

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

January 12, 2022

RAVI SUBRAMANIAN, Clerk

By  Deputy

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

UNITED STATES OF AMERICA,

Plaintiff

v.

JOHN ERIN BINNS,  
a/k/a, "Irdev,"  
a/k/a, "IntelSecrets,"  
a/k/a, "V0rtex,"  
a/k/a, "SubVirt,"

Defendant.

NO. CR22-004 LK

INDICTMENT

The Grand Jury charges that:

**COUNT 1**

**(Conspiracy to Commit Computer Fraud and Abuse)**

**A. Overview**

1. The defendant, JOHN ERIN BINNS ("BINNS"), known by various monikers, such as "Irdev," "IntelSecrets," "V0rtex," and "SubVirt," among others, is a United States citizen who, during the relevant time period described herein, resided in the Republic of Turkey.

2. BINNS, with the assistance of others, known and unknown to the Grand Jury, successfully hacked the protected computers and networks of T-Mobile US, Inc.

1 (“T-Mobile”), a telecommunications company and wireless network operator  
2 headquartered in the Western District of Washington. BINNS, using such unauthorized  
3 network access, stole confidential and sensitive information and other data of value,  
4 including, but not limited to, personally identifiable information (PII) of more than  
5 40 million current, prospective, and former T-Mobile customers, which BINNS offered for  
6 sale and did sell on the dark web.

7 **B. Offense**

8 3. Beginning at a time unknown, but no later than in or about December 2020,  
9 and continuing to the present, in King County, within the Western District of Washington,  
10 and elsewhere, JOHN ERIN BINNS, and others known and unknown to the Grand Jury,  
11 did knowingly and willfully combine, conspire, confederate and agree together to commit  
12 offenses against the United States, to wit:

13 a. to intentionally access computers without authorization, and thereby  
14 obtain information from protected computers, and further to commit the offense for  
15 purposes of private financial gain, and to obtain information with a value exceeding  
16 \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B);  
17 and

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

24 **C. Objects of the Conspiracy**

25 4. The objects of the conspiracy included, through use of deceptive and  
26 fraudulent means, gaining access to protected computers and networks without  
27 authorization and to the data stored thereon. The objects of the conspiracy included  
28 planting malware on the protected computers, and stealing sensitive databases and



1 information, including personal identifiable information (PII) of real persons, and other  
2 confidential files, with the purpose and intent to monetize such non-public material by  
3 obtaining money and things of value, including sums of cryptocurrency, through sale and  
4 further to deprive victims of the exclusive control and ownership of their property.

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

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

8 a. BINNS, from a foreign country, used specially-designed scripts to  
9 scan Internet Protocol (“IP”) addresses belonging to T-Mobile for potential vulnerabilities  
10 and points of unauthorized access to T-Mobile’s protected computers and networks.

11 b. BINNS gained access to T-Mobile’s Bellevue Lab Environment  
12 servers (“Bellevue Lab”), located in the Western District of Washington, by fraudulently  
13 emulating a valid subscriber, related to a particular system tool, and falsely presenting his  
14 access as authentic and authorized.

15 c. BINNS conducted reconnaissance and network scanning and deployed  
16 password-spraying scripts that attempted authentication with username and password pairs.

17 d. BINNS installed a backdoor on the Bellevue Lab and deployed  
18 malicious software (malware) capable of performing system surveys, file transfers,  
19 command execution, file system operations, and tunneling.

20 e. BINNS used stolen passwords and credentials to traverse T-Mobile’s  
21 protected computers and networks and further access, without authorization, additional  
22 server groups located throughout the United States and elsewhere.

23 f. BINNS conducted queries across T-Mobile’s protected computers and  
24 networks, including using names and other information of known associates of BINNS.

25 g. BINNS searched for and located items of potential value, including  
26 databases and information related to current, former, and prospective T-Mobile customers,  
27 which BINNS packaged into output data files.

