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 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 v. ANDREY TURCHIN, a/k/a, "fxmsp," a/k/a, "Andej Turchin," a/k/a, "Adik Dalv," a/k/a, "Vadim bld," Defendant.	NO. CR18-303 RAJ **INDICTMENT**

The Grand Jury charges that:

COUNT 1

(Conspiracy to Commit Computer Hacking)

A. Overview

1. The defendant, ANDREY TURCHIN, operating under the alias "fxmsp," among others, is a computer hacker who resides in the country of Kazakhstan.

2. ANDREY TURCHIN, also known by the names "Andej Turchin," "Adik Dalv," and "Vadim bld," is a member of a prolific, financially motivated cybercriminal group composed of foreign actors that hacks the computer networks of a broad array of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

corporate entities, educational institutions, and governments throughout the world, including the United States, and thereafter advertises and sells such unauthorized access to its victims' protected systems to interested buyers. Members of the cybercriminal group include individuals using such monikers as "fxmsp," "BigPetya," "Lampeduza," "Antony Moricone," "Nikolay," "Ares," and "HeroKuma," among others.

3. The cybercriminal group uses various hacking techniques, such as brute force attacks and phishing email campaigns, to attack and compromise victim networks. Once inside the victim's system, the threat actors deploy additional malicious code, or malware, and move laterally throughout the network. The group ultimately attempts to locate and exfiltrate administrative credentials, to gain broad access and control of the victim's system, and to establish persistence through use of Remote Access Tools (RATs) and other malware implanted on network computers.

4. Members of the cybercriminal group, including ANDREY TURCHIN, advertise victim network access for sale, both through postings on various underground online forums and through private offerings to established or trusted buyers. The cybercriminal group frequents several forums known to host and facilitate criminal activity, such as Exploit.in, fuckav.ru, Club2Card, Altenen, Blackhacker, Omerta, Sniff3r, and L33t, among others. To date, the group has claimed access to, and advertised for sale network access to, a total of more than 300 corporate entities, educational institutions, governments, and governmental agencies and departments, located in roughly 40 countries across six continents, including over 30 such entities located in the United States.

5. The cybercriminal group's prices for network access typically ranges from thousands to tens of thousands dollars, but in some cases, exceeds a hundred thousand dollars, depending on the victim entity and the degree of system access and controls, and the group has derived a substantial but unknown amount in illicit profits from its scheme. Victims incurred additional losses totaling in the tens of millions of dollars identifying and remediating the implanted malware, unauthorized network access, and the consequential network damage.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. Relevant Terms

6. 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.

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

8. Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. RDP allows another computer to interact and control the computer remotely. Another computer can connect to a computer with RDP enabled by being in the same connected network and providing credentials to log in. If a computer is connected to the Internet and has RDP enabled, any computer on the Internet can attempt to connect to that computer. Multiple companies not associated with Microsoft have created third party software that uses and interacts with RDP.

9. The Onion Router, or "Tor," is an anonymity tool used by individuals when they wish to obfuscate the origin of the internet connection (entry point). This is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

accomplished by bouncing the original internet connection through several intermediate computers (relays) that utilize encryption, thus anonymizing the entry point.

10. Malware is malicious computer code running on a computer. Malware can be designed to do a variety of things, including logging every keystroke on a computer, stealing financial information or "user credentials" (passwords or usernames), or commanding that computer to become part of a network of "robot" or "bot" computers known as a "botnet." In addition, malware can be used to transmit data from the infected computer to another destination on the Internet, as identified by an IP address.

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

12. 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.

