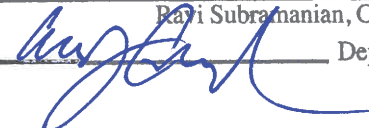


Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

October 10 20 24
Raji Subramanian, Clerk
By  Deputy

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

UNITED STATES OF AMERICA,
Plaintiff,

v.

CONNOR RILEY MOUCKA,
a.k.a. "Alexander Antonin Moucka,"
a.k.a. "judische,"
a.k.a. "catist,"
a.k.a. "waifu,"
a.k.a. "ellyel8,"

and

JOHN ERIN BINNS,
a.k.a. "irdev,"
a.k.a. "j_irdev1337,"

Defendants.

NO. CR 24 - 180 LK

INDICTMENT

The Grand Jury charges that:

COUNT 1
(Conspiracy)

Introduction

1. Beginning on a date unknown, but no later than in or about November 2023, and continuing through at least October 10, 2024, in King County, within the Western District of Washington, and elsewhere, and in an offense begun outside the jurisdiction of

1 any particular state or district of the United States, CONNOR RILEY MOUCKA and
2 JOHN ERIN BINNS, and others known and unknown to the Grand Jury, devised and
3 executed international computer hacking and wire fraud schemes to hack into at least 10
4 victim organizations' protected computer networks, steal sensitive information, threaten to
5 leak the stolen data unless the victims paid ransoms, and offer to sell online, and sell, the
6 stolen data. Through this scheme, the co-conspirators gained unlawful access to billions of
7 sensitive customer records, including individuals' non-content call and text history records,
8 banking and other financial information, payroll records, Drug Enforcement Agency
9 ("DEA") registration numbers, driver's license numbers, passport numbers, Social Security
10 numbers, and other personally identifiable information.

11 2. MOUCKA, BINNS, and their co-conspirators profited from these schemes
12 through several means, including by successfully extorting at least 36 bitcoin (worth
13 approximately \$2.5 million at the time of payment) from at least three victims, and by
14 posting offers to sell victims' stolen data on cybercriminal forums for millions of dollars.

15 **Relevant Individuals and Entities**

16 3. At all times relevant to this Indictment:

17 a. CONNOR RILEY MOUCKA, also known as "Alexander Antonin
18 Moucka," resided in Canada. MOUCKA used online accounts associated with
19 particular nicknames known to the Grand Jury, including but not limited to
20 "judische," "catist," "waifu," and "ellye18."

21 b. JOHN ERIN BINNS resided in Turkey. BINNS also used online
22 accounts associated with particular nicknames known to the Grand Jury, including
23 but not limited to "irdev" and "j_irdev1337."

24 c. Victim-1 was a software-as-a-service provider located in the United
25 States. Victim-1 provided software that allowed U.S. and foreign organizations to
26 upload and store data within cloud computing "instances," or online storage
27 environments, which were intended to be accessible only by users authorized by the

1 customer organizations (hereinafter, “Cloud Computing Instances”). Each user of a
2 Cloud Computing Instance had discrete permissions to access his or her own user
3 account, and, through that account, particular portions of the Cloud Computing
4 Instance. The Cloud Computing Instances were hosted on computer servers
5 controlled by Victim-1, and were located throughout the world, including in
6 Virginia, Oregon, and the Netherlands.

7 d. Victim-2 was a major telecommunications company located in the
8 United States. Victim-2’s Cloud Computing Instance was hosted at computer servers
9 located in Virginia.

10 e. Victim-3 was a major retailer located in the United States. Victim-3’s
11 Cloud Computing Instance was hosted at computer servers located in Oregon.

12 f. Victim-4 was a major entertainment company located in the United
13 States. Victim-4’s Cloud Computing Instance was hosted at computer servers
14 located in Oregon.

15 g. Victim-5 was a major healthcare company with significant operations
16 in the United States. Victim-5’s Cloud Computing Instance was hosted at computer
17 servers located in Virginia.

18 h. Victim-6 was a major foreign company located in Europe with
19 operations and personnel located in the United States. Victim-6’s Cloud Computing
20 Instance was hosted at computer servers located in the Netherlands.