1 h. BINNS thereafter transferred the packaged data files to the Bellevue  
2 Lab, from which BINNS transferred the packaged data files from T-Mobile's protected  
3 computers and networks to an external location in a foreign country.

4 i. BINNS executed scripts to delete original data from T-Mobile's  
5 protected computers and networks.

6 j. BINNS operated one or more accounts on the underground dark web  
7 forum RaidForums, a popular marketplace and database-sharing site frequented by  
8 cybercriminals used to promote data leaks and hacking activity, including to advertise  
9 hacked data for sale. Using RaidForums, BINNS offered and advertised hacked data for  
10 sale, including T-Mobile customer databases and stolen PII.

11 k. BINNS engaged others to assist in the activity and to further the  
12 objects of the conspiracy, including, but not limited to, the following:

13 i. "Coconspirator-1," known by moniker "und0xxed," a citizen  
14 and resident of the United States, who, among other things, assisted BINNS in locating  
15 interested buyers and in facilitating the sale of advertised T-Mobile data; and

16 ii. "Coconspirator-2," a citizen and resident of Germany, who,  
17 among other things, assisted BINNS by providing infrastructure and support, such as  
18 virtual servers and electronic storage, and with the transfer of proceeds derived from the  
19 sale of stolen T-Mobile data; and,

20 iii. "Coconspirator-3," an unidentified person, who, among other  
21 things, provided BINNS with assistance in the intrusion activity.

22 l. BINNS, and others, communicated with one another and others using  
23 various communication platforms. For instance, BINNS created and used accounts on  
24 Telegram, an encrypted messaging service, to communicate with potential buyers and  
25 others seeking information about the T-Mobile hack and the advertised T-Mobile data.

26 m. BINNS, and others, promoted themselves, the T-Mobile hack, and in  
27 turn the advertised T-Mobile data, through use of social media accounts, such as Twitter  
28 accounts. For instance, BINNS, using Twitter account @IntelSecrets, and



1 Coconspirator-1, using Twitter account @und0xxed, disseminated information, by  
2 “tweeting” and “retweeting,” about the hack of T-Mobile and directed interested parties to  
3 contact BINNS at a particular Telegram handle.

4 n. BINNS, and others, further promoted themselves, the T-Mobile hack,  
5 and in turn the advertised T-Mobile data through interviews with news outlets. For  
6 instance, Coconspirator-1 provided information to a cybersecurity website. BINNS  
7 similarly provided an interview to the Wall Street Journal, details of which were included  
8 in an article published on about August 26, 2021.

9 o. BINNS further engaged in misdirection techniques, including the use  
10 of false information. For instance, in certain communications, BINNS included the name  
11 and information of others, which had the intended and material effect of falsely implicating  
12 and drawing attention toward other persons in relation to BINNS’ criminal activity.

13 p. BINNS agreed to sell the advertised T-Mobile data to an interested  
14 buyer (“Buyer-1”), and to no other buyer, for an agreed upon amount (far in excess of  
15 \$5,000), payable in Bitcoin.

16 q. BINNS provided Buyer-1 access to a sample of the advertised  
17 T-Mobile data in order to assess the authenticity of the files and information, in exchange  
18 for a portion of the agreed upon purchase amount. Upon confirmation of authenticity,  
19 BINNS provided Buyer-1 the entirety of the advertised T-Mobile data, in exchange for the  
20 remainder of the agreed upon purchase amount. Each transfer utilized a third-party escrow  
21 service that received the Bitcoin transfers from Buyer-1 and, upon confirmation, released  
22 the Bitcoin to a wallet owned and controlled by BINNS.

23 r. BINNS, contrary to the negotiated arrangement with Buyer-1, retained  
24 a copy of the advertised T-Mobile data, which BINNS and others have attempted to further  
25 monetize and otherwise use to their benefit.

