV, aka "Andrey Kolpakov," "Andriy
20 Kolpakov," "Andre Kolpakov," "Andrew Kolpakov," "santisimo," "santisimoz," and
21 "AndreyKS," shall forfeit to the United States any property, real or personal, which
22 constitutes or is derived from proceeds traceable to such offenses, including but not
23 limited to a judgment for a sum of money representing the property described in this
24 paragraph.

25 39. The allegations contained in Counts 16 through 22 of this Indictment are
26 hereby realleged and incorporated by reference for the purpose of alleging forfeitures
27 pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i). Upon
28 conviction of any of the offenses charged in Counts 16 through 22, the defendant shall

1 forfeit to the United States any property constituting, or derived from, proceeds the
2 defendant obtained, directly or indirectly, as the result of such offenses, and shall also
3 forfeit the defendant's interest in any personal property that was used or intended to be
4 used to commit or to facilitate the commission of such offenses, including but not limited
5 to a judgment for a sum of money representing the property described in this paragraph.

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

15 *(Substitute Assets)*

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

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

24 //

25 //

26

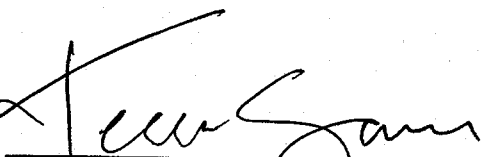
27

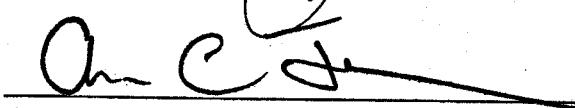
28

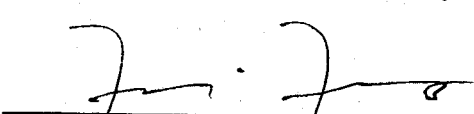
1 the United States of America shall be entitled to forfeiture of substitute property pursuant
2 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
3 Code, Section 2461(c).


4 A TRUE BILL: 21 June 2018
5 DATED:

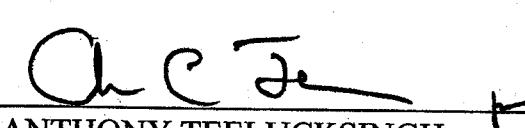
6
7 *(Signature of Foreperson redacted pursuant to*
8 *policy of the Judicial Conference)*
9 FOREPERSON

10 
11 ANNETTE L. HAYES
12 United States Attorney

13 
14 ANDREW C. FRIEDMAN
15 Assistant United States Attorney

16 
17 FRANCIS FRANZE-NAKAMURA
18 Assistant United States Attorney

19 
20 STEVEN MASADA
21 Assistant United States Attorney

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