21 **The Conspiracy**

22 4. Beginning on a date unknown, but no later than in or about November 2023
23 and continuing through at least October 10, 2024, CONNOR RILEY MOUCKA, JOHN
24 ERIN BINNS, and others known and unknown to the Grand Jury, in King County, within
25 the Western District of Washington, and elsewhere, and in an offense begun outside the
26 jurisdiction of any particular state or district of the United States, did knowingly and
27 willfully combine, conspire, confederate, and agree to commit:

- 1 a. Computer fraud, in violation of Title 18, United States Code, Sections
- 2 1030(a)(2)(C) and 1030(c)(2)(B)(i)–(iii), and 1030(a)(7)(B) and
- 3 1030(c)(3)(A);
- 4 b. Wire fraud, in violation of Title 18, United States Code, Section 1343; and
- 5 c. Aggravated identity theft, in violation of Title 18, United States Code,
- 6 Section 1028A.

7 ***Goal of the Conspiracy***

8 5. It was the goal of the conspiracy for MOUCKA, BINNS, and others to enrich
9 themselves by: (a) accessing computers without authorization; (b) stealing sensitive
10 personal identifying, financial, and other valuable information from those computers;
11 (c) threatening to leak the stolen data unless the victims paid ransoms; and (d) offering to
12 sell the stolen data online to other criminals.

13 ***Manner and Means of the Conspiracy***

14 6. It was part of the conspiracy that:

15 a. The co-conspirators, including MOUCKA and BINNS, stole or
16 otherwise obtained stolen access credentials that could be used to access the Cloud
17 Computing Instances of victim organizations and their users.

18 b. The co-conspirators, including MOUCKA and BINNS, used these
19 access credentials to unlawfully access victims' Cloud Computing Instances and to
20 view and download terabytes of private data from within the Cloud Computing
21 Instances, including business information, as well as individuals' non-content call
22 and text history records, banking and other financial information, payroll records,
23 DEA registration numbers, driver's license numbers, passport numbers, Social
24 Security numbers, and other personally identifiable information. MOUCKA,
25 BINNS, and their co-conspirators accessed and obtained data from at least 10
26 different organizations' Cloud Computing Instances using stolen access credentials.

27 c. The co-conspirators, including MOUCKA and BINNS, used software

1 they dubbed “Rapeflake” to identify valuable information residing within the
2 victims’ Cloud Computing Instances, including organization names, user roles, and
3 Internet Protocol (“IP”) addresses, among other information.

4 d. The co-conspirators, including MOUCKA and BINNS, through
5 intermediaries, extorted victims by threatening to sell or otherwise distribute their
6 stolen data unless the victims paid ransoms, which at least three victims paid. In at
7 least one instance, the co-conspirators attempted to re-extort one of these victims
8 with threats of further disclosure of the victim’s stolen data.

9 e. The co-conspirators, including MOUCKA and BINNS, used a range
10 of communication methods in furtherance of their crimes, and changed these
11 accounts frequently, all to protect their anonymity. Many of these services were
12 located abroad, and some offered enhanced privacy protections, such as not
13 collecting or validating customer information, offering limited logging of user IP
14 addresses, and protecting the contents of messages with encryption. Other
15 communication platforms catered specifically to cybercriminals, including the
16 online cybercrime forums BreachForums, Exploit.in, and XSS.is, as well as
17 Telegram channels dedicated to online frauds and other cybercrimes.

18 f. The co-conspirators, including MOUCKA and BINNS, also
19 advertised stolen data for sale online, including on BreachForums, Exploit.in, and
20 XSS.is. These advertisements offered to sell the data in exchange for fiat currency
21 and cryptocurrency. The forums on which these postings were made could be
22 accessed from computers located anywhere in the world, including in the Western
23 District of Washington, and these posts were used to facilitate the extortion of the
24 victim organizations, as well as the sale and attempted sale of the victims’ stolen
25 data.

26 g. The co-conspirators, including MOUCKA and BINNS, leased
27 technological infrastructure, including servers, online hosting, and IP addresses,

1 from service providers all over the world. Many of these services were obtained
2 using fraudulent identity information and a variety of payment methods so as to hide
3 the identities of the accountholders.