26 **E. Overt Acts**

27 6. In furtherance of the conspiracy, and to achieve the objects thereof, BINNS,  
28 and others known and unknown to the Grand Jury, did commit and cause to be committed

1 the following overt acts, among others, in the Western District of Washington and  
2 elsewhere:

3 a. On or about December 17, 2020, BINNS attempted to connect to a  
4 T-Mobile IP address and T-Mobile's network.

5 b. On or about March 7, 2021, BINNS attempted to connect to multiple  
6 T-Mobile IP addresses.

7 c. On or about July 31, 2021, BINNS accessed the Bellevue Lab and  
8 installed "backdoor" malware.

9 d. On or about July 31, 2021, BINNS sent a message to Coconspirator-3,  
10 stating: "Do what I told u to do asap...Bc I found a way to access you know what."

11 e. Between on or about July 31, and August 4, 2021, BINNS accessed  
12 the Bellevue Lab and engaged in network-scanning and password-spraying activity.

13 f. On or about August 4, 5, and 6, 2021, BINNS accessed multiple server  
14 groups, traversed local directories, and enumerated file contents. From those files, he used  
15 passwords for database accounts to access other databases, and copied their contents back  
16 through the Bellevue Lab.

17 g. Between on or about August 5 and 12, 2021, BINNS accessed the  
18 Bellevue Lab and transferred files and databases to an external location.

19 h. On or about August 11, 2021, BINNS, using the "SubVirt" account,  
20 created a post on RaidForums offering to sell recently-hacked data with the following title:  
21 "SELLING-124M-U-S-A-SSN-DOB-DL-database-freshly-breached." The post provided a  
22 small sample of data, which included names and date of birth (DOBs), and priced the  
23 information at six (6) Bitcoin.

24 i. On or about August 13, 2021, BINNS disconnected from the Bellevue  
25 Lab. BINNS' subsequent attempts to access the Bellevue Lab were unsuccessful.

26 j. On or about August 14, 2021, Coconspirator-1, using Twitter,  
27 disclosed the T-Mobile hack, including in the following "tweets":  
28



1 i. “You heard it here first: T-Mobile got DESTROYED on Aug 5,  
2 we have the next TalkTalk ladies and gentlemen [emojis] @TMobile @TMobileHelp”; and

3 ii. “Publicly disclosing a breach of the @TMobile customer/CRM  
4 and other databases including names, addresses, SSNs, DoBs, card numbers, DL numbers,  
5 IMEI/IMSI, and more. 36 million unique entries. The data was held in the Polaris and Titan  
6 data centers. Currently 100% private.”

7 k. On or about August 14, 2021, BINNS, using the “SubVirt” account,  
8 created a revised post on RaidForums offering to sell recently-hacked data with the  
9 following title: “SELLING 30M SSN + DL + DOB database.” The post provided a small  
10 sample of data, which included names and DOBs, and priced the information at six (6)  
11 Bitcoin. The post also provided a Telegram handle as contact information for interested  
12 buyers. A subsequent RaidForums post confirmed that the hacked data belonged to  
13 T-Mobile.

14 l. On or about August 15, 2021, Coconspirator-1, using Twitter,  
15 provided a Telegram handle for others interested in “samples or more info” regarding the  
16 T-Mobile hack and stolen data.

17 m. On or about August 17, 2021, after receiving a Bitcoin payment from  
18 Buyer-1 to an escrow account, BINNS provided Buyer access to a portion of the stolen T-  
19 Mobile data.

20 n. On or about August 22, 2021, after receiving an additional Bitcoin  
21 payment to an escrow account, BINNS provided Buyer-1 access to the complete set of  
22 stolen T-Mobile data.

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

24 **COUNTS 2 - 3**

25 **(Computer Fraud and Abuse: Intentional Damage to Protected Computer)**

26 7. The allegations set forth in Paragraphs 1 through 6 of this Indictment are  
27 re-alleged and incorporated as if fully set forth herein.

