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 23, 2021

WILLIAM M. McCOOL, Clerk

By Stefanie Rather Deputy

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

UNITED STATES OF AMERICA, Plaintiff v. GABRIEL KIMIAIE-ASADI BILDSTEIN, a/k/a, "Kuroi," a/k/a, "Gnostic Players," SEBASTIEN RAOULT, a/k/a, "Sezyo Kaizen," ABDEL-HAKIM EL AHMADI, a/k/a, "Zac," a/k/a, "Jordan Keso," Defendants.	NO. CR21-109 RSL **INDICTMENT**

The Grand Jury charges that:

COUNT 1

(Conspiracy to Commit Computer Fraud and Abuse)

A. Overview

1. The defendant, GABRIEL KIMIAIE-ASADI BILDSTEIN ("BILDSTEIN"), known by various monikers, such as "Kuroi" and "Gnostic Players,"

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

among others, is a French national who, during the time period described herein, resided in or around Tarbes, France.

2. The defendant, SEBASTIEN RAOULT ("RAOULT"), known by various monikers, such as "Sezyo Kaizen," among others, is a French national who, during the time period described herein, resided in or around Epinal, France.

3. The defendant, ABDEL-HAKIM EL AHMADI ("EL AHMADI"), known by various monikers, such as "Zac" and "Jordan Keso," among others, is a French national who, during the time period described herein, resided in or around Lyon, France.

4. BILDSTEIN, RAOULT, and EL AHMADI are members of a group of financially motivated cybercriminal actors commonly referred to as "ShinyHunters" (or "Shiny Hunters"). This cybercriminal group (hereinafter "ShinyHunters Group") has engaged in the hacking of protected computers of corporate entities and the theft of confidential and proprietary information. The ShinyHunters Group has deployed targeted phishing email campaigns designed to deceive and dupe recipients into disclosing login credentials and access keys, and to gain access to company accounts, networks, and infrastructure. The ShinyHunters Group used such unauthorized access to locate and steal internal corporate files and information of value, including customer records, source code and internal user data.

5. The ShinyHunters Group then advertised such sensitive data for sale on various underground dark web forums and, in some cases, solicited ransom payments from its hacking victims by threatening to leak or sell stolen sensitive files. Since early 2020, the ShinyHunters Group has marketed and promoted hacked data from more than 60 companies located in the United States, including the Western District of Washington, and multiple other countries.

B. Offense

6. Beginning at a time unknown, but no later than in or about November 2019, and continuing to in or about June 2021, in King County, within the Western District of Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and EL AHMADI,

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

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 computers without authorization, and thereby obtain information from protected computers, and further to commit the offense for purposes of commercial advantage and private financial gain, to commit the offense 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 the State of Washington, and to obtain information with a value exceeding $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B); and

b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused loss to one or more persons during a 1-year period aggregating at least $5,000 in value and the offense caused 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).

C. Objects of the Conspiracy

7. The objects of the conspiracy included, through use of deceptive and fraudulent means, gaining access to protected computers without authorization and to the data stored thereon. The objects of the conspiracy also included stealing proprietary source code, sensitive databases and information, including personal and financial information, and other confidential files, with the purpose and intent to monetize such non-public material and deprive victims of the exclusive control and ownership of their property. The objects of the conspiracy further included obtaining money and things of value through use of the unauthorized access and control of victim computer networks and through use of the stolen victim data.

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

D. Manner and Means of the Conspiracy

8. The manner and means used to accomplish the conspiracy included, among other things, the following:

a. BILDSTEIN, RAOULT, and EL AHMADI, and others, knowingly and falsely registered domains with hosting services using false names and addresses, including domain names designed to spoof the actual domains of legitimate service providers used by software developers, technology companies, and other employees of business entities. Examples of legitimate service providers spoofed by the ShinyHunters Group include:

(i) "Provider-1": A U.S.-based computer code hosting and development platform used for software development and version control using "git" that offers users, among other things, distributed version control and collaboration features.

(ii) "Provider-2": A U.S.-based proprietary business communication platform that offers users the ability to create and maintain chat rooms organized by topic, private groups, and direct messaging.

