[redacted]

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
March 9, 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 **SUPERSEDING 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.

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

TheDesk.net

"T-Mobile"), a telecommunications company and wireless network operator headquartered in the Western District of Washington. BINNS, using such unauthorized network access, stole confidential and sensitive information and other data of value, including, but not limited to, personally identifiable information (PII), telecommunications service and equipment identifiers, and other "access devices," as defined by law, of more than 40 million current, prospective, and former T-Mobile customers, which BINNS offered for sale and did sell on an online forum.

B. Offense

3. 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, 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 private financial gain, 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

4. The objects of the conspiracy included, through use of deceptive and fraudulent means, gaining access to protected computers and networks without authorization and to the data stored thereon. The objects of the conspiracy included

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

TheDesk.net

planting malware on the protected computers, and stealing sensitive databases and information, including personal identifiable information (PII) of real persons, and other confidential files, with the purpose and intent to monetize such non-public material by obtaining money and things of value, including sums of cryptocurrency, through sale and further to deprive victims of the exclusive control and ownership of their property.

D. Manner and Means of the Conspiracy

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

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

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

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

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

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

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

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

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

TheDesk.net

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

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

j. BINNS operated one or more accounts on the underground online forum RaidForums, a popular marketplace and database-sharing site frequented by cybercriminals used to promote data leaks and hacking activity, including to advertise hacked data for sale. Using RaidForums, BINNS offered and advertised hacked data for sale, including T-Mobile customer databases and stolen customer names, dates of birth, social security numbers, and driver license information.

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

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

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

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

iv. "Coconspirator-4," known by moniker "Omnipotent," who, among other things, assisted BINNS in facilitating the sale of advertised T-Mobile data.

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

TheDesk.net

UNITED STATES ATTORN
700 STEWART STREET, SUITE
SEATTLE, WASHINGTON 98
(206) 553-7970

m. BINNS, and others, promoted themselves, the T-Mobile hack, and in turn the advertised T-Mobile data, through use of social media accounts, such as Twitter accounts. For instance, BINNS, using Twitter account @IntelSecrets, and Coconspirator-1, using Twitter account @und0xxed, disseminated information, by "tweeting" and "retweeting," about the hack of T-Mobile and directed interested parties to contact BINNS at a particular Telegram handle.

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

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

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

q. BINNS provided Buyer-1 access to a sample of the advertised T-Mobile data in order to assess the authenticity of the files and information, in exchange for a portion of the agreed upon purchase amount. Upon confirmation of authenticity, BINNS provided Buyer-1 the entirety of the advertised T-Mobile data, in exchange for the remainder of the agreed upon purchase amount. Each transfer utilized a third-party escrow service, provided by Coconspirator-4, that received the Bitcoin transfers from Buyer-1 and upon confirmation, released the Bitcoin to a wallet owned and controlled by BINNS.

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

TheDesk.net

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

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

j. BINNS operated one or more accounts on the underground online forum RaidForums, a popular marketplace and database-sharing site frequented by cybercriminals used to promote data leaks and hacking activity, including to advertise hacked data for sale. Using RaidForums, BINNS offered and advertised hacked data for sale, including T-Mobile customer databases and stolen customer names, dates of birth, social security numbers, and driver license information.

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

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

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

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

iv. "Coconspirator-4," known by moniker "Omnipotent," who, among other things, assisted BINNS in facilitating the sale of advertised T-Mobile data.

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

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

TheDesk.net

E. Overt Acts

6. In furtherance of the conspiracy, and to achieve the objects thereof, BINNS, 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 December 17, 2020, BINNS attempted to connect to a T-Mobile IP address and T-Mobile's network.

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

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

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

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

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

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

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

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

TheBaklet

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

COUNTS 2 - 3

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

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

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

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

9. The offense caused loss to one or more persons during a 1-year period aggregating at least $5,000 in value, and caused 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) and (c)(4)(B).