1 8. On or about the dates set forth below, in King County, within the Western  
 2 District of Washington, and elsewhere, JOHN ERIN BINNS, and others known and  
 3 unknown to the Grand Jury, knowingly caused the transmission of a program, information,  
 4 code, and command, and, as a result of such conduct, intentionally caused damage without  
 5 authorization to a protected computer.

Count	Date(s)	Description
2	July 31, 2021	Installation of malware, including a backdoor, on T-Mobile's Bellevue Lab
3	August 5-8, 2021	Deletion of data files from T-Mobile's protected computers and networks, using commands and signals that traversed T-Mobile's Bellevue Lab

11 9. The offense caused loss to one or more persons during a 1-year period  
 12 aggregating at least \$5,000 in value, and caused damage affecting 10 or more protected  
 13 computers during a 1-year period.

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

#### COUNT 4

#### **(Computer Fraud and Abuse: Unauthorized Access to Protected Computer)**

17 10. The allegations set forth in Paragraphs 1 through 6 of this Indictment are  
 18 re-alleged and incorporated as if fully set forth herein.

19 11. On or about August 5, 2021, in King County, within the Western District of  
 20 Washington, and elsewhere, JOHN ERIN BINNS, and others known and unknown to the  
 21 Grand Jury, intentionally accessed a computer without authorization, and thereby obtained  
 22 information from a protected computer.

23 12. The offense was committed for purposes of private financial gain and the  
 24 value of the information obtained exceeded \$5,000.

25 All in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B).  
 26  
 27  
 28



COUNTS 5 - 7

**(Wire Fraud)**

13. The allegations set forth in Paragraphs 1 through 6 of this Indictment are re-alleged and incorporated as if fully set forth herein.

**A. Scheme and Artifice to Defraud**

14. Beginning at a time unknown, but no later than in or about December 2020, and continuing to the present, in King County, within the Western District of Washington, and elsewhere, JOHN ERIN BINNS, 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**

15. The essence of the scheme and artifice to defraud is set forth in Paragraph 4 of this Indictment and is re-alleged and incorporated as if fully set forth herein.

16. The essence of the scheme and artifice to defraud further included the fraudulent and unauthorized use of passwords and credentials to access databases and to execute commands and scripts on protected computers and servers. The essence of the scheme and artifice to defraud further included falsely and fraudulently representing the exclusivity of the sale of stolen data in order to elevate the purchase price.

**C. Manner and Means**

17. The manner and means of the scheme and artifice to defraud are set forth in Paragraph 5 of this Indictment and are re-alleged and incorporated as if fully set forth herein.

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

18. On or about the dates set forth below, in King County, within the Western District of Washington, and elsewhere, the defendant BINNS, 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,

1 and promises, did knowingly transmit and cause to be transmitted writings, signs, signals,  
 2 pictures, and sounds, for the purpose of executing such scheme, by means of wire  
 3 communication in interstate and foreign commerce, including the following transmissions,  
 4 each of which constitutes a separate count of this Indictment:

Count	Date(s)	Wire Transmission
5	July 31, 2021	Installation of malicious script establishing backdoor on T-Mobile's Bellevue Lab, located in the Western District of Washington, from outside the State of Washington
6	August 5, 2021	Transfer of electronic data from T-Mobile's Bellevue Lab, from the Western District of Washington, to a location outside the State of Washington
7	August 14, 2021	Tweet by Twitter account @und0xxed about the T-Mobile hack and stolen data, sent from outside the State of Washington and received in the Western District of Washington

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

16 **COUNT 8 - 9**

17 **(Aggravated Identity Theft)**

18 19. The allegations set forth in Paragraphs 1 through 6 and 13 through 18 of this  
 19 Indictment are re-alleged and incorporated as if fully set forth herein.