(iii) "Provider-3": A U.S.-based cloud computing service provider that offers remote hosting and processing services.

b. BILDSTEIN, RAOULT, and EL AHMADI, and others, using the spoofed domains, created websites designed to replicate and spoof login pages of legitimate service providers, such as Provider-1, with the intent and purpose of capturing and stealing authentic user data and credentials, including usernames and passwords, entered by unwitting account holders.

c. BILDSTEIN, RAOULT, and EL AHMADI, and others, used a variety of specially designed scripts and Internet-based tools to search for, identify, and gather contact information for particular company employees and contractors, often software developers, information technology (IT) personnel, and others to access source code and git repositories.

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

d. BILDSTEIN, RAOULT, and EL AHMADI, and others, created and sent phishing emails designed to replicate and spoof communications from legitimate service providers, often purporting to relate to account activity or notifications, with the intent and purpose of inducing recipients to click on embedded links supposedly directing the recipient to the login page of the service provider. In actuality, the embedded links in the phishing emails directed the recipient to one or more of the spoofed login pages hosted on a malicious domain to capture and steal authentic login credentials.

e. BILDSTEIN, RAOULT, and EL AHMADI, and others, used stolen account credentials to access legitimate accounts of others, without authorization, and executed steps to maintain account access (i.e., persistence). For instance, in some cases, the ShinyHunters Group changed account settings and password information and, in some cases, deployed a series of tools and features to bypass password logins altogether.

f. BILDSTEIN, RAOULT, and EL AHMADI, and others, accessed protected computers, including "git" and source code repositories as well as internal infrastructure, through use of stolen access keys, credentials and other exploits. In doing so, the ShinyHunters Group falsely and fraudulently represented that they had authorization to use legitimate access keys and credentials and to access the protected computers and the data stored thereon, when in fact they lacked authorization to do so.

g. BILDSTEIN, RAOULT, and EL AHMADI, and others, copied and cloned data accessible through the compromised accounts, which included, among other things, private "git" repositories, proprietary software source code, internal files and communications, and additional access keys and credentials.

h. BILDSTEIN, RAOULT, and EL AHMADI, and others, scanned stolen code, files, and internal information for credentials and embedded access keys used to interact with a company's network and cloud infrastructure service provider.

i. BILDSTEIN, RAOULT, and EL AHMADI, and others, used stolen credentials and access keys to further access, without authorization, companies' networks and cloud infrastructure, to survey the hosted data, and to copy and clone particular files

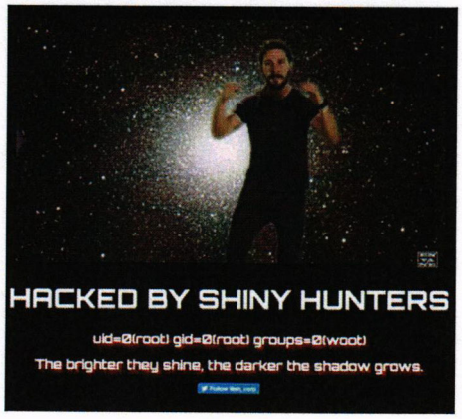
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and information, including, but not limited to, customer databases and personal and financial information.

j. BILDSTEIN, RAOULT, and EL AHMADI, and others, maintained accounts on multiple dark web marketplaces and forums, such as RaidForums and EmpireMarket, known to cater to cybercriminals and illegal activity, through which the ShinyHunters Group offered, advertised, and posted hacked data for sale, including customer databases and personal and financial information.

k. BILDSTEIN, RAOULT, and EL AHMADI, and others, at times contacted victimized companies directly and threatened to sell or leak the companies' hacked data unless a monetary payment or ransom, often in the form of cryptocurrency, was immediately paid.

l. BILDSTEIN, RAOULT, and EL AHMADI, and others, operated social media accounts to promote the ShinyHunters Group and its activities, drive traffic to the dark web marketplaces and forums, and facilitate the sale of hacked data to prospective and actual buyers. The ShinyHunters Group, at times, also publicly leaked samples of hacked data, communicated with media outlets, and, on occasion, used the access to a company's network to deface and electronically vandalize the company's website, which can be accomplished by redirecting Internet traffic to an alternative external domain controlled by cybercriminal actors. An example of a website defacement conducted by the ShinyHunters Group is set forth below:



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

Such conduct was designed to, among other things, promote the ShinyHunter Group's notoriety, substantiate the group's hacking ability and the authenticity of the hacked data, and in turn to facilitate monetization, whether through sales or ransom payments.

m. BILDSTEIN, RAOULT, and EL AHMADI, and others, at times, used the access to a company's network and cloud infrastructure to, without authorization, install and run implanted malicious software (or malware) designed to secretly mine cryptocurrency using the company's computing power and resources, a cyberattack commonly referred to as "cryptojacking." The act of mining cryptocurrency, is the use of computing power to verify cryptocurrency transactions of others, which generates payments, typically in the form of cryptocurrency, to the "miner."

E. Overt Acts

9. In furtherance of the conspiracy, and to achieve the objects thereof, the defendants, BILDSTEIN, RAOULT, and EL AHMADI, 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 or about January 12, 2020, the ShinyHunters Group registered an account on the social media platform Twitter, with the username "sh_corp" and display name "Shiny Hunters." On multiple occasions thereafter, this account was used to post (or "tweet") and to communicate regarding the hacking activity of the ShinyHunters Group.

b. On or about January 25, 2020, the ShinyHunters Group registered an account with the username "ShinyHunters" on the underground forum site EmpireMarket. The account, among others, was used to advertise and sell victim data obtained through hacking activity.

c. On various dates, the ShinyHunters Group opened and used accounts at various domain registrars, submitting false subscriber information, and registered dozens of malicious domains, including more than 36 resembling or incorporating the

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

name of Provider-1. Examples of such conduct include, but are not limited to, the following:

(i) On or about March 30, 2020, the ShinyHunters Group registered one or more domains designed to spoof Provider-1 and Provider-3.

(ii) On or about March 31, 2020, the ShinyHunters Group registered a domain designed to spoof Provider-1.

(iii) On or about April 1, 2020, the ShinyHunters Group registered a domain designed to spoof Provider-2. The following day, the same domain registrar account was used to register a domain designed to spoof Provider-1.

(iv) On or about April 8, 2020, the ShinyHunters Group registered a domain designed to spoof Provider-1.

(v) On or about June 16, 2020, the ShinyHunters Group registered a domain designed to spoof Provider-1.

d. On various dates, the ShinyHunters Group communicated and collaborated to develop aspects of the phishing campaign, malware, and hacking efforts targeting victims. Examples of such conduct include the following:[1]

(i) On or about April 1, 2020, BILDSTEIN, RAOULT, and EL AHMADI, and others, over a communication platform, shared information related to the phishing campaign, including recently created malicious domains designed to spoof Provider-1.

(ii) On or about April 3, 2020, RAOULT and EL AHMADI used accounts hosted at Provider-1 to access multiple malicious domains in an apparent effort to develop and test aspects of the phishing campaign.

(iii) On or about August 14, 2020, RAOULT and another individual, over a communication platform, discussed the recent hack of a U.S. company

[1] The ShinyHunters Group members communicated predominantly in French. Summarized and quoted communications described herein were translated to English.

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

and the possibility of identifying a buyer of the hacked data.

(iv) On or about November 12, 2020, RAOULT, over a communication platform, shared a copy of an archive file containing scripts designed to steal user data from compromised Provider-1 accounts and search for access keys for infrastructure hosted at Provider-3.

e. On or about May 27, 2020, the ShinyHunters Group posted on RaidForums a list of over 20 company databases currently available for sale, along with the message: "here is the list of databases that we put on sale for the moment (We only sell what we've dumped ourselves)."

f. Over the course of numerous months, the ShinyHunters Group targeted corporate entities with a sophisticated phishing campaign, which enabled the ShinyHunters Group to gain access, without authorization, to accounts and data maintain at various service providers, including Provider-1, Provider-2, and Provider-3. Illustrative examples of the ShinyHunters Group's victims include, but are not limited to, the following:

(i) "Victim-1," a technology company headquartered in the Western District of Washington: On or about March 28, 2020, and March 29, 2020, the ShinyHunters Group sent phishing email messages to a software engineer, located in or around Bellevue, Washington, employed by Victim-1. The ShinyHunters Group used stolen credentials to access the Provider-1 account of an employee of Victim-1 and cloned private Victim-1 code repositories. BILDSTEIN and EL AHMADI discussed the hack of Victim-1 and theft of hundreds of private repositories over a communication platform. The ShinyHunters Group publicly claimed to have stolen a large amount of Victim-1 source code and published a sample thereof.