COUNT 4

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

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

11. On or about August 5, 2021, in King County, within the Western Distric Washington, and elsewhere, JOHN ERIN BINNS, and others known and unknown to t Grand Jury, intentionally accessed a computer without authorization, and thereby obta information from a protected computer.

UNITED STATES ATTOR
700 STEWART STREET, SUIT
SEATTLE, WASHINGTON 9
(206) 553-7970

TheDesk.net

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

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

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

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

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

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

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

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

TheDesk.net

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

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

COUNTS 5 - 7

(Wire Fraud)

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

TheDesk.net

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

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, 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 Superseding 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

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

COUNT 8

(Conspiracy to Commit Access Device Fraud)

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

A. Offense

20. 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,

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

File Next.net

and elsewhere, JOHN ERIN BINNS, 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 knowingly, and with intent to defraud, traffic in and use one or more unauthorized access devices during a one-year period, and by such conduct obtain things of value aggregating $1,000 and more during that period, such conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(2); and,

b. to knowingly, and with intent to defraud, possess fifteen and more unauthorized access devices, such conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(3); and,

c. without the authorization of the issuer of the access device, to knowingly, and with intent to defraud, solicit a person for the purpose of offering for sale, and selling information regarding, an access device, such conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(6).

B. Objects of the Conspiracy

21. The objects of the conspiracy are set forth in Paragraph 4 of this Superseding Indictment and is re-alleged and incorporated as if fully set forth herein.

22. The objects of the conspiracy further included the transfer, possession, and sale of millions of "unauthorized access devices," as defined by law, with the purpose and intent to monetize such non-public material by obtaining money and things of value, including sums of cryptocurrency, through sale and further to deprive victims of the exclusive control and ownership of their property.

C. Manner and Means of the Conspiracy

23. The manner and means of the conspiracy are set forth in Paragraph 5 of this Superseding Indictment and are re-alleged and incorporated as if fully set forth herein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE
SEATTLE, WASHINGTON 98

TheDeskNet

D. Overt Acts

24. The overt acts commit by BINNS, and others known and unknown to the Grand Jury, in furtherance of the conspiracy and to achieve the objects thereof, are set forth in Paragraph 6 of this Superseding Indictment and are re-alleged and incorporated as if fully set forth herein.

All in violation of Title 18, United States Code, Section 1029(b)(2).

COUNT 9

(Access Device Fraud: Unauthorized Solicitation)

25. The allegations set forth in Paragraphs 1 through 6 and 13 through 24 of this Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

26. On or about August 14, 2021, in King County, within the Western District of Washington, and elsewhere, JOHN ERIN BINNS, and others known and unknown to the Grand Jury, knowingly and with intent to defraud, solicited other persons with the purpose of offering, and selling information regarding, unauthorized access devices, as defined by 18 U.S.C. § 1029(e)(1) and (e)(3), to wit: account information, social security numbers, driver license information, identification numbers, and other telecommunications service, equipment, and instrument identifiers, without the authorization of the issuer, such conduct affecting interstate and foreign commerce, in that the solicitation occurred through use of the Internet and between devices located within and outside of the Western District of Washington.

All in violation of Title 18, United States Code, Sections 1029(a)(6) and 2.

COUNTS 10 - 11

(Aggravated Identity Theft)

27. The allegations set forth in Paragraphs 1 through 6 and 13 through 26 of th Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

28. On or about the dates listed below, 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 transfer, possess, and use, without lawful

UNITED STATES ATTORN
700 STEWART STREET, SUITE
SEATTLE, WASHINGTON 98
(206) 553-7970

The Record

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, computer fraud and abuse, in violation of 18 U.S.C. § 1030(a), as charged in Counts 2 through 4; wire fraud, in violation of 18 U.S.C. § 1343, as charged in Counts 5 through 7; conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029(b)(2), as charged in Count 8; and access device fraud, in violation of 18 U.S.C. § 1029(a)(6), as charged in Count 9, knowing that the means of identification belonged to another actual person.