4 h. The co-conspirators, including MOUCKA and BINNS, demanded
5 payments and made payments for services in cryptocurrency, including bitcoin, and
6 conducted complex cryptocurrency transfers in order to hide the source and
7 destination of their funds. Some of these transfers included transferring bitcoin into
8 monero, an anonymity-enhanced cryptocurrency, to further confound attempts to
9 trace the source and destination of their funds. The co-conspirators, including
10 MOUCKA and BINNS, used virtual asset service providers located all over the
11 world, including in the United States.

12 ***Overt Acts***

13 7. In furtherance of the conspiracy, and in order to effect the purpose and objects
14 thereof, the co-conspirators, including MOUCKA and BINNS, committed various overt
15 acts in King County, within the Western District of Washington, and elsewhere, including,
16 but not limited to, the following:

17 ***Victim-1***

18 a. Between at least on or about April 17, 2024, and at least on or about
19 May 24, 2024, MOUCKA and BINNS accessed Victim-1's protected computer
20 networks without authorization.

21 b. On or about April 17, 2024, and April 19, 2024, MOUCKA and
22 BINNS used Rapeflake to run searches within Victim-1's Cloud Computing
23 Instance and to obtain information, all without authorization.

24 ***Victim-2***

25 c. Between at least on or about April 14, 2024, and at least on or about
26 April 28, 2024, MOUCKA and BINNS accessed Victim-2's Cloud Computing
27 Instance without authorization.

1 d. On or about at least April 14, 2024, April 15, 2024, and April 24, 2024,
2 MOUCKA and BINNS exfiltrated approximately 50 billion customer call and text
3 records, including dialed numbers, pertaining to Victim-2's customers from its
4 Cloud Computing Instance.

5 e. On or about May 17, 2024, MOUCKA and BINNS caused a ransom
6 demand to be sent to Victim-2, which requested payment in cryptocurrency in
7 exchange for deletion of Victim-2's stolen data.

8 f. On or about May 17, 2024, MOUCKA and BINNS caused hyperlinks
9 to be sent to Victim-2, which Victim-2 reviewed and confirmed could be used to
10 access copies of its stolen data.

11 g. On or about May 17, 2024, MOUCKA and BINNS caused Victim-2
12 to send a ransom payment in exchange for the deletion of Victim-2's stolen data.

13 h. Beginning on or about May 17, 2024, and through at least on or about
14 July 26, 2024, one or more of the co-conspirators conducted a complex series of
15 cryptocurrency transactions designed to hide the source and destination of the
16 ransom payment paid by Victim-2, including by converting the payments into
17 monero.

18 i. On or about May 23, 2024, May 25, 2024, and July 1, 2024, a co-
19 conspirator used portions of Victim-2's ransom payment to pay for overseas
20 technical infrastructure used to further the co-conspirators' crimes.

21 j. Between at least on or about August 15, 2024, and at least on or about
22 October 2, 2024, the co-conspirators demanded additional payments from Victim-2
23 to avoid publication, sale, and other unauthorized use of Victim-2's customers' data.

24 ***Victim-3***

25 k. Between at least on or about April 14, 2024, and at least on or about
26 May 24, 2024, MOUCKA and BINNS accessed Victim-3's Cloud Computing
27 Instance without authorization.

1 l. On or about April 17, 2024, and April 19, 2024, the co-conspirators
2 used Rapeflake on at least two different occasions to run searches within Victim-
3 3's Cloud Computing Instance and to obtain information, all without
4 authorization.

5 m. Between at least on or about April 14, 2024, and at least on or about
6 May 24, 2024, MOUCKA and BINNS exfiltrated customer records, including the
7 names, email addresses, residential addresses, dates of birth, and gift card numbers
8 belonging to millions of Victim-3's customers.

9 n. Between at least on or about May 29, 2024, and at least on or about
10 May 31, 2024, acting through an intermediary, the co-conspirators attempted to
11 extort Victim-3, demanding a ransom to prevent publication or further publication
12 of Victim-3's stolen data online.

13 o. On or about June 27, 2024, Co-Conspirator-1 posted on a
14 cybercriminal forum a link to download a copy of Victim-3's stolen data, which was
15 made accessible to computers anywhere in the world, including within the Western
16 District of Washington.

17 p. On or about June 28, 2024, the co-conspirators transferred or caused
18 to be transferred over 10 gigabytes of Victim-3's stolen data—to include names,
19 email addresses, residential addresses, dates of birth, and gift card numbers
20 belonging to millions of Victim-3's customers—to a computer located in the
21 Western District of Washington.