(ii) "Victim-2," a U.S.-based media and entertainment company: On or about April 9, 2020, the ShinyHunters Group sent a phishing email message to an employee of Victim-2. The ShinyHunters Group used stolen credentials to access the

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

Provider-1 account of an employee of Victim-2 and cloned private Victim-2 code repositories.

(iii) "Victim-3," a management and communication platform provider, based in the Western District of Washington: On or about April 29, 2020, ShinyHunters Group used stolen credentials to access the Provider-1 account of an employee of Victim-3 and cloned private Victim-3 code repositories. The ShinyHunters Group also used stolen access keys to access Victim-3's network, hosted on Provider-3, and cloned multiple databases, including customer files and information. The ShinyHunters Group later offered stolen Victim-3 databases for sale.

(iv) "Victim-4," a foreign e-commerce company: In about March 2020, the ShinyHunters Group compromised the cloud infrastructure of Victim-4 and cloned numerous internal databases, including customer files and information. On or about May 1, 2020, the ShinyHunters Group posted for sale stolen Victim-4 databases, including millions of customer records. BILDSTEIN and EL AHMADI, over a communication platform, discussed the hack of Victim-4 and the sale of stolen data, in which EL AHMADI questioned BILDSTEIN about selling Victim-4 without telling him.

(v) "Victim-5," a U.S.-based clothing and apparel company: On or about June 19, 2020, and on dates thereafter, the ShinyHunters Group used stolen credentials to access the Provider-1 account of an employee of Victim-5 and cloned private Victim-5 code repositories. The ShinyHunters Group later published stolen databases of Victim-5. RAOULT and another individual, over a communication platform, discussed the decision to leak, rather than sell, Victim-5 data.

(vi) "Victim-6," a U.S.-based diet and fitness company: On or about August 14, 2020, the ShinyHunters Group used stolen credentials to access the Provider-1 account of an employee of Victim-6 and cloned private Victim-6 code repositories. RAOULT and another individual, over a communication platform, discussed the hack of Victim-6 and the possible profit ("good booty") from the theft and sale of Victim-6's customer data.

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

(vii) "Victim-7," a U.S.-based video game developer: On or about October 12, 2020, the ShinyHunters Group used stolen credentials to access the Provider-1 account of an employee of Victim-7 and cloned private Victim-7 code repositories. On the same date, and thereafter, the ShinyHunters Group used stolen access keys and other information to further access, without authorization, Victim-7's network hosted on Provider-3 cloud infrastructure and cloned data stored thereon. The ShinyHunters Group later published Victim-7's stolen data, which included millions of user records.

(viii) "Victim-8," a foreign-based stock trading platform: On or about March 30, 2021, the ShinyHunters Group compromised a cloud storage account of Victim-8 and cloned private Victim-8 code repositories, including customer records. The ShinyHunters Group offered Victim-8's data for sale and further contacted Victim-8, by email, threatening to sell or leak Victim-8's databases unless Victim-8 paid the group an amount of money in virtual currency Bitcoin (BTC) or Monero (XMR).

All in violation of Title 18, United States Code, Sections 371 and 3559(g)(1).

COUNT 2

(Conspiracy to Commit Wire Fraud)

10. The allegations set forth in Paragraphs 1 through 5 and 7 through 9 of this Indictment are re-alleged and incorporated as if fully set forth herein.

A. Offense

11. Beginning at a time unknown, but no later than in or about November 2019, and continuing to in or about June 2021, in King County, within the Western District of Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and EL AHMADI, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree together to commit an offense 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

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

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. Objects of the Conspiracy

12. The objects of the conspiracy are set forth in Paragraph 7 of this Indictment and are re-alleged and incorporated as if fully set forth herein.