Count	Date(s)	Description
10	August 17, 2021	Personal information of real persons, obtained from protected computers and networks of T-Mobile, possessed and transferred to Buyer-1
11	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 12

(Conspiracy to Commit Money Laundering)

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

A. The Offense

30. 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:

TheRack.net

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; access device fraud, in violation of Title 18, United States Code, Section 1029(a); and conspiracy to commit such offenses, as charged in Counts 1 through 9 of this Superseding 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 represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and,

b. to knowingly engage and attempt to engage, in monetary transactions by, through and to a financial institution, affecting interstate and foreign commerce, in criminally derived property of a value greater than $10,000, such property having been derived from a 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; access device fraud, in violation of Title 18, United States Code, Section 1029(a); and conspiracy to commit such offenses, as charged in Counts 1 through 9 of this Superseding Indictment, in violation of Title 18, United States Code, Section 1957.

B. Manner and Means of the Money Laundering Conspiracy

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

a. BINNS opened one or more accounts and maintained wallets at a particular foreign-based cryptocurrency exchange, and executed fund transfers and required payments by means of cryptocurrency, such as Bitcoin, with the intent and

FreePacer.net

purpose to conceal and disguise the nature, location, source, ownership, and control of the funds, including proceeds of illegal activity.

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

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

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

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

f. **Example 2:** On about August 22, 2021, at the direction of BINNS, Buyer-1 initiated and caused a transfer of an agreed amount of Bitcoin (greater than the equivalent of $10,000) to an escrow wallet controlled by Coconspirator-4, in exchange for

TheDesk.net

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101

the entirety of the advertised T-Mobile data. Upon further confirmation, the approximate amount of Bitcoin, less an escrow fee, was transferred from the escrow wallet to another cryptocurrency wallet. Through a series of subsequent transfers, the majority of the funds from this purchase were transferred to wallets believed to be owned and controlled by BINNS.

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

FORFEITURE ALLEGATION

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

33. Upon conviction of the offense charged in Count 1, the defendant shall forfeit to the United States all property that constitutes or is traceable to proceeds he obtained from the commission of the offense, as well as any personal property he used to commit 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), Title 18, United States Code, Section 982(a)(2)(B), and Title 18, United States Code, 1030(i) and includes, but is not limited to, a sum of money reflecting the proceeds the defendant obtained from the offense.

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

35. Upon conviction of any of the offenses charged in Counts 5 through 7, the defendant shall forfeit to the United States any property that constitutes or is traceable to proceeds he obtained from the commission of 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

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

TheDeskNet

States Code, Section 2461(c), and includes, but is not limited to, a sum of money reflecting the proceeds the defendant obtained from the relevant offense.

36. Upon conviction of either of the offenses charged in Counts 8 and 9, the defendant shall forfeit to the United States any property that constitutes or is traceable to proceeds he obtained from the commission of the offense, as well as any personal property that was used or intended to be used in the offense. All such property is forfeitable pursuant to Title 18, United States Code, Section 982(a)(2)(B) and Title 18, United States Code, Section 1029(c)(1)(C) and includes, but is not limited to, a sum of money reflecting the proceeds the defendant obtained from the relevant offense.

37. Upon conviction of the offenses charged in Count 12, the defendant shall forfeit to the United States any property that constitutes or is traceable to proceeds he obtained from the commission of the offense, as well as any property that was involved in the offense. All such property is forfeitable pursuant to Title 18, United States Code, Section 982(a)(1) and includes, but is not limited to, a sum of money reflecting the proceeds the defendant obtained from the offense.

38. **Substitute Assets.** 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,

//

//

//

FileDesk.net

[redacted]

It is the intent of the United States to seek the forfeiture of any other property of the defendant, up to the value of the above-described forfeitable property, pursuant to Title 21, United States Code, Section 853(p).

A TRUE BILL:

DATED: 9 March 2022

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

FOREPERSON

NICHOLAS W. BROWN
United States Attorney

ANDREW C. FRIEDMAN
Assistant United States Attorney

STEVEN T. MASADA
Assistant United States Attorney

TheDesk.net