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. CR24-180 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

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

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

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

Relevant Individuals and Entities

3. At all times relevant to this Indictment:

a. CONNOR RILEY MOUCKA, also known as "Alexander Antonin Moucka," resided in Canada. MOUCKA used online accounts associated with particular nicknames known to the Grand Jury, including but not limited to "judische," "catist," "waifu," and "ellyel8."

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

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

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

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

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

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

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

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

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

The Conspiracy

4. Beginning on a date unknown, but no later than in or about November 2023 and continuing through at least October 10, 2024, CONNOR RILEY MOUCKA, JOHN ERIN BINNS, and others known and unknown to the Grand Jury, 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, did knowingly and willfully combine, conspire, confederate, and agree to commit:

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

a. Computer fraud, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i)–(iii), and 1030(a)(7)(B) and 1030(c)(3)(A);

b. Wire fraud, in violation of Title 18, United States Code, Section 1343; and

c. Aggravated identity theft, in violation of Title 18, United States Code, Section 1028A.

Goal of the Conspiracy

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

Manner and Means of the Conspiracy

6. It was part of the conspiracy that:

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

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

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

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

they dubbed "Rapeflake" to identify valuable information residing within the victims' Cloud Computing Instances, including organization names, user roles, and Internet Protocol ("IP") addresses, among other information.

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

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

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

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

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

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

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

Overt Acts

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

Victim-1

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

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

Victim-2

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

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

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

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

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

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

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

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

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

Victim-3

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

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

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

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

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

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

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

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

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

Victim-3's customers unless paid a ransom.

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

Victim-4

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

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

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

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

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

Victim-5

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

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

authorization.

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

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

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

Victim-6

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

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

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

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

COUNTS 2 THROUGH 6

(Computer Fraud and Abuse)

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

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

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

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

			advantage and private financial gain, in furtherance of identity theft, and the value of such information exceeding $5,000.
5	Between at least on or about April 17, 2024, and at least on or about May 10, 2024	MOUCKA and BINNS	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	Between at least on or about May 29, 2024, and at least on or about June 1, 2024	MOUCKA	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.

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 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2.

COUNTS 7 AND 8

(Extortion in Relation to Computer Fraud)

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

11. 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, with

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

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

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 1030(a)(7)(B), 1030(c)(3)(A), and 2.

COUNTS 9 THROUGH 18

(Wire Fraud)

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

Scheme and Artifice to Defraud

13. 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 any particular state or district of the United States, CONNOR RILEY MOUCKA, JOHN ERIN BINNS, and others known and unknown to the Grand Jury, devised and intended to devise a scheme to defraud Victim-1 and Victim-1's customers, including Victims 2 through 6 and others, to obtain money and property by means of materially false and

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

fraudulent pretenses, representations, and promises.

Essence of the Scheme

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

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

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

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

Manner and Means

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

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

Execution of the Scheme and Artifice to Defraud

19. On or about the dates set forth below, in King County, within the Western District of Washington, and elsewhere, 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, for the purpose of executing the scheme described above, caused to be transmitted, and aided and abetted the transmission of, by means of wire communication in interstate commerce, the writings, signs, signals, pictures, and sounds described below for each count, with each transmission constituting a separate count:

Count	Approximate Date (On or About)	Defendant Charged	Description
9	April 14, 2024	MOUCKA and BINNS	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.
10	April 17, 2024	MOUCKA and BINNS	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.
11	April 24, 2024	MOUCKA and BINNS	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.
12	May 2, 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.
13	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.

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

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.

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

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

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

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

23. Upon conviction of any of the offenses alleged in Counts 2–8, 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; 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 limited to, a judgment for a sum of money representing the amount of proceeds the defendant obtained as a result of the offense.

24. Upon conviction of any of the offenses alleged in Counts 9–18, CONNOR RILEY MOUCKA and JOHN ERIN BINNS shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to such offense. 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), and includes, but is not limited to, a judgment for a sum of money representing the amount of proceeds the defendant obtained as a result of the wire-fraud scheme alleged above.

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

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or,

e. has been commingled with other property which cannot be divided without difficulty,

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

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: yes
DATED: 10/10/2024

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

FOREPERSON

TESSA M. GORMAN
United States Attorney

/s/ Nicole M. Argentieri
NICOLE M. ARGENTIERI
Principal Deputy Assistant Attorney General, Criminal Division

ANDREW C. FRIEDMAN
Assistant United States Attorney

LOUISA K. BECKER
Senior Counsel
Computer Crime & Intellectual Property Section

SOK TEA JIANG
Assistant United States Attorney

GEORGE BROWN
Trial Attorney
Computer Crime & Intellectual Property Section

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