22 q. On or about July 10, 2024, Co-Conspirator-2 published on a
23 cybercriminal forum stolen personal identifying information belonging to dozens of
24 Victim-3's customers, including names and email addresses, which was made
25 accessible to computers anywhere in the world, including within the Western
26 District of Washington. In doing so, the co-conspirators attempted to extort Victim-
27 3, stating that they would release additional private information pertaining to

1 Victim-3's customers unless paid a ransom.

2 r. On or about October 1, 2024, the co-conspirators caused stolen
3 personal identifying information belonging to Victim 3's customers, including
4 names and email addresses, to be transferred to computers located in the Western
5 District of Washington.

6 *Victim-4*

7 s. Between at least on or about April 14, 2024, and at least on or about
8 May 18, 2024, MOUCKA and BINNS accessed Victim-4's Cloud Computing
9 Instance without authorization.

10 t. On or about April 17, 2024, the co-conspirators used Rapeflake to run
11 searches within Victim-4's Cloud Computing Instance and to obtain information,
12 all without authorization.

13 u. On or about May 27, 2024, Co-Conspirator-3 posted on a
14 cybercriminal forum an offer to sell stolen data associated with hundreds of millions
15 of Victim-4's customers. The same day, the co-conspirators posted sample data,
16 which included customers' account numbers and residential address information.

17 v. Between at least on or about May 24, 2024, and at least on or about
18 July 5, 2024, acting through an intermediary, the co-conspirators attempted to extort
19 Victim-4 to pay a ransom to prevent further publication of Victim-4's stolen data
20 online.

21 w. On or about September 27, 2024, the co-conspirators caused stolen
22 personal identifying information belonging to Victim 4's customers, including
23 account numbers and residential address information, to be transferred to computers
24 located in the Western District of Washington.

25 *Victim-5*

26 x. Between at least on or about May 24, 2024, and at least on or about
27 June 1, 2024, MOUCKA accessed Victim-5's Cloud Computing Instance without

1 authorization.

2 y. Between at least on or about June 11, 2024, and at least on or about
3 July 28, 2024, acting through an intermediary, the co-conspirators attempted to
4 extort Victim-5 to pay a ransom in order to prevent publication or further publication
5 of Victim-5's stolen data online.

6 z. On or about July 30, 2024, Co-Conspirator-2 posted on a
7 cybercriminal forum an offer to sell stolen personally identifying information,
8 including names and identification numbers belonging to over a million of Victim-
9 5's customers.

10 aa. On or about August 21, 2024, the co-conspirators caused stolen
11 personal identifying information belonging to Victim 5's customers to be transferred
12 to computers located in the Western District of Washington.

13 ***Victim-6***

14 bb. Between at least on or about April 17, 2024, and at least on or about
15 May 8, 2024, MOUCKA and BINNS accessed Victim-6's Cloud Computing
16 Instance without authorization.

17 cc. Between at least on or about April 17, 2024, and at least on or about
18 May 8, 2024, MOUCKA and BINNS exfiltrated private records, including names,
19 addresses, Social Security numbers, and payroll records for Victim-6's employees
20 across multiple countries, including the United States.

21 dd. On or about May 13, 2024, acting on behalf of MOUCKA and
22 BINNS, an intermediary contacted Victim-6 to begin ransom negotiations.

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

24 **COUNTS 2 THROUGH 6**

25 **(Computer Fraud and Abuse)**

26 8. The allegations set forth in paragraphs 1 through 7 of this Indictment are
27 realleged and incorporated as if fully set forth herein.

9. On or about the dates identified below, in King County, within the Western District of Washington, and elsewhere, and in an offense begun outside the jurisdiction of any particular state or district of the United States, CONNOR RILEY MOUCKA and JOHN ERIN BINNS did intentionally access, and aided and abetted accessing, protected computers, namely the private Cloud Computing Instances belonging to the below-identified victims, without authorization and thereby obtained and attempted to obtain information from protected computers for commercial advantage and private financial gain, in furtherance of the criminal acts of identity fraud and access device fraud in violation of Title 18, United States Code, Sections 1028(a)(7) and 1029(a)(2), and with the value of such information exceeding \$5,000.

