

UNITED STATES DISTRICT COURT

for the

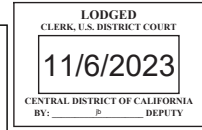
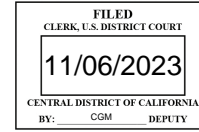
Central District of California

United States of America

v.

SERGEY VLADIMIROVICH OCHIGAVA,

Defendant.



Case No. 2:23-mj-05719-duty

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about November 4, 2023, in the county of Los Angeles in the Central District of California, the defendant violated:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 2199	Stowaway on Aircraft

This criminal complaint is based on these facts:

*Please see attached affidavit.*

Continued on the attached sheet.

*/s/ Caroline Walling*  
Complainant's signature

Caroline Walling, SA FBI  
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: November 6, 2023

*Joel Richlin*  
Judge's signature

City and state: Los Angeles, California

Hon. Joel Richlin  
Printed name and title

**AFFIDAVIT**

I, Caroline A. Walling, being duly sworn, declare and state as follows:

**I. PURPOSE OF AFFIDAVIT**

1. This affidavit is made in support of a criminal complaint and arrest warrant against SERGEY VLADIMIROVICH OCHIGAVA ("OCHIGAVA") for a violation of Title 18, United States Code, Section 2199 (Stowaway on Aircraft).

2. This affidavit is also made in support of an application for a warrant to search a black iPhone SE with a silver back, IMEI number 356609082196518, including any and all subscriber identity modules (aka "SIM" cards) found within the case of said phone (collectively, the "SUBJECT DEVICE"), as described more fully in Attachment A, for evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Section 2199 (Stowaway on Aircraft) (the "SUBJECT OFFENSE"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant and does not purport to set forth all of my knowledge of the investigation into this matter. Unless specifically indicated otherwise, all conversations and

statements described in this affidavit are related in substance and in part only.

**II. BACKGROUND OF AFFIANT**

4. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so for approximately nine years. Since 2018, I have been assigned to the Los Angeles International Airport ("LAX") Office of the FBI, where I investigate violations of federal law which occur within the airport environment and onboard aircraft.

5. My training and experience includes interviewing victims, suspects, and witnesses along with preparation and execution of search warrants and criminal complaints.

**III. SUMMARY OF PROBABLE CAUSE**

6. On November 4, 2023, at approximately 1 p.m., OCHIGAVA arrived at Los Angeles International Airport (LAX) on board Scandinavian Airlines, also known as "SAS" or "SK," flight 931 from Copenhagen Airport (CPH), in Denmark. When OCHIGAVA presented himself for entry at the Customs and Border Protection (CBP) checkpoint at LAX, CBP officers discovered that OCHIGAVA was not a listed passenger on the flight manifest for SK 931, or any other incoming international flight. OCHIGAVA was unable to produce a passport or a visa to enter the United States. When questioned, QCHIGAVA gave false and misleading information about his travel to the United States, including initially telling CBP that he left his ~~U.S.~~ passport on the airplane.

**IV. STATEMENT OF PROBABLE CAUSE**

7. Based on my review of law enforcement reports, surveillance video recordings, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

**A. OCHIGAVA flew on SK931 from CPH to LAX on November 4, 2023**

8. According to the SK flight crew who worked on SK 931 on November 4, 2023, most of them noticed OCHIGAVA on the flight. The crew noticed OCHIGAVA because he wandered around the plane and kept changing his seat. In addition, he asked for two meals during each meal service, and at one point attempted to eat the chocolate that belonged to members of the cabin crew. The crew members did not see his boarding pass but did note that the seat he initially took during boarding (i.e., seat 36D) was supposed to be an unoccupied seat. Some members of the crew conducted head counts for their specific sections, but only to make sure that the aircraft was balanced for takeoff and landing. They did not tally the numbers up. One member of the cabin crew stated that it looked like OCHIGAVA was trying to talk to other passengers on the flight, but most of the passengers ignored him.

9. I reviewed the video footage from the LAX security cameras located LAX Tom Bradley International Terminal Gate 156 on November 4, 2023. SK 931 parked and deplaned at Gate 156 around 1:00 p.m. on November 4, 2023. Around 1:08 p.m., I

observed a male who appeared to be OCHIGAVA deplaning SK 931 on surveillance footage.

10. According to CBP records, OCHIGAVA was not listed as a passenger on the manifest for SK 931 on November 4, 2023.

**B. OCHIGAVA Landed at LAX and Presented Himself to Immigration Authorities**

11. According to CBP reports and my conversations with CBP officers at LAX, on November 4, 2023, a man later identified as OCHIGAVA presented himself to CBP passport control primary officers and the following transpired:

a. Speaking English, OCHIGAVA informed a CBP officer that he had left his passport on the plane. OCHIGAVA informed the officer that he had arrived on SK 931. The CBP officer directed OCHIGAVA to customer service (also known as "GEM" representatives) so that they could page SK and assist OCHIGAVA.

b. OCHIGAVA approached a GEM representative and told her that he had left his documents on the plane. He informed the GEM representative that he arrived on SK from Copenhagen. When asked what documents he had left on the plane, OCHIGAVA told the GEM representative that he left his United States passport on the plane. OCHIGAVA relayed to the GEM representative that he sat in seat 48G. A GEM representative attempted to contact a representative from SK.

