

**SUPERIOR COURT OF JUSTICE
(CENTRAL SOUTH REGION)**

IN THE MATTER OF an application pursuant to section 13 of the *Extradition Act* for a warrant for the provisional arrest of **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 IN THE MATTER OF an Application for a sealing order prohibiting public access to this Application

B E T W E E N:

**THE ATTORNEY GENERAL OF CANADA
ON BEHALF OF THE UNITED STATES OF AMERICA**

Applicant

and

**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**

Person Sought
for Extradition

AFFIDAVIT

I, Cst. [REDACTED] Whittington of the Royal Canadian Mounted Police, MAKE OATH

AND SAY AS FOLLOWS:

1. I am currently employed with the National Cybercrime Investigative Team with the Royal Canadian Mounted Police ("RCMP"). I am assigned to assist with the request from the United States of America for the extradition of **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 ("MOUCKA")**. As such, I have knowledge of the matters deposed to in this affidavit. I believe the information contained in this affidavit to be true.

2. I affirm this affidavit in support of an application by the Attorney General of Canada for a warrant for the provisional arrest of **MOUCKA**, pursuant to section 13 of the *Extradition Act* (the “Act”).

I. The Minister of Justice Canada has authorized the Attorney General of Canada to apply for a warrant of provisional arrest.

3. Attached as Exhibit “A” is a copy of the Minister’s authorization in this matter, dated October 25, 2024. It states that:

The United States of America has requested that Canada seek the provisional arrest of **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**.

The Attorney General of Canada is authorized to apply for a provisional arrest warrant.

II. It is Necessary in the Public Interest to Arrest MOUCKA, including to prevent him from escaping or committing an offence

4. Attached as Exhibit “B” is a copy of the Request for Provisional Arrest to Canada, which includes the Statement of Facts and Urgency (“Request”) in this matter, which I have read.

5. I believe it is necessary in the public interest to issue a warrant for the arrest of MOUCKA. My belief is based on the following information set out in the Request:

- a) Seriousness of the allegations: MOUCKA is wanted for prosecution in the U.S. for alleged computer intrusion/ransom offences. MOUCKA and his co-conspirators, including John Erin Binns, hacked into at least 10 companies’ protected computer networks, stole sensitive information, threatened to leak the stolen data unless the victims paid a ransom, and published, sold, or offered to sell this stolen data online.¹
- b) To date, MOUCKA and his co-conspirators have gained unlawful access to billions of sensitive customer records, including non-content call and text history records, banking information, medical information, Social Security

¹ Statement of Facts at p 1.

numbers, payroll records, and other personally identifiable information. The co-conspirators have successfully extorted at least \$2.5 million from at least three victims and continue to attempt to extort victims. Finally, the co-conspirators have posted, and continue to post, offers to sell victims' stolen data on cybercriminal forums.²

- c) Risk of flight: MOUCKA poses a serious risk of flight. He has the means to flee. He has earned at least approximately \$2.5 million in ransom payments for stolen data from Victim-1 customers already interviewed by the FBI.³
- d) Based on lawfully obtained screenshots from MOUCKA's iCloud account, MOUCKA controls a significant amount of cryptocurrency stored in wallets that have not yet been found by law enforcement, including an unknown bank account or crypto wallet showing a balance of \$3,496,076.97. These funds could be used to facilitate his flight and would support him afterwards.⁴
- e) Evidence also indicates MOUCKA is aware of the gravity of this case and the exposure he will face upon extradition to the United States. He has repeatedly discussed his operational security measures and attempts to delete evidence in order to evade identification and apprehension. MOUCKA has repeatedly purchased new laptops and deleted and created new accounts over the course of his offences.⁵
- f) The investigation has also revealed that MOUCKA has considered obtaining foreign citizenship. For example, in February 2024, he sent a message stating, "I can get dual citizenship to Czech Republic pretty sure. I want an eu passport." The U.S. authorities have no information about whether he has actually sought to do so.⁶
- g) Additionally, media outlets have contacted U.S. authorities about this matter and one outlet indicated it intends to name MOUCKA in an article to be submitted for publication on October 25, 2024. U.S. authorities believe that this publication would increase risk of flight and lead MOUCKA to destroy evidence and publish stolen information.⁷
- h) Risk of further criminality: Evidence gathered over the last several months also establishes that MOUCKA continues to be actively engaged in hacking activities. MOUCKA's campaign has involved the theft of terabytes of sensitive data from tens, if not hundreds, of victims. Additionally, MOUCKA has repeatedly extorted and re-extorted his victims, resulting in enormous and

² Statement of Facts at p 1.

³ Statement of Facts at p 16.

⁴ Statement of Facts at pp 13 and 16.

⁵ Statement of Facts at p 16.

⁶ Statement of Facts at p 16.

⁷ Statement of Facts at p 16.

ongoing harm not only to the corporations impacted but also the millions of individuals whose data was stored by these corporations.⁸

- i) MOUCKA and his conspirators continue to sell, publish, and otherwise leak this data online, and every day that he is allowed to remain free, his harms will continue. As recently as October 2024, MOUCKA attempted to re-extort at least one victim, repeatedly threatening to release more of this company's data even after the company paid a ransom. MOUCKA has also continued to publish private data stolen from victims online, and to aggressively market this data for sale. Stolen data was posted publicly at least as recently as on or about September 30, 2024.⁹
- j) Risk of danger to the public, to police, and to himself: MOUCKA poses an ongoing danger to the public, to police, and to himself. On January 10, 2024, MOUCKA, using his Nutz Discord Account, said "I think I'd make a really good serial killer" and repeatedly referenced committing mass killings and obtaining firearms.¹⁰
- k) MOUCKA also discussed committing suicide and suicide by cop on both January 11, 2024, and January 18, 2024; on the latter occasion, MOUCKA stated, "I think I want to do suicide by cop." In another message, MOUCKA stated, "I need guns to kill Canadians."¹¹

III. MOUCKA is in Canada

6. I believe that MOUCKA is in Canada and resides at [REDACTED], Kitchener, Ontario. My belief is based on the following:

- a) The Request states that MOUCKA's address is [REDACTED] Kitchener, Ontario.
- b) The Request states that MOUCKA's Apple account provides evidence of his identity, location and criminal activity. Specifically:
 - i. Apple records produced in response to legal process showed MOUCKA's account (i) was accessed from IP address 24.246.30.67 ["the Canadian IP Address"] over 500 times between April 1, 2023, and August 20, 2024; (ii) had a residential address of [REDACTED] Kitchener, Ontario, N2A 1X4, a phone number (250 [REDACTED]), and a machine ID of [REDACTED]; (iii) reflected numerous purchases using the Canadian IP Address between June 22 and July 8,

⁸ Statement of Facts at p 17.

⁹ Statement of Facts at pp 17-18.

¹⁰ Statement of Facts at p 18.

¹¹ Statement of Facts at p 18.