Count	Approximate Date (On or About)	Defendant Charged	Description
2	Between at least on or about April 14, 2024, and at least on or about April 28, 2024	MOUCKA and BINNS	Accessed a Cloud Computing Instance belonging to Victim-2 and thereby obtained approximately 50 billion customer call and text records, including dialed numbers, for commercial advantage and private financial gain, in furtherance of identity theft, and the value of such information exceeding \$5,000.
3	Between at least on or about April 14, 2024, and at least on or about May 24, 2024	MOUCKA and BINNS	Accessed a Cloud Computing Instance belonging to Victim-3 and thereby obtained the names, email addresses, residential addresses, dates of birth, and gift card numbers of millions of Victim-3's customers, for commercial advantage and private financial gain, in furtherance of access device fraud and identity theft, and the value of such information exceeding \$5,000.
4	Between at least on or about April 14, 2024, until at least on or about May 18, 2024	MOUCKA and BINNS	Accessed a Cloud Computing Instance belonging to Victim-4 and thereby obtained account numbers and residential address information of Victim-4's customers, for commercial

1			advantage and private financial gain, in furtherance of identity theft, and the value of such information exceeding \$5,000.
2			
3			
4	5	Between at least on or about April 17, 2024, and at least on or about May 10, 2024	MOUCKA and BINNS
5			Accessed a Cloud Computing Instance belonging to Victim-6 and thereby obtaining names, addresses, Social Security numbers, and payroll records for Victim-6's employees across multiple countries, including the United States, for commercial advantage and private financial gain, in furtherance of access device fraud and identity theft, and the value of such information exceeding \$5,000.
6			
7			
8			
9			
10	6	Between at least on or about May 29, 2024, and at least on or about June 1, 2024	MOUCKA
11			Accessed a Cloud Computing Instance belonging to Victim-5 and thereby obtained personal identifying information, including names and identification numbers belonging to Victim 5's customers, for commercial advantage and private financial gain, in furtherance of identity theft, and the value of such information exceeding \$5,000.
12			
13			
14			
15			
16			

17 The Grand Jury alleges that each of these offenses occurred during, and in
 18 furtherance of, the conspiracy charged in Count 1.

19 All in violation of Title 18, United States Code, Sections 1030(a)(2)(C),
 20 1030(c)(2)(B)(i)-(iii), and 2.

21 **COUNTS 7 AND 8**

22 **(Extortion in Relation to Computer Fraud)**

23 10. The allegations contained in paragraphs 1 through 7 of this Indictment are
 24 realleged and incorporated as if fully set forth herein.

25 11. On or about the dates identified below, in King County, within the Western
 26 District of Washington, and elsewhere, and in an offense begun outside the jurisdiction of
 27 any particular state or district of the United States, CONNOR RILEY MOUCKA, with

1 intent to extort from persons money and things of value, transmitted in interstate and
 2 foreign commerce, and aided and abetted transmitting, communications containing threats
 3 to impair the confidentiality of information obtained from protected computers without
 4 authorization.

Count	Approximate Date (On or About)	Description
7	June 20, 2024	Threat to disclose information stolen from Victim-4's Cloud Computing Instance unless a ransom was paid.
8	July 10, 2024	Threat to disclose information stolen from Victim-3's Cloud Computing Instance unless a ransom was paid.

11 The Grand Jury alleges that each of these offenses occurred during, and in
 12 furtherance of, the conspiracy charged in Count 1.

13 All in violation of Title 18, United States Code, Sections 1030(a)(7)(B),
 14 1030(c)(3)(A), and 2.

15 **COUNTS 9 THROUGH 18**
 16 **(Wire Fraud)**

17 12. The allegations contained in paragraphs 1 through 3 of this Indictment are
 18 realleged and incorporated as if fully set forth herein.

19 **Scheme and Artifice to Defraud**

20 13. Beginning on a date unknown, but no later than in or about November 2023
 21 and continuing through at least October 10, 2024, in King County, within the Western
 22 District of Washington, and elsewhere, and in an offense begun outside the jurisdiction of
 23 any particular state or district of the United States, CONNOR RILEY MOUCKA, JOHN
 24 ERIN BINNS, and others known and unknown to the Grand Jury, devised and intended to
 25 devise a scheme to defraud Victim-1 and Victim-1's customers, including Victims 2
 26 through 6 and others, to obtain money and property by means of materially false and
 27

1 fraudulent pretenses, representations, and promises.