13. Brute force attacks are a technique developed over time by people who seek to obtain valid credentials to gain access to a protected system, software, or data. A brute force attack will use a trial-and-error method of consecutively guessing credentials against the protected medium until a guess is successful in obtaining access to the protected medium. A brute-force attack is typically conducted using automated software along with a list of commonly used or known passwords, also known as dictionaries, to guess the credentials.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

C. Offense

14. Beginning at a time unknown, but no later than October 2017, and continuing through on or about December 12, 2018, in King County and Cowlitz County, within the Western District of Washington, and elsewhere, the defendant, ANDREY TURCHIN, 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 intentionally access a computer without authorization, and exceed authorized access to a computer, and thereby obtained information from a protected computer, and the offense was committed for purposes of commercial advantage or private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States and the laws of a state, including Washington, and the value of the information obtained exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (ii) and (iii); 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 one-year period aggregating at least $5,000 in value and damage affecting 10 or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

D. Objectives of the Conspiracy

15. The objectives of the conspiracy included hacking into protected computer networks using malicious software (hereinafter, "malware") designed to provide conspirators with unauthorized access to, and control of, victim computer systems. The objectives of the conspiracy further include conducting surveillance of victim computer networks, exfiltrating and using administrative credentials, and installing additional malware on victim computer networks for purposes of establishing persistence, all for the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

purpose of selling such access to victim computer networks to other cybercriminal actors for financial gain.

E. Manner and Means of the Conspiracy

16. The manner and means used to accomplish the conspiracy included the following:

a. The conspirators employed hacking techniques to gain access, without authorization, to protected computer networks, broadly targeting victims worldwide, including entities located in the United States and specifically in the Western District of Washington. The cybercriminal group used various attack vectors to distribute and implant malware designed to gain unauthorized access to, take control of, and exfiltrate data from the computer systems of a broad array of corporate and governmental entities and educational institutions.

b. The conspirators often initiated brute force attacks of login credentials to access Internet-connected RDP-enabled computers on a victim network. The conspirators scanned the Internet for open ports and performed surveillance on targeted victim networks in order to identify victim computers vulnerable to brute force attacks over RDP.

c. The conspirators also initiated attacks by delivering, directly and through intermediaries, one or more phishing emails with an attached malicious file or embedded Internet hyperlink, using wires in interstate and foreign commerce, to an employee of the targeted victim. The attached file usually contained embedded malware designed to allow the conspiracy to gain unauthorized access to the victim computer. The phishing emails were designed to deceive the recipient in order to induce the recipient to activate the malware, such as by opening an attachment or clicking on a link contained in the phishing email. If the recipient unwittingly activated the malware, the computer on which it was opened became infected and provided access to the infected computer to one or more computers controlled by the conspiracy.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Once the conspirators, using wires in interstate and foreign commerce, successfully gained access to the victim computer and obtained valid login credentials, the conspirators gained the ability to connect one or more conspiracy-controlled computers to the victim computer.

e. The conspirators installed additional malware, including password-stealing malware and remote access trojan malware, to obtain and establish administrative and persistent remote control of the victim computer. At times, the conspirators modified antivirus software settings to allow malware to continue to run undetected.

f. The conspirators used the unauthorized access to the victim's computer to conduct additional surveillance of other computer systems located within the victim's computer network. The conspirators used the victim's computer to move laterally within the network, infecting other victim computer systems on the network with malware to gain additional access within the victim computer network. The goal was to locate and steal login credentials for domain administrators of the victim computer network, which would allow the conspiracy to have full administrative control over the victim computer network.

g. The conspirators also at times used the unauthorized access to a victim's computer network to pivot into a separate, specific company's networks, effectively exploiting one victim's existing relationships and connections to compromise its clients, partners, and others.

h. After gaining access to a victim computer network and establishing a level of control and persistence, the conspirators offered the access to the victim computer network for sale, typically through RDP or a "backdoor" created on the victim networks through implanted malware. In marketing the access to prospective buyers, the conspirators often described the degree of access (e.g., partial or full) and administrative control and set a purchase price for the particular network access. The group's asking prices, which were often, but not always, consistent across various forums, generally ranged from thousands to tens of thousands dollars, but in some cases exceed $100,000,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

depending on the victim entity and the degree of system access and controls. With respect to some entities, for instance, those deemed potentially high-value targets (e.g., financial institutions), the group further negotiated a cut, or percentage, of future profits derived by the buyer from use of the purchased unauthorized network access.