2024, including purchases of an iPhone 15 Pro, MacBook Air, and iPad Pro 1, all of which were billed to "Alexander Moucka" and shipped to [REDACTED] in Kitchener, Ontario, Canada ("Target Location"); and (iv) reflected payments on the account by an "Alexander Moucka" using both PayPal and Mastercard, some of which used the Canadian IP Address;¹²

- ii. U.S. authorities reviewed information stored in the Apple account's iCloud storage. iCloud is a file hosting, storage, and sharing service provided by Apple. Numerous photos in the Apple account's iCloud provide direct and circumstantial evidence of MOUCKA's involvement in the criminal activity and his location. For example, the iCloud account contains multiple photos of MOUCKA's Canadian passport, including one with full name Connor Riley Moucka, passport number [REDACTED], date of birth 18 August 1999, in Kitchener, Canada;¹³
 - iii. MOUCKA's Apple iCloud account contains (1) a screenshot of an order receipt for an iPad Pro that shipped to "Alexander Moucka" at [REDACTED] Kitchener, ON N2A 1X4; and (2) a Best Buy order receipt from July 2, 2024 for a SteelSeries wireless gaming headset, to be shipped to "Alexander Moucka" at [REDACTED] Kitchener, ON N2A1X4.
- c) The Request includes evidence that MOUCKA's Google account and Discord account have also been accessed at the same Canadian IP Address:
- i. A WHOIS lookup showed that the Canadian IP Address is provisioned by TekSavvy Solutions Inc., a Canadian service provider, and geolocates to Waterloo, Ontario, Canada.¹⁴
 - ii. Google account connormoucka5[at]gmail.com has also used the Canadian IP Address as recently as August 26, 2024.¹⁵
 - iii. IP records from Discord showed that the user of the Nutz Discord Account logged into the account from the Canadian IP Address over 3,350 times between October 28, 2023, and April 4, 2024.¹⁶
- d) On October 21, 2024, officers of the RCMP attended at [REDACTED] Kitchener, Ontario, to confirm that MOUCKA resides at that location. Shortly after 2:20pm, a plain clothes officer knocked on the front door and rang the bell. MOUCKA answered the door and identified himself as "Alex". At one point,

¹² Statement of Facts at pp 11-12.

¹³ Statement of Facts at p 12.

¹⁴ Statement of Facts at p 15.

¹⁵ Statement of Facts at p 15.

¹⁶ Statement of Facts at p 15.

MOUCKA said "You woke me up Sir". The plain clothes officer observed that MOUCKA was disheveled and very obviously freshly-awoken.

- e) Attached as Exhibit "C" are photographs of MOUCKA taken by the surveillance team on October 21, 2024. I have compared these photographs to the photographs attached to the Request and confirm and it is one and the same person.

7. The Request describes the person sought with the following identifiers:

Name (include A/K/As): Connor Riley Moucka a.k.a. Alexander Antonin Moucka
Country(ies) of Citizenship: Canada
Date(s) of Birth: August 18, 1999
Place of Birth: Kitchener, Ontario, Canada
Race: White
Gender: Male
Hair Color: Brown
Eye Color: Brown

IV. A Warrant for MOUCKA's Arrest has been issued

8. Included at Exhibit "B" in the Request is a copy of the warrant for the arrest of MOUCKA issued by the United States District Court for the Western District of Washington on October 10, 2024.

V. Sealing Order

9. It is requested that this court file be sealed, until MOUCKA is arrested, at which point the court file can be unsealed. The grounds for the sealing order are as follows: If MOUCKA were to become aware of this court file and its contents before his arrest, the risk of flight would increase, as would the risk that he might attempt to delete or destroy evidence in order to evade apprehension and identification. Furthermore, as stated above, MOUCKA poses a danger to the public, to police, and to himself, and those risks would be elevated if he were to become aware of this court file and its contents before police are able to execute his arrest.

SWORN REMOTELY pursuant to)
O.Reg 431/20 by [redacted] Whittington)
stated as being located in the City of)
Ottawa in the Province of Ontario,)
before me at the City of Vaughan,)
in the Province of Ontario on)
October 28, 2024.)

Axmith, Lynne

Digitally signed by Axmith, Lynne
DN: C=CA, O=GC, OU=Jus-Jus, CN="Axmith, Lynne"
Reason: I am approving this document with my legally
binding signature
Location:
Date: 2024.10.28 08:10:46-04'00'
Foxit PDF Editor Version: 13.1.0

Lynne Axmith
A commissioner in and for the
Province of Ontario, City of Toronto
for the Government of Canada,
Department of Justice
Expires January 11, 2026

Whittington, [redacted] Digitally signed by [redacted]
[redacted],000207711 [redacted] 0207711
Date: 2024.10.28 08:06:21 -04'00'
[redacted] Whittington

This is Exhibit "A" referred to in the affidavit of Jaclyn Whittington sworn before me this 28th day of October, 2024.

Axmith, Lynne

Digitally signed by Axmith, Lynne
DN: c=CA, o=GC, ou=Jus-Imm, cn="Axmith, Lynne"
Reason: I am approving this document with my legally binding
signature
Location:
Date: 2024.10.28 08:11:19-0400
Font: PDF, Embed Version: 13.1.0

A Commissioner for taking Affidavits

Form 1
Section 12 - Authority to apply for a
provisional arrest warrant

TO: The Attorney General of Canada

In the matter of an extradition request pursuant to the provisions of the *Extradition Act*, S.C. 1999, c.18

SUPERIOR COURT OF JUSTICE

BETWEEN:

**THE ATTORNEY GENERAL OF CANADA
(on behalf of the United States of America)**

- and -

**CONNOR RILEY MOUCKA
AKA ALEXANDER ANTONIN MOUCKA; JUDISCHE;
CATIST; WAIFU; AND ELLYEL8**

**AUTHORIZATION TO APPLY
FOR A PROVISIONAL ARREST WARRANT
(Section 12 *Extradition Act*)**

The United States of America has requested that Canada seek the provisional arrest of Connor Riley Moucka AKA Alexander Antonin Moucka; judische; catist; waifu; and ellyel8.

The Attorney General of Canada is authorized to apply for a provisional arrest warrant.

DATED at Gatineau, Quebec, on the 25th day of October 2024.



Vicky Liew, Counsel,
International Assistance Group
for the Minister of Justice of Canada

This is Exhibit "B" referred to in the affidavit of Jaclyn Whittington sworn before me this 28th day of October, 2024.

Axmith, Lynne
A Commissioner for taking Affidavits

Digitally signed by Axmith, Lynne
DN: C=CA, O=GC, OU=Jus-Jus, CN="Axmith, Lynne"
Reason: I am approving this document with my
legally binding signature
Location:
Date: 2024.10.28 08:11:50-0400'
Font: PDF Editor Version: 12.1.0

REQUEST FOR PROVISIONAL ARREST TO CAN

RETURN COMPLETED FORM TO:

Office of International Affairs
Criminal Division
U.S. Department of Justice

Phone: (202) 514-0000
Fax: (202) 514-0080

STATE/DISTRICT REQUESTING PA: U.S. Attorney's Office for the Western District of Washington; Computer Crime & Intellectual Property Section, Criminal Division

A. IDENTIFICATION OF FUGITIVE:

Name (include A/K/As): Connor Riley Moucka, a/k/a Alexander Antonin Moucka

Country(ies) of Citizenship: Canada

Date(s) of Birth: August 18, 1999 Place of Birth: Kitchener, Ontario, Canada

Proof of Citizenship attached (if U.S. citizen): (e.g., passport, naturalization or birth certif.)

Race: White Gender: male female

Height: 183cm Weight: Unknown Hair Color: Brown Eye Color: Brown

Scars/Other Characteristics: N/A

Photograph Attached: Yes Fingerprints Attached: No

Driver's License No.: [REDACTED] State issued: Ontario

Passport No.: [REDACTED] Date & Place Issued: Jan. 16, 2017, Denver (Canadian passport)

Nat'l ID Card No.: N/A Date & Place Issued: N/A

Specific Address/Exact Location in Canada: [REDACTED] Kitchener, Ontario N2A1X4

If in custody in Canada, Charges & Anticipated Date of Release: N/A

Canadian law enforcement contact in Canada (NOT U.S. contact in Canada) with knowledge of facts, fugitive's location.

Name & Title: Cpl. David Kennealy
Agency: Royal Canadian Mounted Police

Law enforcement contact in U.S. with knowledge of facts, fugitive's location:

Name & Title: Special Agent Hannah Trepte
Agency: Federal Bureau of Investigation

B. CHARGES AND BASIS FOR REQUEST

1. U.S. Charging Or Commitment Document (attach copy)

Check One: X Indictment
 Superseding Indictment
 Complaint
 Judgment/conviction order
 Other (DESCRIBE)

Number: CR24-180 LK
Date Filed: October 10, 2024
Name and Location of Court: U.S. District Court for the Western District of
Washington; Seattle, Washington

Has the Charging Document been unsealed (or, been unsealed for the limited purpose of sharing the U.S. State Department and a foreign government for purposes of extradition)?