2 **Essence of the Scheme**

3 14. The essence of the scheme and artifice to defraud is set forth in Paragraph 5
4 of this Indictment, which is realleged and incorporated as if fully set forth herein.

5 15. The essence of the scheme and artifice to defraud further included the
6 fraudulent and unauthorized use of credentials to access protected computer systems,
7 namely the Cloud Computing Instances belonging to Victims 1 through 6 and many others,
8 and to execute commands on those protected computer systems. The essence of the scheme
9 and artifice to defraud further included MOUCKA and BINNS implicitly representing that
10 logins and commands that they sent during the unauthorized accesses of the victims' Cloud
11 Computing Instances were authorized logins and commands rather than logins and
12 commands sent by persons using stolen credentials and without authorization.

13 16. The essence of the scheme and artifice to defraud further included the use of
14 the stolen or otherwise unlawfully obtained credentials in other ways for CONNOR RILEY
15 MOUKA and JOHN ERIN BINNS' own benefit, including stealing sensitive personal
16 identifying, financial, and other valuable information from those computers, using the
17 stolen data to fraudulently cause victims to pay ransoms, and selling and attempting to sell
18 that stolen data.

19 17. The essence of the scheme and artifice to defraud further included
20 fraudulently asserting that, if victims paid ransoms, the co-conspirators would delete the
21 co-conspirators' copies of the stolen data, return the data to the victims, and refrain from
22 further unauthorized dissemination of the victims' stolen data.

23 **Manner and Means**

24 18. The manner and means of the scheme and artifice to defraud are set forth in
25 Paragraphs 6-7 of this Indictment, which are realleged and incorporated as if fully set forth
26 herein.

1 **Execution of the Scheme and Artifice to Defraud**

2 19. On or about the dates set forth below, in King County, within the Western
 3 District of Washington, and elsewhere, and in an offense begun outside the jurisdiction of
 4 any particular state or district of the United States, CONNOR RILEY MOUCKA and
 5 JOHN ERIN BINNS, for the purpose of executing the scheme described above, caused to
 6 be transmitted, and aided and abetted the transmission of, by means of wire communication
 7 in interstate commerce, the writings, signs, signals, pictures, and sounds described below
 8 for each count, with each transmission constituting a separate count:

9

Count	Approximate Date (On or About)	Defendant Charged	Description
10 9	11 April 14, 2024	12 MOUCKA and BINNS	13 Used stolen credentials to fraudulently access the Cloud Computing Instance belonging to Victim-2 located in the State of Virginia from a computer located outside the United States.
14 10	15 April 17, 2024	16 MOUCKA and BINNS	17 Used stolen credentials to fraudulently access the Cloud Computing Instance belonging to Victim-6 located in the Netherlands, from a computer located outside the United States and through a computer located inside the United States.
18 11	19 April 24, 2024	20 MOUCKA and BINNS	21 Used stolen credentials to fraudulently access the Cloud Computing Instance belonging to Victim-2 located in the State of Virginia from a computer located outside the United States.
22 12	23 May 2, 2024	24 MOUCKA and BINNS	25 Used stolen credentials to fraudulently access the Cloud Computing Instance belonging to Victim-4 located in the State of Oregon from a computer located outside the United States and through a computer located within the Western District of Washington.
26 13	27 May 3, 2024	MOUCKA and BINNS	Used stolen credentials to fraudulently access the Cloud Computing Instance belonging to Victim-4 located in the State of Oregon from a computer located outside the United States and through a computer located within the Western District of Washington.

14	May 3, 2024	MOUCKA and BINNS	Used stolen credentials to fraudulently access the Cloud Computing Instance belonging to Victim-3 located in the State of Oregon from a computer located outside the United States through a computer located within the Western District of Washington.
15	June 1, 2024	MOUCKA	Used stolen credentials to fraudulently access the Cloud Computing Instance belonging to Victim-5 located in the State of Virginia from a computer located outside the United States.
16	June 28, 2024	MOUCKA and BINNS	Caused the stolen personal identifying information of Victim-3's customers to be electronically transmitted from outside the State of Washington to a computer located within the Western District of Washington.
17	October 1, 2024	MOUCKA	Caused the stolen personal identifying information of Victim-5's customers to be electronically transmitted from outside the State of Washington to a computer located within the Western District of Washington.
18	October 1, 2024	MOUCKA and BINNS	Caused the stolen personal identifying information of Victim-3's customers to be electronically transmitted from outside the State of Washington to a computer located within the Western District of Washington.