i. Typically, the conspirators broadly advertised such unauthorized network access for sale on various underground criminal forums. Since October 2017, group members have offered for sale the unauthorized network access to over 300 distinct victim entities across six continents, including over 30 entities located in the United States. Examples of advertised network access to U.S. entities include:

(i) On about October 12, 2017, ANDREY TURCHIN offered for sale on an online forum network access for numerous entities, including a port authority located in Cowlitz County, Washington ("Victim-1"), a distributor of petroleum products based in Alaska, a law firm based in Colorado, an online money transfer and digital payment services company located in New York, and a software developer located in California, as well as the Ministry of Housing, Utilities and Urban Communities of an African country, an African bank, and a luxury hotel group with locations across Europe, North Africa, Latin America, and the Caribbean.

(ii) On about March 20, 2018, ANDREY TURCHIN offered for sale network access for numerous entities, including a port authority (Victim-1) and a U.S. airline based in New York, as well as the Ministry of Finance of an African country, the Ministry of Mining and Energy of an Asian country, a South Asian media company, and multiple financial services offices. ANDREY TURCHIN further claimed to have access to more than 200 government and law enforcement networks in the United Kingdom, some of which were also advertised for sale.

(iii) On about April 1, 2018, ANDREY TURCHIN offered for sale access to point-of-sale terminals at various restaurants, cafes, retail stores, and other businesses in over a dozen countries, including a company headquartered in Seattle, Washington, and numerous other popular chains with locations in the Western District of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Washington.

(iv) On about July 17, 2018, ANDREY TURCHIN offered for sale network access to two hotel chains, including a U.S. chain that operates hotels throughout the United States, including the Western District in Washington, and abroad.

(v) On about September 5, 2018, "Antony Moricone," "Lampeduza," and "Nikolay" posted on separate online forums near-identical offers for sale of network access to multiple U.S. entities, including computer networks of an U.S. county located in the state of Texas ("Victim-2").

(vi) On about September 9, 2018, "Antony Moricone," "Lampeduza," and "Nikolay" posted on separate online forums similar offers for sale of network access to numerous entities, including an olive oil manufacturing business located in Chico, California, as well as an Asian pharmaceutical and biotechnology company.

(vii) On about September 22, 2018, "Antony Moricone" and "Lampeduza" posted on separate online forums similar offers for sale of network access to the same entities, including a private school located in California, as well as multiple college institutions located in foreign countries, an African power company, and a municipality in a Middle Eastern country.

(viii) On about September 25, 2018, "Antony Moricone," "Lampeduza," and "Nikolay" posted on separate online forums similar offers for sale of network access to a university located in Puerto Rico.

j. At other times, the group members offered such unauthorized network access to particular trusted or established buyer as part of a direct sale. In certain circumstances, the group offered bulk purchase discounts, namely, the bulk sale of access to multiple victims' network in exchange for a discounted price.

k. The group executed transactions through use of a broker service and allowed buyers to effectively sample the network access before finalizing a purchase. More specifically, the potential buyer typically transmitted funds toward the agreed-upon purchase price into escrow arranged by the broker. The group then provided the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

prospective buyer with access for a limited period, e.g., a six-hour window, during which the buyer could test the quality and reliability of the remote access and control established in the victim's protected network. If acceptable, the deal was finalized, whereby the funds were released to the cybercriminal group and the buyer received the conspirators' unrestricted network access.

l. Following a sale, the conspirators typically provided the buyer with ongoing technical assistance with respect to purchased network access for a negotiated period of time.

m. The conspirators took various steps to obfuscate their identity and location. For instance, cybercriminal group members typically used monikers and communicated with one another and with prospective customers through Jabber, a web-based instant messaging service that allows for person-to-person and group communication across multiple platforms and that supports end-to-end encryption. The group members further often used Tor and other tools and methods to obscure the web traffic and in turn their location and identity. The group members also made efforts to conceal the flow of funds through use of cryptocurrency, such as Bitcoin, in various financial transactions.