YES X NO

2. Minimum Sentence

Offenses for which extradition is requested are punishable by at least one year in prison:
YES X NO

3. Statute of Limitations (attach copy)

Does statute of limitations preclude prosecution or incarceration?
YES NO X

4. **U.S. Arrest Warrant** (attach copy)

Fugitive is wanted to (check one): Stand Trial
 Be Sentenced
 Serve a Sentence
 Serve Remaining Sentence (indicate how much left to serve) _____

Number: CR24-180-1 LK
Date Filed: October 10, 2024
Issued By: U.S. District Court for the Western District of Washington
Name and Location of Court: U.S. District Court for the Western District of Washington; Seattle, Washington

C. REQUESTING AUTHORITY, AUTHORIZATION, AND FINANCIAL COMMITMENTS

1. Requesting Authority

Federal District U.S. Attorney's Office for the Western District of Washington

2. Prosecutor Authorization

Provide the name of the prosecutor authorizing this PA request:

Name: George Brown
Title: Trial Attorney, Computer Crime & Intellectual Property Section

BY SUBMITTING THIS FORM, THE PROSECUTOR COMMITS TO:

(1) PREPARING A FORMAL EXTRADITION REQUEST WITHIN THE TIME SPECIFIED BY OIA UPON THE ARREST OF THE FUGITIVE IN CANADA; AND

(2) ACCEPTING RESPONSIBILITY FOR EXTRADITION-RELATED COSTS.

Statement of Facts
Supporting the Provisional Arrest of Connor Riley Moucka

Statement of Facts

The information set forth in this request has been gathered by U.S. authorities from approximately April 2024 through the present and includes information from (a) U.S. and foreign victim companies, including information from interviews and victim computer systems; (b) U.S. and foreign service providers, including information lawfully obtained via search warrants, court orders, and other legal demands; and (c) open-source information and information provided by private sector incident response companies and other persons.

U.S. authorities are investigating MOUCKA, who also uses various online monikers, including, but not limited to, judische, catist, waifu, and ellyel8. MOUCKA also claimed to an online girlfriend in a Discord chat that he changed his name to Alexander, but his “birth name” “is actually Connor.” Discord is an online communications and messaging company.

MOUCKA and his co-conspirators, including John Erin Binns, hacked into at least 10 companies’ protected computer networks, stole sensitive information, threatened to leak the stolen data unless the victims paid a ransom, and published, sold, or offered to sell this stolen data online.

Many of the victims in this investigation were storing data with a U.S. software-as-a-service company (Victim-1). Victim-1 provides cloud computing “instances” to its customers, which provide cloud data analysis capabilities. These cloud computing instances store data of Victim-1’s customers, and Victim-1 generally collects some IP logging information on behalf of its customers. Victim-2 through Victim-5 are customers of Victim-1.

MOUCKA and his co-conspirators targeted companies with a common utility (dubbed “rapeflake” by the hackers and “Frostbite” by security researchers). This utility is a software tool that the co-conspirators used to perform reconnaissance on Victim-1 instances. Private sector security researchers have determined that “rapeflake” could be used to query information from databases. To date, MOUCKA and his co-conspirators have gained unlawful access to billions of sensitive customer records, including non-content call and text history records, banking information, medical information, Social Security numbers, payroll records, and other personally identifiable information. The co-conspirators have successfully extorted at least \$2.5 million from at least three victims and continue to attempt to extort victims. Finally, the co-conspirators have posted, and continue to post, offers to sell victims’ stolen data on cybercriminal forums.

Infiltration and Stealing of Data from Victim companies

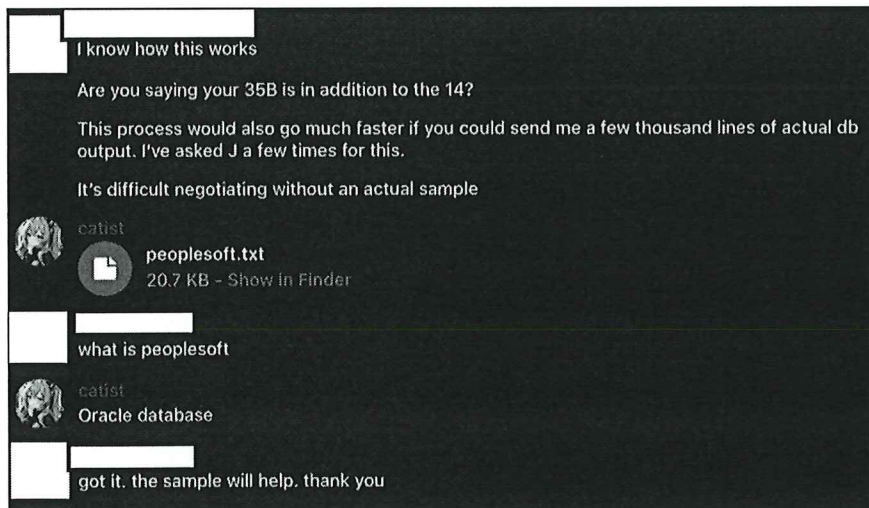
Victim-1 customers targeted by MOUCKA and his co-conspirators have provided evidence of the following hacking and extortion activities.

Victim 2

Victim-2 is a major U.S. telecommunications company and wireless network operator. As discussed below, U.S. authorities determined that MOUCKA and at least one co-conspirator, John Erin Binns, successfully hacked into Victim-2's computer systems and stole approximately 50 billion call and text records (but not the content of the calls or texts) belonging to Victim-2 and its customers, which MOUCKA and his co-conspirators monetized by extorting Victim-2.

On April 19, 2024, the FBI received information suggesting that a threat actor had obtained unauthorized access to Victim-2's computer networks. The FBI lawfully obtained screenshots of Telegram chat messages with a user serving as an intermediary, Individual-1, as well as another user labeled "J (irdev)," later discovered to be John Erin Binns. Binns confirmed to Individual-1 that he had call records with "14 billion entries" from Victim-2 and requested the phone number of an FBI agent who had previously investigated Binns for another breach into a different U.S. telecommunications provider, for which Binns was previously charged in the Western District of Washington.

The FBI approached Victim-2, which confirmed that it had been breached and that the sample data Individual-1 received in the Telegram chats was real Victim-2 customer data. The FBI also lawfully obtained copies of Telegram communications between Individual-1 and the Telegram username @judische (labeled with the display name "catist") which contained a sample of Victim-2's data. Victim 2 confirmed the data is authentic:



The Judische Telegram account was later determined to be MOUCKA, as described below.

Victim-2 used an outside incident response firm to conduct an investigation and determined that a machine-to-machine credential had been compromised and used to access Victim-2's cloud instance without authorization. Furthermore, the firm determined that particular IP addresses were used by the threat actors to access Victim-2's cloud instance and exfiltrate hundreds of gigabytes

of Victim-2's information. These included a specific IP address ("malicious IP address") from which the malicious actor connected to Victim-2's cloud instance on approximately April 14 and 15, 2024. Information from Victim-2 indicated that the malicious IP address was hosted by a U.K. provider. The U.S. authorities also sent legal process to the U.K. provider. As discussed below, Binns logged into one of his communications accounts from the malicious IP address around the same time that the data exfiltration occurred.

The FBI obtained logs of sessions, authentication, and jobs from Victim-1. Combined with logs from Victim-2 showing the amount of data exfiltrated from its cloud instance, these logs provided details about the intrusions that occurred between at least April 14 through at least April 28, 2024, during which time malicious IP addresses that were not part of Victim-2's normal activities conducted unauthorized activities on its system. Victim-2's logs further show that hundreds of gigabytes of data were exfiltrated.

