

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 Stephan Kratter Deputy

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

UNITED STATES OF AMERICA, Plaintiff

NO. CR21-109 RSL

INDICTMENT

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.

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,"

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

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

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

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

19 5. The ShinyHunters Group then advertised such sensitive data for sale on
20 various underground dark web forums and, in some cases, solicited ransom payments
21 from its hacking victims by threatening to leak or sell stolen sensitive files. Since early
22 2020, the ShinyHunters Group has marketed and promoted hacked data from more than
23 60 companies located in the United States, including the Western District of Washington,
24 and multiple other countries.

25 **B. Offense**

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

1 and others known and unknown to the Grand Jury, did knowingly and willfully combine,
2 conspire, confederate and agree together to commit offenses against the United States, to
3 wit:

4 a. to intentionally access computers without authorization, and thereby
5 obtain information from protected computers, and further to commit the offense for
6 purposes of commercial advantage and private financial gain, to commit the offense in
7 furtherance of a criminal and tortious act in violation of the Constitution and the laws of
8 the United States and the laws of a state, including the State of Washington, and to obtain
9 information with a value exceeding \$5,000, in violation of Title 18, United States Code,
10 Sections 1030(a)(2)(C) and (c)(2)(B); and

11 b. to knowingly cause the transmission of a program, information,
12 code, and command, and as a result of such conduct, intentionally cause damage without
13 authorization to a protected computer, and the offense caused loss to one or more persons
14 during a 1-year period aggregating at least \$5,000 in value and the offense caused
15 damage affecting 10 or more protected computers during a 1-year period, in violation of
16 Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B).

17 **C. Objects of the Conspiracy**

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

1 **D. Manner and Means of the Conspiracy**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

11 **E. Overt Acts**

12 9. In furtherance of the conspiracy, and to achieve the objects thereof, the
13 defendants, BILDSTEIN, RAOULT, and EL AHMADI, and others known and unknown
14 to the Grand Jury, did commit and cause to be committed the following overt acts, among
15 others, in the Western District of Washington and elsewhere:

16 a. On or about January 12, 2020, the ShinyHunters Group registered an
17 account on the social media platform Twitter, with the username "sh_corp" and display
18 name "Shiny Hunters." On multiple occasions thereafter, this account was used to post
19 (or "tweet") and to communicate regarding the hacking activity of the ShinyHunters
20 Group.

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

25 c. On various dates, the ShinyHunters Group opened and used accounts
26 at various domain registrars, submitting false subscriber information, and registered
27 dozens of malicious domains, including more than 36 resembling or incorporating the
28

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

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

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

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

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

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

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

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

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

24 (iii) On or about August 14, 2020, RAOULT and another
25 individual, over a communication platform, discussed the recent hack of a U.S. company
26

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

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

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

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

10 f. Over the course of numerous months, the ShinyHunters Group
11 targeted corporate entities with a sophisticated phishing campaign, which enabled the
12 ShinyHunters Group to gain access, without authorization, to accounts and data maintain
13 at various service providers, including Provider-1, Provider-2, and Provider-3.

14 Illustrative examples of the ShinyHunters Group’s victims include, but are not limited to,
15 the following:

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

25 (ii) “Victim-2,” a U.S.-based media and entertainment company:
26 On or about April 9, 2020, the ShinyHunters Group sent a phishing email message to an
27 employee of Victim-2. The ShinyHunters Group used stolen credentials to access the
28

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

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

10 (iv) "Victim-4," a foreign e-commerce company: In about March
11 2020, the ShinyHunters Group compromised the cloud infrastructure of Victim-4 and
12 cloned numerous internal databases, including customer files and information. On or
13 about May 1, 2020, the ShinyHunters Group posted for sale stolen Victim-4 databases,
14 including millions of customer records. BILDSTEIN and EL AHMADI, over a
15 communication platform, discussed the hack of Victim-4 and the sale of stolen data, in
16 which EL AHMADI questioned BILDSTEIN about selling Victim-4 without telling him.

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

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

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

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

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

16 **COUNT 2**

17 **(Conspiracy to Commit Wire Fraud)**

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

20 **A. Offense**

21 11. Beginning at a time unknown, but no later than in or about November 2019,
22 and continuing to in or about June 2021, in King County, within the Western District of
23 Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and EL AHMADI,
24 and others known and unknown to the Grand Jury, did knowingly and willfully combine,
25 conspire, confederate and agree together to commit an offense against the United States,
26 to wit: to knowingly and willfully devise and execute and attempt to execute, a scheme
27 and artifice to defraud, and for obtaining money and property by means of materially
28 false and fraudulent pretenses, representations, and promises; and in executing and

1 attempting to execute this scheme and artifice, to knowingly cause to be transmitted in
2 interstate and foreign commerce, by means of wire communication, certain signs, signals
3 and sounds as further described below, in violation of Title 18, United States Code,
4 Section 1343.

5 **B. Objects of the Conspiracy**

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

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

17 **C. Manner and Means of the Conspiracy**

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

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

22 **COUNTS 3 - 6**

23 **(Wire Fraud)**

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

26 **A. Scheme and Artifice to Defraud**

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

Indictment - 12

United States v. Bildstein, et al.

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

1 Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and EL AHMADI,
 2 and others known and unknown to the Grand Jury, devised and intended to devise a
 3 scheme and artifice to defraud and to obtain money and property by means of materially
 4 false and fraudulent pretenses, representations and promises.

5 **B. Essence of the Scheme**

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

8 **C. Manner and Means**

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

12 **D. Execution of the Scheme and Artifice to Defraud**

13 19. On or about the dates set forth below, in King County, within the Western
 14 District of Washington, and elsewhere, the defendants, BILDSTEIN, RAOULT, and
 15 EL AHMADI, and others known and unknown to the Grand Jury, having devised a
 16 scheme and artifice to defraud, and to obtain money and property by means of materially
 17 false and fraudulent pretenses, representations, and promises, did knowingly transmit and
 18 cause to be transmitted writings, signs, signals, pictures, and sounds, for the purpose of
 19 executing such scheme, by means of wire communication in interstate and foreign
 20 commerce, including the following transmissions, each of which constitutes a separate
 21 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

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

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

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

4 **FORFEITURE ALLEGATION**

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

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

13 26. Upon conviction of any of the offenses charged in Counts 2 through 6, each
14 of the relevant defendants shall forfeit to the United States any property, real or personal,
15 which constitutes or is derived from proceeds traceable to such offenses, including but
16 not limited to a sum of money representing the proceeds the relevant defendant obtained
17 from the offense. All such property is forfeitable pursuant to Title 18, United
18 States Code, Section 981(a)(1)(C) (by way of Title 28, United States Code, Section
19 2461(c)).

20 ***(Substitute Assets)***

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

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

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

4 A TRUE BILL:

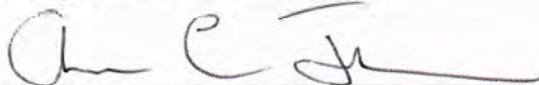
5
6 DATED: 6/23/2021

7 *Signature of Foreperson redacted pursuant*
8 *to the policy of the Judicial Conference of*
9 *the United States.*

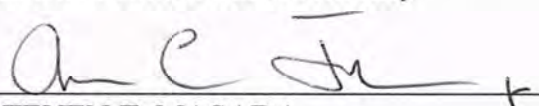
10 _____
11 FOREPERSON

12
13 

14 TESSA M. GORMAN
15 Acting United States Attorney

16 

17 ANDREW C. FRIEDMAN
18 Assistant United States Attorney

19 

20 STEVEN T. MASADA
21 Assistant United States Attorney