F. Overt Acts

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

a. On about October 1, 2017, ANDREY TURCHIN started a thread on a prominent Russian-language online forum commonly used by hackers and cybercriminals. ANDREY TURCHIN claimed the ability to sell access to various corporate networks, servers, and their administrative accounts.

b. On about October 1, 2017, one or more co-conspirators remotely accessed without authorization the protected computer network of a port authority

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(Victim-1) located in the Western District of Washington.

c. On about October 12, 2017, one or more co-conspirators remotely accessed the protected computer network of the port authority (Victim-1).

d. On about October 12, 2017, ANDREY TURCHIN, on an online forum, posted for sale network access to numerous entities in multiple countries, including the port authority (Victim-1).

e. On about November 14, 2017, a co-conspirator registered a Google account (@gmail.com), using the alias "Ivan Ivanov" and other inaccurate information from an IP address resolving to a foreign country.

f. On about November 15, 2017, a co-conspirator, using the alias "Ivan Ivanov" and the aforementioned Google account, registered a domain with a U.S.-based service provider, paid for through one or more cryptocurrency transfers. One or more co-conspirators then used this domain to register and establish one or more of the IP addresses used to access the protected network of the port authority (Victim-1).

g. On about November 19, 2017, one or more co-conspirators remotely accessed the protected computer network of the port authority (Victim-1).

h. On about December 23, 2017, a co-conspirator accessed an administrative account on protected computer network of the port authority (Victim-1) through an IP address that resolved to Kazakhstan.

i. On about December 23, 2017, ANDREY TURCHIN, on an online forum, posted for sale network access to numerous entities in multiple countries, including full network access to the port authority (Victim-1).

j. On about January 10, 2018, one or more co-conspirators remotely accessed the protected computer network of the port authority (Victim-1).

k. On about April 1, 2018, ANDREY TURCHIN, on an online forum, posted for sale, access to point-of-sale terminals at various restaurants, cafes, retail stores, and other businesses, including a company headquartered in Seattle, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

l. On about September 30, 2018, "Nikolay," on an online forum, posted that access to a U.S. county in Texas (Victim-2) had been sold for $150,000.

m. On about October 22, 2018, "Antony Moricone" and "Lampeduza," on separate online forums, posted for sale network access to the numerous entities, including the Ministry of Finance of an African country previously advertised by "fxmsp."

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

COUNT 2

(Unauthorized Access to a Protected Computer)

18. The allegations set forth in Paragraphs 1 through 17 of this Indictment are re-alleged and incorporated as if fully set forth herein.

19. Beginning on or about October 1, 2017, and continuing until a date unknown, in Cowlitz County, within the Western District of Washington, and elsewhere, the defendant, ANDREY TURCHIN, and others known and unknown to the Grand Jury, intentionally accessed a computer without authorization, and exceeded authorized access to a computer, and thereby obtained information from a protected computer, specifically, one or more protected computers of an entity, Victim-1, referenced above, and (i) the offense was committed for purposes of commercial advantage or private financial gain, (ii) the offense was committed in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States and the laws of Washington, and (iii) the value of the information obtained exceeded $5,000.

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

COUNT 3

(Intentional Damage to a Protected Computer)

20. The allegations set forth in Paragraphs 1 through 17 of this Indictment are re-alleged and incorporated as if fully set forth herein.

21. Beginning on or about October 1, 2017, and continuing until a date unknown, in Cowlitz County, within the Western District of Washington, and elsewhere,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the defendant, ANDREY TURCHIN, 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, one or more protected computers of an entity, Victim-1, referenced above, 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.