Victim-1 also has access to its customer's logs. These logs provide IP addresses used by the threat actors. The FBI combined information from the logs of Victim-1 and Victim-2 to confirm that Victim-2's data was successfully exfiltrated on April 14, 2024, April 15, 2024, and April 24, 2024, and to confirm the IP addresses used in the intrusions.

The lawfully obtained Telegram chats between MOUCKA, Binns, and Individual-1 contain detailed, inculpatory information about the activity of MOUCKA and Binns and confirm that MOUCKA was actively inside of Victim-2's systems. For example, on April 23, 2024, a person using the @judische moniker, later determined to be MOUCKA as explained below, told Individual-1, "I can search yeah, or he [Binns] can. He understands the structure of the data better than I do, I just provided access to him." The FBI determined that "he" referred to Binns because of the information above that Binns had already exfiltrated some Victim-2 information approximately a week before these messages. Binns also messaged Individual-1 on April 22, 2024, stating, "My partner is trying to get more data"—referring to MOUCKA. MOUCKA, while using the @judische Telegram username, had the following conversation with Individual-1 on April 23, 2024:

MOUCKA: . . . Did he tell you how many lines he has?
Individual-1: 14billion or something like that
MOUCKA: this many for the current month 34356004473 / 34 billion
Individual-1: Wait what? You have access to live data?
MOUCKA: yes
Individual-1: Or you can just see it
MOUCKA: live
Individual-1: And you can download it)??
MOUCKA: Yes / I can download or query
Individual-1: Whoah
MOUCKA: I can also delete and add

The same day, MOUCKA also talked about the data that “he has exfiltrated and indexed at 14B,” suggesting Binns had already downloaded 14 billion records. The next day, MOUCKA discussed his ongoing exfiltration of approximately 34 billion records:

MOUCKA: “He [Binns] has 14B September and I’ll have 35B October”

Individual-1: “ok well get what you can. it just adds more value”

MOUCKA: “okay good, I’ll get as much as I can”

MOUCKA: “Can try to get 34B sept and 35B Oct”

On April 24, 2024, MOUCKA, Binns, and Individual-1 started a Telegram group chat to discuss selling Victim-2’s information. As noted above, Victim-2 provided the U.S. authorities with information confirming a large amount of data was exfiltrated on April 14, April 15, and April 24.

Victim-2 also communicated and negotiated with Individual-1 about a ransom demand in May, 2024. It ultimately paid a ransom to have the stolen data deleted from the server on which the co-conspirators were storing it. Victim-2 confirmed that it has been re-extorted in the last few weeks. Specifically, Individual-1 contacted them again, on behalf of “catist” (MOUCKA), and engaged in ransom negotiations.

Victim 3

Victim-3 is a major retailer located in the United States. On or about May 23, 2024, a well-known computer security and incident response company notified Victim-3 that it was a potential victim of a similar computer intrusion. On May 29, 2024, representatives from Victim-3 met with the FBI and confirmed that three categories of its information had been stolen from its cloud instance, including customer information for approximately 20 million customers, gift card information, and internal company business documents. Victim-3 also stated that it was actively negotiating through the same intermediary, Individual-1, that negotiated with Victim-2.

The FBI also reviewed logs provided by Victim-1, which indicated that Victim-3’s instance was accessed without authorization from approximately April 14, 2024, through May 24, 2024 and that the rapeflake utility was deployed on Victim-3’s computer systems. (As discussed below, MOUCKA claimed to have written the rapeflake utility.) Victim-3 hired an incident response company to investigate the breach and confirmed its instance had been compromised using stolen login credentials belonging to a former contractor located outside the United States. According to the incident response firm’s investigation, this former contractor’s credential was likely compromised via a credential stealer in approximately 2021 and available in cybercriminal marketplaces as early as May 2021. Stolen credentials are generally available for free and for purchase on the dark web.

U.S. authorities obtained and reviewed written records provided by Victim-3, including emails with Individual-1. On May 24, 2024, two members of Victim-3’s information security team were contacted via LinkedIn by Individual-1, who used his true name. Individual-1 offered to broker a deal with the hacker and provided a sample of the data. Individual-1 later requested a

phone call with Victim-3 and spoke to Victim-3's counsel. On May 29, 2024, Individual-1 indicated that he thought they "c[ould] close around [\$]275[,000]." Then, on or about May 30, 2024, Individual-1 emailed Victim-3 that the threat actor wanted \$450,000.

Individual-1 subsequently informed Victim-3 that another victim had paid a substantial ransom. After several email exchanges and at least one telephone call with Individual-1, Victim-3 ceased communications.

In or about June 2024, a co-conspirator created a post on BreachForums and stated they were making the Victim-3 database available for download after Victim-3's refusal to pay a ransom. The FBI discovered this post, which included a link for download. The FBI accessed this link and downloaded approximately 10.6 GB of compressed materials. When unpacked, the data was approximately 86.1 GB and contained numerous files with filenames that matched queries run by the threat actors in Victim-1's logs for Victim-3's instance. The FBI downloaded the data from BreachForums and verified that it was consistent with the information from Victim-3's investigation. Specifically, the downloaded data included customer names, emails, billing addresses, personal identifying information, purchase information, and full gift card numbers with expiration dates.

The FBI sent the first 30 lines of the tables of the downloaded data to Victim-3, which confirmed that it was a true and accurate representation of its data, with minor modifications (the timestamps were off in some instances and there were some duplicated rows).

As part of ongoing extortion efforts involving Victim-3 data, a co-conspirator posted on BreachForums another sample of Victim-3's data for sale in or about July 2024.

The post demanded a ransom payment, which Victim-3 never paid.

Victim 4

Victim-4 is a major U.S. entertainment and marketing company. The FBI obtained logs about Victim-4's cloud computing instance from Victim-1. According to those logs, the threat actors breached Victim-4's cloud instance from at least on or about April 14, 2024, through at least May 18, 2024. Victim-4 informed FBI that the types of data stolen included names, contact information, partial payment card numbers, and in some instances driver's license numbers and/or passport numbers. Additionally, Victim-4 confirmed that only one account on its Victim-1 cloud computing instance had been breached.

On or about May 17, 2024, Victim-4 learned about a potential breach, which it later confirmed. On May 29, 2024, the FBI interviewed Victim-4 and discovered it was investigating a breach of its Victim-1 cloud computing instance in which threat actors may have stolen information related to its customers' contact information and payment card information. Victim-4 reviewed logs from its cloud instance and learned the actors accessed their instance without authorization.

In or about May 2024, a co-conspirator posted on the cybercriminal forum Exploit.in a sale of Victim-4's data that purportedly included millions of users and payment card details. The post

included sample data without any names but with sale order IDs, account numbers, account created data, and partial addresses. The FBI subsequently visited this post in or around June 2024 and September 2024.

The FBI learned that the information offered for sale was not the same as the data stolen from Victim-4, but Victim-4 stated that it appeared to have some overlap with what was stolen from their Victim-1 instance, suggesting that the threat actors were potentially mixing data.

During this same time period, Individual-1 contacted Victim-4 several times offering to act as an intermediary between Victim-4 and the threat actors and/or advising about MOUCKA's use of the data. For example, on June 20, 2024, Individual-1 reached out to two different people associated with Victim-4 via email. In one communication, Individual-1 stated, "[t]he hacker has recently leaked 1 million user records and is threatening to leak more. They have also dropped their price point to about 100k USD. At that price, I imagine they will sell it at least 3-4x."

In or about July 2024, Individual-1 indicated that he had been "extremely successful in the past in getting his demands down to a more reasonable amount." Individual-1 attached a BreachForums post, which included an extortion attempt.

As part of continued extortion attempts, a co-conspirator made a subsequent post on a cybercriminal forum in an attempt to extort Victim-4.