20 20. On or about the dates listed below, in King County, within the Western  
 21 District of Washington, and elsewhere, JOHN ERIN BINNS, and others known and  
 22 unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful  
 23 authority, a means of identification of another person, a real person, as described below,  
 24 during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is,  
 25 computer fraud and abuse, as charged in Counts 2 through 4, and wire fraud, in violation of  
 26 18 U.S.C. § 1343, as charged in Counts 5 through 7, knowing that the means of  
 27 identification belonged to another actual person.  
 28



Count	Date(s)	Description
8	August 17, 2021	Personal information of real persons, obtained from protected computers and networks of T-Mobile, possessed and transferred to Buyer-1
9	August 22, 2021	Personal information of real persons, obtained from the protected computers and networks of T-Mobile, possessed and transferred to Buyer-1

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

**COUNT 10**

**(Conspiracy to Commit Money Laundering)**

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

**A. The Offense**

22. Beginning at a time unknown, but no later than August 2021, and continuing to the present, in King County, within the Western District of Washington, and elsewhere, JOHN ERIN BINNS, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree, with other persons known and unknown to the Grand Jury, to commit offenses against the United States in violation of Title 18, United States Code, Section 1956 and 1957, to wit:

a. to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, computer fraud and abuse, in violation of Title 18, United States Code, Section 1030; wire fraud, in violation of Title 18, United States Code, Section 1343; and conspiracy to commit such offenses, as charged in Counts 1 through 7 of this Indictment, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and, while conducting and attempting to conduct such financial transactions, knowing that the property involved in the financial transactions

1 represented the proceeds of some form of unlawful activity, in violation of Title 18, United  
2 States Code, Section 1956(a)(1)(B)(i); and

3 b. to knowingly engage and attempt to engage, in monetary transactions  
4 by, through and to a financial institution, affecting interstate and foreign commerce, in  
5 criminally derived property of a value greater than \$10,000, such property having been  
6 derived from a specified unlawful activity, that is, computer fraud and abuse, in violation  
7 of Title 18, United States Code, Section 1030; wire fraud, in violation of Title 18, United  
8 States Code, Section 1343; and conspiracy to commit such offenses, as charged in Counts 1  
9 through 7 of this Indictment, in violation of Title 18, United States Code, Section 1957.

10 **B. Manner and Means of the Money Laundering Conspiracy**

11 23. The manner and means used to accomplish the objectives of the conspiracy  
12 included, among others, the following:

13 a. BINNS opened one or more accounts and maintained wallets at a  
14 particular foreign-based cryptocurrency exchange, and executed fund transfers and  
15 required payments by means of cryptocurrency, such as Bitcoin, with the intent and  
16 purpose to conceal and disguise the nature, location, source, ownership, and control of the  
17 funds, including proceeds of illegal activity.

18 b. BINNS further utilized intermediary transfers to further conceal and  
19 disguise the nature, location, source, ownership, and control of the funds, including  
20 proceeds of illegal activity. Such transfers typically were divided into many separate  
21 transfers of smaller amounts in order to avoid reporting requirements and the attention of  
22 regulators, utilizing a technique commonly referred to as a “peel chain.”

23 c. BINNS further agreed to provide cryptocurrency to Coconspirator-2 in  
24 exchange for credit cards issued in the name of others and other items of value.

25 d. Illegally obtained proceeds were transferred to accounts located in  
26 foreign countries and ultimately to accounts maintained and controlled by BINNS and his  
27 co-conspirators and associates.



1 e. **Example 1:** On or about August 17, 2021, at the direction of BINNS,  
2 Buyer-1 initiated and caused a transfer of an agreed amount of Bitcoin (greater than the  
3 equivalent of \$10,000) to an escrow wallet, in exchange for a sample set of the advertised  
4 T-Mobile data. Upon further confirmation, the approximate amount of Bitcoin, less an  
5 escrow fee, was transferred from the escrow wallet to another cryptocurrency wallet  
6 associated with BINNS. Thereafter, the Bitcoin amount was separated into smaller  
7 amounts and sent to different destinations. For instance, on August 17, 2021, a portion of  
8 the Bitcoin amount (greater than the equivalent of \$10,000) was transferred to and  
9 deposited in a wallet maintained at a foreign cryptocurrency exchange owned and  
10 controlled by BINNS. Through a series of transfers, other portions of the Bitcoin amount  
11 were transferred to wallets associated with Coconspirator-2. Through a series of additional  
12 transfers, the majority of the Bitcoin amount was transferred to other wallets believed to be  
13 owned and controlled by BINNS.