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

COUNT 4

(Conspiracy to Commit Wire Fraud)

22. The allegations set forth in Paragraphs 1 through 17 of this Indictment are re-alleged and incorporated as if fully set forth herein.

23. Beginning at a time unknown, but no later than October 2017, and continuing through on or about December 12, 2018, within the Western District of Washington, and elsewhere, the defendant, ANDREY TURCHIN, 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: 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.

24. The objectives of the conspiracy included gaining increasing levels of access to, and control of, protected computers of victim entities through the use of deception and false representations and fraudulently obtained credentials. The objectives of the conspiracy further included, using such access and control obtained through deceptive

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

means, to compromise additional computers and networks both internally and externally to the victim entity. The ultimate purpose of the conspiracy involved the selling of access to victim computer networks to other cybercriminal actors for financial gain.

25. The manner and means used to accomplish the conspiracy are forth in Paragraph 16, above, which is incorporated herein, and included the following:

a. The conspirators, using wires in interstate and foreign commerce, gained unauthorized access to a computer through hacking techniques, all of which involved deceptive acts. At times, group members employed brute force attacks, which, when successful, involved the false representation that the hacker was an authorized person, such as an employee. Alternatively, group members at times employed phishing campaigns, which involved false representations to induce the recipient to unwittingly activate malware and infect the computer.

b. Once the conspirators successfully gained access to the victim computer, the actor located and stole valid login credentials, which in turn were used to gain further access to and control of the victim's network through false representations, with the goal of establishing undetected persistence.

c. Thereafter, the conspirators offered the access to the victim computer network for sale, typically through advertisement postings or through direct sales on various online forums. As part of any sale, the group provided buyers with stolen victim credentials, which enabled the purchaser to access the victim networks and the ability to deploy additional malware for the purchaser's designs and purposes, thereby exposing the victim, as well as its employees, customers, and business partners, to a wide spectrum of illicit conduct.

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

COUNT 5

(Access Device Fraud)

26. The allegations set forth in Paragraphs 1 through 17 of this Indictment are re-alleged and incorporated as if fully set forth herein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. On or about December 23, 2017, in Cowlitz County, within the Western District of Washington, and elsewhere, the defendant, ANDREY TURCHIN, and others known and unknown to the Grand Jury, knowingly and with intent to defraud, used and trafficked in unauthorized access devices, specifically, account usernames and passwords for Victim-1, and other means of account access that can be used, alone and in conjunction with another access device, to obtain a thing of value, and by such conduct, obtained information with a value aggregating $1,000 or more during a one-year period; said activity affecting interstate and foreign commerce

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

FORFEITURE ALLEGATION

28. The allegations contained in Count 1 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), 981(a)(1)(C), and 1030(i) and Title 28, United States Code, Section 2461(c). Upon conviction of the offense charged in Count 1, 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 the offense, including but not limited to a sum of money reflecting those proceeds, as well as his interest any personal property that was used or intended to be used to commit or to facilitate the commission of the offense.

29. The allegations contained in Counts 2 and 3 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 offense charged in Counts 2 and 3, 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 the offense including but not limited to a sum of money reflecting those proceeds, as well as his interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offense.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

30. The allegations contained in Count 4 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 the offense charged in Count 4, the defendant shall forfeit to the United States any property, real or personal, constituting, or derived from, proceeds the defendant obtained, directly or indirectly, as the result of the offense, including but not limited to a sum of money reflecting those proceeds.

31. The allegations contained in Count 5 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 1029(c)(1)(C). Upon conviction of the offense charged in Count 5, the defendant shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such offense, including but not limited to a sum of money reflecting those proceeds, as well as his interest in any property used or intended to be used to commit the offense.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

32. 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,

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

A TRUE BILL:

DATED: 12-12-2018

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

FOREPERSON

ANNETTE L. HAYES
United States Attorney

ANDREW C. FRIEDMAN
Assistant United States Attorney

STEVEN T. MASADA
Assistant United States Attorney

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970