In early October 2024, MOUCKA posted a poll on Telegram using another account believed to be controlled by him with display name "scarlet the meow cat" and username @nyakira. In the poll, he asked people to vote on whether he should leak more of Victim-4's data; the post was lawfully reviewed by U.S. authorities. Victim-4 never paid a ransom.

Victim 5

Victim-5 is a large foreign corporation headquartered in Europe. On or about May 9, 2024, the FBI notified Victim-5 about a potential breach of its computer systems.

In the Telegram chats provided to the FBI by Individual-1, "ellye18", who was later identified as MOUCKA as shown below, discussed having ongoing access to Victim-5 as of April 25, 2024. MOUCKA stated:

Individual-1: wait. you have access to [Victim-5]??

MOUCKA: Yes [Victim-5] lol

Individual-1: that might be too big for now. we might want to start smaller

Individual-1 and MOUCKA also discussed the nature of the data MOUCKA had access to, and MOUCKA stated that he focused on "HR" data first. MOUCKA later stated, "yeah for [Victim-5] let me figure out the best way to query that many mssql without the data masks but without altering the schema to remove the mask bc they might notice."

The FBI provided Victim-5 with a screenshot of sample HR data from the Telegram chats and initial indicators of compromise. Victim-5 conducted an internal investigation and subsequently validated the data from the screenshot, confirmed that its Victim-1 instance had been breached, verified that the initial breach occurred on or about April 17, 2024, and indicated that the breach continued through at least May 10, 2024. According to Victim-5’s internal investigation and a review of their logs, this breach was the result of compromised credentials of two employees. The stolen data included names, addresses, company identification numbers, and payroll accounts for employees across multiple countries, including in the United States.

Victim-5 subsequently informed the FBI that three types of data had been exfiltrated. First, Victim-5’s employee data, including those of employees based in the United States, had been stolen, which included employees’ names, social security numbers, and addresses, as well as company payroll records.

Victim-5 provided the extortion emails that it received to the FBI. These included an email from the same intermediary, Individual-1. On May 13, 2024, Individual-1 notified Victim-5 that the “threat actor” was “actively downloading” Victim-5’s data, and provided some sample data and a link to another account with additional data. Victim-5 downloaded sample data from Individual-1 and verified that it contained Victim-5’s data.

The FBI also compared IP records from Victim-5’s logs with the login records for a Discord account controlled by Binns (the Irdev Discord Account). The FBI’s comparison showed that common IP addresses were used to log into both Victim-5’s network and Binns’s Irdev Discord Account, within short timeframes and via one of the same providers, as follows:

IP Address	Irdev Discord (UTC)	Victim-5 (UTC)	ISP
194.230.144.126	4/18/2024 10:48	4/18/2024 11:10	Sunrise (Switzerland)
194.230.144.126	4/18/2024 12:51	4/18/2024 11:45	Sunrise (Switzerland)

Additional Victims

Based on widespread reporting, as well as published analyses by security research firms, U.S. authorities are aware of over 100 other companies that may have been victim to similar computer intrusions conducted by some of the same co-conspirators and using a similar methodology. The FBI has communicated with several U.S. and foreign companies who believe they were victims of similar computer intrusions by the same actors and confirmed at least 10 companies’ cloud instances that were accessed without authorization. Victims generally are Victim-1 customers, many of whom were targeted using “rapeflake.” Many victims received samples of their stolen data and were extorted in similar ways.

Three Key Discord Accounts Are Controlled by MOUCKA and Linked to the Intrusions

U.S. authorities reviewed IP logs from the intrusions into victim companies and identified malicious IP addresses at specific times. U.S. authorities then obtained court orders requiring

electronic communication service providers to identify accounts that had been accessed by the malicious IP addresses at specific dates and timestamps. Discord identified accounts accessed from the malicious IP addresses during the same time periods of the intrusions, and the government then obtained search warrants on various accounts, as U.S. authorities learned that the threat actor would delete and create numerous accounts. U.S. authorities determined that three identified accounts were controlled by MOUCKA and provided key evidence of his identity: (i) User ID 547214862313455626, with unique username azurape (the Azurape Discord Account); (ii) User ID 1166162535477678110, with prior unique username zzzzzzzzzzzzzzzzzzzzznutz (the Nutz Discord Account); and (iii) User ID 750491727025930364, with unique username wetworkmakeitrain (the Wetwork Discord Account).

Most importantly, the Azurape Discord Account directly links MOUCKA to the @judische Telegram account that used the rapeflake tool to steal information from companies, as discussed above. For example, approximately 10 days after a security firm published a report about this hacking campaign, the Azurape Discord Account claimed ownership of the @judische Telegram account and subsequently sent a link to another Discord user to a public report from a computer security company about the Victim-1 hack, stating “you can extrapolate to whom this articles about” [sic]:

Timestamp	Username	Contents
		i think i mentioned [redacted] to you a few weeks before news hit; you can extrapolate to whom this articles about and i can tell you the amount this very low effort campaign made at high 7 figures now as a test run. i would prospect you for my team if you aren't scared that it's high-risk, i would assert it's not or i'd be in jail probably before we even discussed WS2k3 ROP with cat_warrior/rdynamic in jan 2019. if you would accept first round of this i would introduce you to the lead developer on my team and you can see if you have chemistry or decline if you don't. USA won't even exist in 10 years either, keep in mind. none of us are stupid, we won't get caught so you don't need to judge any of our characters if we'll snitch or not.
2024-06-19 01:08:31.906000+00:00	azurape#0	https://cloud.google.com/blog/topics/threat-intelligence/unc553 [redacted] data-theft-extortion
2024-05-22 14:43:10.434000+00:00	azurape#0	bitcoin or any crypto ur okay with and ill say the rest on tg
2024-05-22 14:42:50.043000+00:00	azurape#0	@judische
2024-05-21 23:37:38.789000+00:00		whats your tg /i message you there
2024-05-21 23:34:39.496000+00:00	[redacted]	depends, whats the specific work and whats the compensation
2024-05-21 23:32:28.480000+00:00	azurape#0	do u want to work?

In addition to this May 2024 example, Azurape identified @judische as his Telegram moniker in February 2024 and April 2024 to other users in Discord chat messages.

Around late May 2024, the Azurape Discord Account stated that “all i can do is hack” and that “i had [a co-conspirator] post [Victim-4] sample sales threat and they instantly started to negotiate.” Shortly thereafter, in mid-June 2024, MOUCKA used the Azurape Discord Account to ask a third party for “help decrypt[ing] [Victim-4] creditcards” in exchange for “2m.” About two days later, the Azurape Discord Account said, “hopefully they do not find the code for rapeflake” because “its clear i wrote it.”

Between December 2023 and February 2024, the Azurape Discord Account repeatedly communicated with Binns’s Irdev Discord Account. In the Azurape Discord Account, MOUCKA’s second online girlfriend called him “Connor” several times. He also pointed to his Telegram username, which cannot be easily changed, at least as early as February 2024:

Date	Time	Username	Contents
2/14/2024	22:35:50	azurape#0	do you have telegram
			here add this on tg when ur on '@judische', since am closing this vm
2/14/2024	23:04:58	azurape#0	[REDACTED]
2/14/2024	23:21:44	[REDACTED]	Okay

The Wetworks Discord Account links the Azurape and Nutz Discord Accounts. Specifically, the Wetwork Discord Account's user identifies the Azurape Discord Account as his main account. In response to a court order, Discord researched the Azurape Discord Account and the Wetworks Discord Account and linked them by cookie information, meaning that the same user account on the same computer accessed both accounts. The Wetwork Discord Account and the Nutz Discord Account also have significant IP overlap, including at least eight instances where both accounts were logged into from the same IP address within 10 minutes of each other. Moreover, non-content header information from Discord showed that the Wetwork Discord Account had communicated with the Irdev Discord Account, controlled by Binns, in the months preceding the computer intrusions under investigation.