The Grand Jury alleges that each of these offenses occurred during, and in furtherance of, the conspiracy charged in Count 1.

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

COUNTS 19 AND 20

(Aggravated Identity Theft)

20. On or about the below dates, in King County, within the Western District of Washington, and elsewhere, and in an offense begun outside the jurisdiction of any particular state or district of the United States, CONNOR RILEY MOUCKA and JOHN ERIN BINNS did knowingly transfer, possess, and use, and aided and abetted the transfer, possession, and use of, without lawful authority, the means of identification of another person specified below—a real person—during and in relation to the specified violations of Title 18, United States Code, Section 1343 that are charged above.

Count	Approximate Date (On or About)	Defendant Charged	Means of Identification and Related Count
19	June 1, 2024	MOUCKA	Username and password of a real person for a protected computer belonging to Victim-5 (Count 15)
20	June 28, 2024	MOUCKA and BINNS	Names, email addresses, residential addresses, and dates of birth, which belonged to real persons who were Victim-3's customers (Count 16)

The Grand Jury alleges that each of these offenses occurred during, and in furtherance, of the conspiracy charged in Count 1.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATIONS

21. The allegations contained in Counts 1–20 above are hereby realleged and incorporated by reference for the purpose of alleging forfeiture.

22. Upon conviction of the offense alleged in Count 1, CONNOR RILEY MOUCKA and JOHN ERIN BINNS shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of such offense; pursuant to Title 18, United States Code, Section 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to such offense; pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offense; and, pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of the offense, and any property, real or personal, constituting or derived from, any proceeds obtained, directly or indirectly, as a result of such offense. Such property includes, but is not

1 limited to, a judgment for a sum of money representing the amount of proceeds the
2 defendant obtained as a result of the offense.

3 23. Upon conviction of any of the offenses alleged in Counts 2–8, CONNOR
4 RILEY MOUCKA and JOHN ERIN BINNS shall forfeit to the United States, pursuant to
5 Title 18, United States Code, Section 982(a)(2)(B), any property constituting, or derived
6 from, proceeds obtained directly or indirectly, as the result of such offense; and, pursuant
7 to Title 18, United States Code, Section 1030(i), any personal property that was used or
8 intended to be used to commit or to facilitate the commission of the offense, and any
9 property, real or personal, constituting or derived from, any proceeds obtained, directly or
10 indirectly, as a result of such offense. Such property includes, but is not limited to, a
11 judgment for a sum of money representing the amount of proceeds the defendant
12 obtained as a result of the offense.

13 24. Upon conviction of any of the offenses alleged in Counts 9–18, CONNOR
14 RILEY MOUCKA and JOHN ERIN BINNS shall forfeit to the United States any
15 property, real or personal, which constitutes or is derived from proceeds traceable to such
16 offense. Such property is forfeitable pursuant to Title 18, United States Code, Section
17 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c), and includes, but
18 is not limited to, a judgment for a sum of money representing the amount of proceeds the
19 defendant obtained as a result of the wire-fraud scheme alleged above.

20 **Substitute Assets.** If any of the above-described forfeitable property, as a result of
21 any act or omission of the defendant,


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

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

5 A TRUE BILL: *yes*
6 DATED: *10/10/2024*

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

10 FOREPERSON

11 

12 TESSA M. GORMAN
13 United States Attorney

14 */s/ Nicole M. Argentieri*

15 NICOLE M. ARGENTIERI
16 Principal Deputy Assistant Attorney
17 General, Criminal Division

18 

19 ANDREW C. FRIEDMAN
20 Assistant United States Attorney

21 

22 LOUISA K. BECKER
23 Senior Counsel
24 Computer Crime & Intellectual Property
25 Section

26 

27 SOK TEA JIANG
Assistant United States Attorney



GEORGE BROWN
Trial Attorney
Computer Crime & Intellectual Property
Section