13. The objects of the conspiracy further included the use of malicious emails, domains, and websites to trick legitimate account holders to disclose their personal login credentials and other information. The objects of the conspiracy further included using those credentials and information, including by falsely representing that the conspirators were the authorized users of those credentials and information, to obtain property, such as proprietary source code, sensitive databases and information, including personal and financial information, and other confidential files, with the purpose and intent to monetize such non-public material and deprive victims of the exclusive control and ownership of their property.

C. Manner and Means of the Conspiracy

14. The manner and means used to accomplish the conspiracy are forth in Paragraph 8 of this Indictment and are re-alleged and incorporated as if fully set forth herein.

All in violation of Title 18, United States Code, Sections 1349 and 3559(g)(1).

COUNTS 3 - 6

(Wire Fraud)

15. The allegations set forth in Paragraphs 1 through 5, 7 through 9, and 13 of this Indictment are re-alleged and incorporated as if fully set forth herein.

A. Scheme and Artifice to Defraud

16. Beginning at a time unknown, but no later than in or about November 2019, and continuing to in or about June 2021, in King County, within the Western District of

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

Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and EL AHMADI, 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.

B. Essence of the Scheme

17. The essence of the scheme and artifice to defraud is set forth in Paragraph 7 of this Indictment and are re-alleged and incorporated as if fully set forth herein.

C. Manner and Means

18. The manner and means of the scheme and artifice to defraud are set forth in Paragraph 8 of this Indictment and are re-alleged and incorporated as if fully set forth herein.

D. Execution of the Scheme and Artifice to Defraud

19. On or about the dates set forth below, in King County, within the Western District of Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and EL AHMADI, 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, each of which constitutes a separate count of this Indictment:

Count	Date(s)	Wire Transmission
3	March 28, 2020	Email message purporting to be from Provider-1 to an employee of Victim-1, received in the Western District of Washington from outside the State of Washington
4	March 28, 2020	Connection to a domain by an employee of Victim-1, located in the Western District of Washington, which transmitted an electronic signal to a device located outside the State of Washington

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

Count	Date(s)	Wire Transmission
5	March 29, 2020	Email message purporting to be from Provider-1 to an employee of Victim-1, received in the Western District of Washington from outside the State of Washington
6	March 29, 2020	Connection to a domain by an employee of Victim-1, located in the Western District of Washington, which transmitted an electronic signal to a device located outside the State of Washington

20. The grand jury alleges that these crimes were committed during, and in furtherance of, the Conspiracy charged in Count 2.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS 7 - 9

(Aggravated Identity Theft)

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

22. On or about the dates listed below, in King County, within the Western District of Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and EL AHMADI, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, a real person, as described below, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, as charged in Count 2, and wire fraud, in violation of 18 U.S.C. § 1343, as charged in Counts 3 through 6, knowing that the means of identification belonged to another actual person.

Count	Date(s)	Means of Identification
7	March 28, 2020	Login credentials of a contract employee of Victim-1, initials P.K., a real person
8	April 9, 2020	Login credentials of an employee of Victim-2, initials R.M., a real person
9	April 29, 2020	Login credentials of an employee of Victim-3, initials J.M., a real person

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

23. The grand jury alleges that these crimes were committed during, and in furtherance of, the Conspiracy charged in Count 2.

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

FORFEITURE ALLEGATION

24. All of the allegations contained in this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture.

25. Upon conviction of the offense charged in Count 1, each of the relevant defendants shall forfeit to the United States any property that constitutes or is traceable to proceeds the defendant obtained from the commission of the offense, including but not limited to a sum of money reflecting the proceeds the relevant defendant obtained from the offense. All such property is forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C) (by way of Title 28, United States Code, Section 2461(c)).

26. Upon conviction of any of the offenses charged in Counts 2 through 6, each of the relevant defendants 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 sum of money representing the proceeds the relevant defendant obtained from the offense. All such property is forfeitable pursuant to pursuant to Title 18, United States Code, Section 981(a)(1)(C) (by way of Title 28, United States Code, Section 2461(c)).

(Substitute Assets)

27. 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,

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

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: 6/23/2021

Signature of Foreperson redacted pursuant to the policy of the Judicial Conference of the United States.

FOREPERSON

TESSA M. GORMAN
Acting 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