Discord records also showed numerous connections between the Nutz Discord Account and the Azurape Discord Account, suggesting these accounts were under common control by MOUCKA, including:

- (i) a common IP address was used to access both the Nutz Discord Account and the Azurape Discord Account on April 19, 2024, during the timeframe of the intrusion to Victim-2;
- (ii) the Nutz Discord Account sent over 183 messages to, or that included, the Azurape Discord Account in early January 2024;
- (iii) common IP addresses were used in November 2023 to access the Nutz Discord Account and a file-hosting account that was later used to host Victim-2's stolen data (in or around April 2024); and
- (iv) Mullvad, a privacy-oriented virtual private network (VPN) provider that does not collect or maintain personal identifying information about its users and could be used to hide the identity and location of the person accessing this account, was used to access the Azurape Discord Account, the Nutz Discord Account, and other accounts of interest in the investigation, including the file-hosting account.

The Azurape Discord Account also claimed to control the moniker "ellyel8," which is a moniker that has been linked to @judische by the Telegram chats:

6/19/2024	22:06:17	azurape#0	but the FBI agents that EDR my discord account can't EDR my telegram account
6/19/2024	22:07:27	azurape#0	ellyel8
6/19/2024	22:10:51	azurape#0	i will edit then delete this message in a few hrs when i check this vmware
6/19/2024	22:11:08		i dont really uh
6/19/2024	22:11:11		give a fuck
6/19/2024	22:11:16		or know anything about any of that
6/19/2024	22:11:42	azurape#0	help me decrypt [REDACTED] creditcards and ill give u 2m

The redaction in the above screenshot also shows that Azurape requested help decrypting credit cards obtained from Victim-4, whose name is redacted.

The FBI conducted analysis of IP address information obtained through legal process concerning the Azurape, Wetwork, and Nutz Discord Accounts. While many accounts used Mullvad VPN, the FBI identified various IP address overlaps connecting these accounts to other indicators associated with the computer intrusions. For example, the stolen Victim-2 data was uploaded to a file-sharing service with an account registered using the email address ibizacarbombings[at]protonmail.com. The FBI analyzed IP logs from the ibizacarbombings[at]protonmail.com file-sharing account (the Ibiza File-Sharing Account) and the Nutz Discord Account and discovered that both were accessed from the same IP address within four minutes or less on two occasions, months before the intrusions occurred:

Account	IP Address	Date	Time
Nutz Discord Account	198.44.140.172	12/31/2023	15:32:00
Nutz Discord Account	198.44.140.172	12/31/2023	15:37:00
Ibiza File-Sharing Account	198.44.140.172	12/31/2023	15:41:44
Nutz Discord Account	198.44.140.172	12/31/2023	15:44:00
Nutz Discord Account	198.44.140.172	12/31/2023	15:46:00
Ibiza File-Sharing Account	198.44.140.172	12/31/2023	15:50:07
Nutz Discord Account	198.44.140.172	12/31/2023	16:02:00


According to information obtained from Discord, in June 2024, MOUCKA, using the Azurape Discord Account, sent a message to another user with his monero address, apparently because the recipient had “left over” monero. (Monero is an anonymity-enhanced cryptocurrency.) The monero address MOUCKA supplied is directly traceable to the ransom payment made by Victim-2; specifically, at least some of the bitcoin ransom paid by Victim-2 was converted into monero and sent to the same address MOUCKA provided in the Discord chat.

Linking the Intrusions to MOUCKA and Binns


U.S. authorities obtained screenshots of Telegram chat messages among three key individuals: (1) @judische, who labeled this account with other display names, including “ellyel8” and “catist,” who has been identified as MOUCKA; (2) “Irdev,” identified as co-conspirator John Erin Binns, a dual U.S. and Turkish citizen residing in Turkey; and (3) Individual-1, who has negotiated with victim companies.

The Telegram chats obtained lawfully by the FBI include information that was not known to the public and was likely only known by those involved in the intrusions. For example, Binns and MOUCKA, using Telegram username @judische, labeled here with moniker “ellyel8,” discussed breaching Victim-2’s systems and obtaining tens of billions of customer records in chats dated April 24, 2024, before any public announcement of the intrusion into Victim-2.

24 April 2024

 ellyel8 06:41
I potentially found another 35B for October 2022

Going to check it it includes previous months or if that’s just 06:42
October

 ellyel8 12:08
Can the current buyer afford to keep buying these after the 14B if I
keep exfiltrating? Because I’m 20% done on the 35B. so you should tell
him to just get 1M ready just in case these are monthly so we don’t
have to wait multiple days again, there’s 35B per month.

I’ll need you to send 300k for irdev to send the 14B to keep 12:17
exfiltrating though because this is time consuming and the data is
expensive to store.

Additionally, MOUCKA and Binns posted screenshots and samples of data belonging to Victim-2 and Victim-5 in the Telegram chats on April 29, 2024. Both Victim-2 and Victim-5 confirmed the samples were actual data stolen from their respective systems. MOUCKA discussed having breached other victims’ computer systems, which the FBI subsequently confirmed had been breached; victims had not yet disclosed their breaches at the time of the Telegram messages.

MOUCKA’s Apple Account Provides Evidence of His Identity, Location, and Criminal Activity

U.S. authorities discovered an Apple account with email address nnnnddddwwdffggaa[at]icloud.com, which Apple identified in response to a court order based on shared login IP addresses with MOUCKA’s Nutz Discord Account. Apple produced records in response to legal process showing that the account (i) was accessed from IP address 24.246.30.67

(the Canadian IP Address) over 500 times between April 1, 2023, and August 20, 2024; (ii) had a residential address of [REDACTED] Kitchener, Ontario, N2A 1X4, a phone number (250 2845735), and a machine ID of 2101216876af01722038830fecef63285f517ec6; (iii) reflected numerous purchases using the Canadian IP Address between June 22 and July 8, 2024, including purchases of an iPhone 15 Pro, MacBook Air, and iPad Pro 1, all of which were billed to “Alexander Moucka” and shipped to [REDACTED] in Kitchener, Ontario, Canada (“Target Location”); and (iv) reflected payments on the account by an “Alexander Moucka” using both PayPal and Mastercard, some of which used the Canadian IP Address. While the first name on the account details is “Ddddd” and the last name is “Ddddddd,” Apple provided iTunes Music Store information that indicates “Alexander Moucka” made iTunes purchases using his Apple account in October 2023 from the Canadian IP Address, and stated his address was the Target Location. According to the information from Apple, the Apple ID nnnnddddwwdffggaa[at]icloud.com was created on February 25, 2020.

Additionally, U.S. authorities reviewed information stored in the Apple account’s iCloud storage. iCloud is a file hosting, storage, and sharing service provided by Apple. Numerous photos in the Apple account’s iCloud provide direct and circumstantial evidence of MOUCKA’s involvement in the criminal activity and his location.

For example, the iCloud account contains multiple photos of MOUCKA’s Canadian passport, including this one with full name Connor Riley Moucka, passport number [REDACTED] date of birth 18 August 1999, in Kitchener, Canada:



It appears that a photo of MOUCKA’s passport was sent to someone involved in processing a payment of approximately \$17,000 for a Rolex. Other photos and screenshots appear to depict

transaction records from June and July 2024 for purchases billed to “Alexander Moucka” and shipped to the Target Location. Some of these transactions were made from the Canadian IP Address, which ties MOUCKA to some of the criminal infrastructure as discussed below.

The FBI also reviewed screenshots showing significant amounts of money in cryptocurrency, including of: (1) an unknown bank account or crypto wallet showing a balance of \$3,496,076.97; (2) a wallet with a balance of 4,995,000,000 in unknown currency; (3) an unknown wallet software with a balance of nearly \$20,000 in ETH, a form of virtual currency; and (4) the exchange rate for Turkish Lira. U.S. authorities also seized seed phrases for a monero wallet and a bitcoin wallet, two additional forms of virtual currency.