14 f. **Example 2:** On about August 22, 2021, at the direction of BINNS,  
15 Buyer-1 initiated and caused a transfer of an agreed amount of Bitcoin (greater than the  
16 equivalent of \$10,000) to an escrow wallet, in exchange for the entirety of the advertised  
17 T-Mobile data. Upon further confirmation, the approximate amount of Bitcoin, less an  
18 escrow fee, was transferred from the escrow wallet to another cryptocurrency wallet.  
19 Through a series of subsequent transfers, the majority of the funds from this purchase were  
20 transferred to wallets believed to be owned and controlled by BINNS.

21 All in violation of Title 18, United States Code, Section 1956(h).

22 **FORFEITURE ALLEGATION**

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

25 25. Upon conviction of the offense charged in Count 1, the defendant shall forfeit  
26 to the United States all property that constitutes or is traceable to proceeds he obtained  
27 from the commission of the offense, as well as any personal property he used to commit the  
28 offense. All such property is forfeitable pursuant to Title 18, United States Code, Section

1 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c), Title 18, United  
2 States Code, Section 982(a)(2)(B), and Title 18, United States Code, 1030(i) and includes,  
3 but is not limited to, a sum of money reflecting the proceeds the defendant obtained from  
4 the offense.

5 26. Upon conviction of any of the offenses charged in Counts 2 through 4, the  
6 defendant shall forfeit to the United States any property that constitutes or is traceable to  
7 proceeds he obtained from the commission of the offense, as well as any personal property  
8 he used to commit the offense. All such property is forfeitable pursuant to Title 18, United  
9 States Code, Section 982(a)(2)(B) and Title 18, United States Code, 1030(i) and includes,  
10 but is not limited to, a sum of money reflecting the proceeds the defendant obtained from  
11 the relevant offense.

12 27. Upon conviction of any of the offenses charged in Counts 5 through 7, the  
13 defendant shall forfeit to the United States any property that constitutes or is traceable to  
14 proceeds he obtained from the commission of the offense. All such property is forfeitable  
15 pursuant to Title 18, United States Code, Section 981(a)(1)(C), by way of Title 28, United  
16 States Code, Section 2461(c), and includes, but is not limited to, a sum of money reflecting  
17 the proceeds the defendant obtained from the relevant offense.

18 28. Upon conviction of the offenses charged in Count 10, the defendant shall  
19 forfeit to the United States any property that constitutes or is traceable to proceeds he  
20 obtained from the commission of the offense, as well as any property that was involved in  
21 the offense. All such property is forfeitable pursuant to Title 18, United States Code,  
22 Section 982(a)(1) and includes, but is not limited to, a sum of money reflecting the  
23 proceeds the defendant obtained from the offense.

24 //

25 //

26 //

27

28



1           29.    **Substitute Assets.** If any of the property described above, as a result of any  
2 act or omission of the defendant,

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

9 //

10 //

11 //

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28


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

4 A TRUE BILL:


5 DATED: 12 January 2022

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

9 \_\_\_\_\_  
10 FOREPERSON

11   
12 \_\_\_\_\_  
13 NICHOLAS W. BROWN  
14 United States Attorney

15   
16 \_\_\_\_\_  
17 ANDREW C. FRIEDMAN  
18 Assistant United States Attorney

19   
20 \_\_\_\_\_  
21 STEVEN T. MASADA  
22 Assistant United States Attorney  
23  
24  
25  
26  
27  
28