Screenshots of chat messages, which appear to be from encrypted messaging applications, confirm that others refer to the user of this Apple account as “Connor.” There are screenshots that appear to depict (1) MOUCKA asking for hacking tools, (2) MOUCKA bragging about successful computer intrusions on encrypted messaging applications, and (3) MOUCKA’s cryptocurrency accounts. Other screenshots appear to depict orders for computer hardware, such as laptops and tablets from Apple, which appear to have been purchased with numerous gift cards to conceal the source of MOUCKA’s funds. These were shipped to the Target Location.

One photo in the iCloud account directly implicates MOUCKA in the computer intrusion into Victim-2.

It contains the specific IP address of a virtual private server on which MOUCKA stored a large amount of Victim-2’s sensitive data. Additionally, the screenshot depicts (1) filenames of sensitive data exfiltrated by MOUCKA and confirmed by the FBI to belong to a victim; (2) the fact the data was stored in a subdirectory named “[Victim-1],”; and (3) the name of the intermediary, Individual-1.

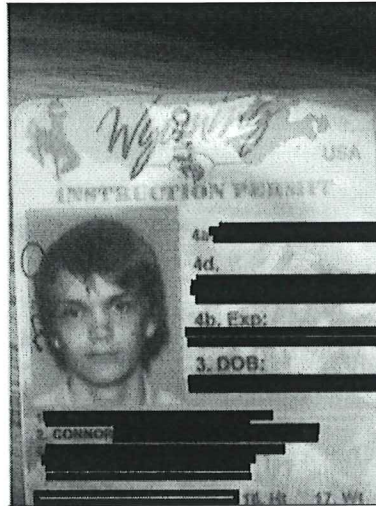
The iCloud account also contains screenshots of Telegram communications where one user asked another user believed to be MOUCKA’s second online girlfriend, “Did you manifest [Victim-4]?” In other screenshots between these two, they discuss how “nobody likes [alternative name for Victim-4],” and “ur goin to jail soon.” The iCloud account also contains a screenshot from the “Rolls Royce Cashout Chat,” a Telegram group in which MOUCKA, using the @judische Telegram account and other users discussed attacks on Victim-5. The iCloud account also contains a screenshot of a chat discussing an unknown crime that referenced vsys.host and alexhost.com, two hosting providers used to store victim data stolen from Victim-1 customers.

Additional Evidence Connecting MOUCKA to the monikers @judische and “Catist,” the Three Discord Accounts, and the Canadian IP Address

Records from the Nutz Discord Account indicate that its user is MOUCKA, who also goes by Alexander Moucka. For example, the Nutz Discord Account’s user:

- (i) states that his birth name is Connor and that he changed it to Alexander;

- (ii) shares a redacted picture of a Wyoming State Instruction Permit showing the name Connor and a photograph that appears to match known photographs of MOUCKA from an FBI records check:



- (iii) provides several redacted images of Ontario photo identification cards in which the photographs appear to be MOUCKA:



- (iv) posts multiple screenshots of the weather in the Kitchener and Toronto area;
- (v) asserts he was raised by his grandparents until he was 11 years old and lived with them again from age 16 through approximately 2022; and
- (vi) discusses that he lived in Wyoming when he was younger.

This information is consistent with information that the FBI obtained from a records check for MOUCKA, which showed that a Connor Riley MOUCKA previously resided in Wyoming and was born on August 18, 1999. As discussed above, the FBI discovered photos of MOUCKA's

Canadian passport in his Apple account; that information is also consistent with the identification documents from Discord and the information from the FBI records check.

The FBI's investigation has uncovered a range of other evidence connecting @judische, "catist," and accounts associated with the intrusion activity to Connor MOUCKA and/or Alexander Moucka.

IP records from Discord showed that the user of the Nutz Discord Account logged into the account from the Canadian IP Address over 3,350 times between October 28, 2023, and April 4, 2024, including: (i) near-daily logins between October 28, 2023 and December 30, 2023, and between January 2, 2024 and February 16, 2024; (ii) more than five logins between 21:41:54 UTC and 23:49:57 UTC on February 2, 2024; and (iii) nearly every day between February 25, 2024, and April 4, 2024, including multiple logins on some days. A WHOIS lookup showed that the Canadian IP Address is provisioned by TekSavvy Solutions Inc., a Canadian service provider, and geolocates to Waterloo, Ontario, Canada. The FBI has no indication that the Canadian IP Address is associated with a VPN.

As set forth above, MOUCKA's Apple account, nnnnddddwwdfffggaa[at]icloud.com, was accessed from the same Canadian IP Address over 500 times between April 1, 2023, and August 20, 2024. Google account connormoucka5[at]gmail.com has also used the Canadian IP Address as recently as August 26, 2024.

MOUCKA Resides at the Target Location

The address of the Target Location was obtained from records obtained from at least four different providers as being the listed address or shipping destination for accounts opened in or tied to MOUCKA's true name, such as cloud service, instant messaging and payment method accounts, as described below.

Specifically, in addition to the iTunes purchases described above, MOUCKA's Apple iCloud account contains (1) a screenshot of an order receipt for an iPad Pro that shipped to "Alexander Moucka" at [REDACTED] Kitchener, ON N2A 1X4; and (2) a Best Buy order receipt from July 2, 2024 for a SteelSeries wireless gaming headset, to be shipped to "Alexander Moucka" at [REDACTED] Kitchener, ON N2A1X4.

The Nutz Discord Account also confirms that MOUCKA resides at the Target Location. MOUCKA used this account to post multiple screenshots related to the weather in the Kitchener and Toronto area, and repeatedly accessed this account using the Canadian IP Address. The Canadian IP Address geolocates to Waterloo, Ontario, Canada. The Target Location is in the Kitchener-Waterloo area.

In addition, the Azurape Discord Account, controlled by MOUCKA, posted a picture in a January 2024 conversation, indicating it was a photo of the user's backyard after a recent snowfall. The FBI reviewed the image and identified multiple structures that are consistent with structures in or near the Target Location which were identified using (1) publicly available overhead satellite

imagery surrounding the backyard of the Target Location, and (2) publicly available street-level images near the Target Location.

Google Pay provided information about connormoucka5[at]gmail.com in response to legal process, which also included the full address of the Target Location and the full name “Connor Moučka” as of April 2023.

PayPal provided account information in response to legal process for an account with email address connormoucka5[at]gmail.com in the name of “Connor R Moucka.” The Target Location is listed as both his billing address and shipping address. The PayPal information also indicates that MOUCKA’s date of birth is August 18, 1999. The PayPal account was created on November 29, 2017.

Urgency

The evidence gathered by this investigation establishes that MOUCKA poses both a danger to the public and a serious risk of flight that require his immediate apprehension. Additionally, media outlets have contacted U.S. authorities about this matter and one outlet indicated it intends to name MOUCKA in an article to be submitted for publication on October 25, 2024. U.S. authorities believe that this publication would increase risk of flight and lead MOUCKA to destroy evidence and publish stolen information, including the extremely sensitive call and text history records stolen from Victim-2.

Risk of Flight

MOUCKA has the means to flee. MOUCKA has earned at least approximately \$2.5 million in ransom payments for stolen data from Victim-1 customers already interviewed by the FBI. The FBI anticipates identifying additional victims who paid ransoms that have not yet been reported to law enforcement.

Based on lawfully obtained screenshots from MOUCKA’s iCloud account, MOUCKA controls a significant amount of cryptocurrency stored in wallets that have not yet been found by law enforcement. These proceeds could be used to facilitate his flight and would support him afterwards.

Evidence also indicates MOUCKA is aware of the gravity of this case and the exposure he will face upon extradition to the United States. He has repeatedly discussed his operational security measures and attempts to delete evidence in order to evade identification and apprehension. MOUCKA has repeatedly purchased new laptops and deleted and created new accounts over the course of his offenses. For example, in April 2024, he discussed on Discord “nuking” (i.e., deleting) his accounts to avoid law enforcement capture of his communications:

According to records from Discord, the zzxxvwww Discord account was registered using

4/4/2024	23:16:21	zzxxvwww	so basically the fbiâ€™s trying to get that [redacted] girls phone and theyâ€™re going to do celebrite on it. so I just wanted to delete my account and any way she can contact me before that happens.
----------	----------	----------	---

MOUCKA’s nnnnddddwwdffggaa[at]icloud.com account (discussed above) and used prior usernames “catist” and “meowist,” among others. It was also repeatedly accessed from the Canadian IP Address.

In another post, MOUCKA discusses closing a virtual machine (“vm”):

Date	Time	Username	Contents
2/14/2024	22:35:50	azurape#0	do you have telegram
			here add this on tg when ur on '@judische', since am closing this vm
2/14/2024	23:04:58	azurape#0	[redacted]
2/14/2024	23:21:44	[redacted]	Okay

These are only two of several examples in which MOUCKA discusses his belief that his accounts are being actively monitored and the steps he is taking (including account and message deletion) to avoid detection and apprehension.

These considerations present a strong motivation for him to attempt to destroy evidence of his crimes, alert his co-conspirators, flee the jurisdiction, and potentially to cause harm to himself or others, as outlined below.

The investigation has also revealed that MOUCKA has considered obtaining foreign citizenship. For example, in February 2024, he sent a message stating, “I can get dual citizenship to Czech Republic pretty sure. I want an eu passport.” The U.S. authorities have no information about whether he has actually sought to do so.

Risk of Harm to the Community

Evidence gathered over the last several months also establishes that MOUCKA continues to be actively engaged in hacking activities and poses an ongoing danger to the public, to police, and to himself.

MOUCKA’s campaign has involved the theft of terabytes of sensitive data from tens, if not hundreds, of victims. Additionally, MOUCKA has repeatedly extorted and re-extorted his victims, resulting in enormous and ongoing harm not only to the corporations impacted but also the millions of individuals whose data was stored by these corporations.

MOUCKA and his conspirators continue to sell, publish, and otherwise leak this data online, and every day that he is allowed to remain free, his harms will continue. As recently as October 2024, MOUCKA attempted to re-extort at least one victim, repeatedly threatening to

release more of this company’s data even after the company paid a ransom. MOUCKA has also continued to publish private data stolen from victims online, and to aggressively market this data for sale.

In addition, MOUCKA has recently posted multiple Telegram “polls” asking other users whether he should post stolen data from other victims. Stolen data was posted publicly at least as recently as on or about September 30, 2024.

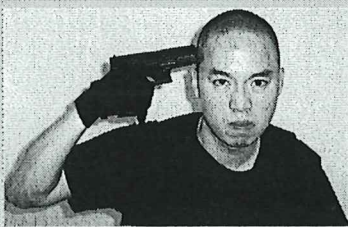
MOUCKA has also discussed harming himself and others.

On January 10, 2024, MOUCKA, using his Nutz Discord Account (username “zzzzzzzzzzzzzzzzzznutz”) stated that sanctioned suicide “Seems epic.” He also talks about “mass mailing sodium nitrate pills” to Black people in Michigan and Ohio. Less than 10 minutes later, he says “I think I’d make a really good serial killer.”

MOUCKA repeatedly references committing mass killings and obtaining firearms:

Timestamp	Time (UTC)	Username	Contents
1/10/2024	2:26:21	zzzzzzzzzzzzzzzzzznutz	Idk what to do bc I want to go outside to kill niggers, but I donâ€™t want to go outside because thereâ€™s niggers outside. is a nigger paradox

1/10/2024	23:41:18	zzzzzzzzzzzzzzzzzznutz	I can buy a glock from tg with a switch
1/10/2024	23:41:39	zzzzzzzzzzzzzzzzzznutz	full auto switch if u donâ€™t know what that means
1/10/2024	23:41:48	zzzzzzzzzzzzzzzzzznutz	But it turns a glock 17 into a glock 18

1/11/2024	1:22:33	zzzzzzzzzzzzzzzzzznutz	He seems epic	
1/11/2024	1:24:06	zzzzzzzzzzzzzzzzzznutz	I think Iâ€™d be a good mass shooter	
1/11/2024	1:24:59	zzzzzzzzzzzzzzzzzznutz	tbh Iâ€™d buy a box van and an m134 and just mount it inside hidden and remote controlled	
1/11/2024	1:25:04	zzzzzzzzzzzzzzzzzznutz	Then just mow down a crowd	
1/11/2024	1:25:26	zzzzzzzzzzzzzzzzzznutz	I could be hidden the entire time	

MOUCKA also discussed committing suicide and suicide by cop on both January 11, 2024, and January 18, 2024; on the latter occasion, MOUCKA stated, “I think I want to do suicide by cop.” In another message, MOUCKA stated, “I need guns to kill Canadians.”

A much more fulsome recitation of MOUCKA’s statements that suggest he poses a public safety threat has been provided to RCMP through law enforcement channels.

UNITED STATES DISTRICT COURT

for the

Western District of Washington

United States of America

v.

Case No.

CR 24-180-1 LK

CONNOR RILEY MOUCKA

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) CONNOR RILEY MOUCKA

who is accused of an offense or violation based on the following document filed with the court:

- Indictment, Superseding Indictment, Information, Superseding Information, Complaint, Probation Violation Petition, Supervised Release Violation Petition, Violation Notice, Order of the Court

This offense is briefly described as follows:

- Count 1 18 U.S.C. § 371 (Conspiracy)
Counts 2 through 6 18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2 (Computer Fraud and Abuse)
Counts 7 and 8 18 U.S.C. §§ 1030(a)(7)(B), 1030(c)(3)(A), and 2 (Extortion in Relation to Computer Fraud)
Counts 9 through 18 18 U.S.C. §§ 1343 and 2 (Wire Fraud)
Counts 19 and 20 18 U.S.C. §§ 1028A(a)(1) and 2 (Aggravated Identity Theft)

Date: 10/10/2024

Signature of Issuing Officer: tfarrell, Deputy Clerk

City and state: Seattle, Washington

tfarrell, Deputy Clerk
Printed name and title

Return

This warrant was received on (date) and the person was arrested on (date) at (city and state)

Date:

Arresting officer's signature

Printed name and title

DEFENDANT ARREST WARRANT INFO SHEET

(One for each defendant)

DEFENDANT'S NAME: Connor Riley Moucka

ALIAS: Alexander Antonin Moucka, judische, catist, waifu, ellye18, zfa

LAST KNOWN RESIDENCE: Kitchener, Canada

LAST KNOWN EMPLOYMENT:

PLACE OF BIRTH: Kitchener, Canada

DATE OF BIRTH: August 18, 1999

SOCIAL SECURITY NUMBER:

HEIGHT:

WEIGHT:

SEX: M

RACE: Caucasian

HAIR: Brown

EYES: Brown

SCARS, TATTOOS, AND/OR OTHER DISTINGUISHING MARKS:

FBI NUMBER:

COMPLETE DESCRIPTION OF AUTO:

INVESTIGATIVE AGENT AND AGENCY: FBI Special Agent Hannah Trepte

AGENT CONTACT INFO: 206-287-3628; htrep@fbi.gov

DRUG CASES:

OCDETF CASE YES NO

This is Exhibit "C" referred to in the affidavit of [REDACTED] sworn before me this 28th day of October, 2024.

Axsmith, Lynne

A Commissioner for taking Affidavits

2024.10.21 14:37



2024.10.21 14:37