c. A GEM representative approached another CBP officer for assistance. The GEM representative explained that OCHIGAVA left his passport on the plane. The CBP officer offered to assist the processing of OCHIGAVA while they waited

for an airline representative. The CBP officer began to process OCHIGAVA. The CBP officer attempted to process OCHIGAVA but could not find any information for OCHIGAVA. The CBP officer then asked OCHIGAVA for his name, date of birth, and flight information. The CBP officer had OCHIGAVA write down the information. The CBP officer then attempted again to locate OCHIGAVA in the CBP system, but the CBP officer could not find any information for OCHIGAVA.

d. The CBP officer notified his supervisor that he could not find OCHIGAVA in the CBP systems. A CBP supervisor responded. The CBP officers searched OCHIGAVA's bag and found foreign identification cards for OCHIGAVA, which appeared to be Russian identification cards and an Israeli identification card. CBP officers discovered a partial photograph of a passport on the SUBJECT DEVICE. The partial photograph of the passport showed OCHIGAVA's name, date of birth, and passport number, but did not show the passport holder's photograph. CBP officers ran the name and date of birth, as well as just the passport number in their system, and again could not find documentation showing that OCHIGAVA had a flight into the United States on November 4, 2023. The CBP officers and the CBP supervisor could not find any record of OCHIGAVA in their system. According to the CBP supervisor, OCHIGAVA should be in their system if he had a booking for a flight or was on a flight into the United States.

e. According to the CBP officer, the CBP system contained information of all passengers who were on flights into the United States, as well as additional identity information

which allowed CBP to authenticate the identities of the incoming passengers. The CBP officer had never encountered a situation where a passenger in the CBP inspection area was not in the CBP system.

f. According to a CBP chief, a Russian citizen must have a visa and a valid passport to enter the United States. The Russian identity document found in OCHIGAVA's possession was a Russian identification card for travel within Russia but was not an international passport required for admission into the United States. An Israeli citizen must have a valid passport and an Electronic System for Travel Authorization ("ESTA") to enter the United States. The Israeli identification card found in OCHIGAVA's possession was not a passport, and no ESTA application could be found in the CBP system for OCHIGAVA. If OCHIGAVA had applied for an ESTA, it would have shown up in CBP's system.

g. A CBP officer searched the United States Department of State's visa database for a visa application for OCHIGAVA, and they could not find any documentation in that showed that OCHIGAVA had applied for or received a visa.

h. The CBP supervisor checked with the CBP control booth. The CBP control booth was responsible for keeping track of all the passengers arriving into the United States from every international flight, and where the passengers were in the processing system within CBP (i.e., showing that the passengers have either been allowed into the United States, or sent for further admissibility review). CBP officers in the control

booth queried all of the passengers from SK 931, along with all the passengers who had arrived at LAX on every European flight before 3:00 p.m. on November 4, 2023. The control booth confirmed that all of those passengers were accounted for. OCHIGAVA had not yet processed through CBP at the time that CBP showed that 100% of the passengers who arrived from Europe before 3:00 p.m. had been accounted for. According to CBP records, there were no additional passengers from SK 931 to process, and no additional passengers to process who arrived from Europe before 3:00 p.m. Based on these findings, the CBP supervisor believed she was dealing with a stowaway and OCHIGAVA was detained by the CBP Admissibility Review Unit (ARU) for further review of his admissibility to the United States.

**C. Information from Scandinavian Airlines**

12. SK never found a passport on board SK 931 on November 4, 2023.

13. After the SK station manager was informed that there was a passenger in CBP who claimed to have been on SK 931 on November 4, 2023, the station manager confirmed with CBP that everyone who was on the manifest for SK 931 was accounted for. The station manager realized that they were "plus one" on the passenger load for SK 931.

**D. OCHIGAVA's Statements to the FBI**

14. On November 5, 2023, FBI Task Force Officer (TFO) Alison Meier and I interviewed OCHIGAVA at an interview room in ARU. Russian translation service was provided by a Russian speaking CBP officer.



15. Before beginning the interview, OCHIGAVA was read his Miranda rights in Russian and English. OCHIGAVA stated, among other things, the following:

a. OCHIGAVA had a PhD in economics and marketing. He last worked as an economist in Russia a long time ago. OCHIGAVA claimed he had not been sleeping for three days and did not understand what was going on. OCHIGAVA stated he might have had a plane ticket to come to the United States, but he was not sure. OCHIGAVA did not remember how he got on the plane in Copenhagen. OCHIVAGA also would not explain how or when he got to Copenhagen or what he was doing there. When asked how he got through security in Copenhagen, OCHIGAVA claimed he did not remember how he went through security without a ticket.

b. During the interview, OCHIGAVA permitted the interviewers to go through the camera roll on the SUBJECT DEVICE. The most recent photograph in the camera roll was of television screens displaying flight information for flights flying all over the world (including flights to Amsterdam, Munich, Lisbon, Malaga, London, etc.). The bottom of the screen read: OBS: Ingen højtalerudkald. According to Google translate, the word "Højtalerudkald" is the Danish word for loudspeaker call. Open source research revealed that CPH is the biggest airport in Denmark, and that Danish is the official language of Denmark. The interviewers were allowed to look at a five more photographs on the SUBJECT DEVICE before OCHIGAVA turned off the phone. The other photographs consisted of

screengrabs from the "Maps" app showing a hostel in Kiel, Germany, and street maps from an unknown foreign city.

**V. TRAINING AND EXPERIENCE ON THE SUBJECT OFFENSE**

16. Based on my knowledge, training, and experience, as well as information related to me by other agents, I know that federal aviation regulations require a passenger to present valid country entry documents to match a valid boarding pass in order to fly to the United States. A valid boarding pass can either be in paper or digital form, or both.

**VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES**

17. As used herein, the term "digital device" includes the SUBJECT DEVICE.

18. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

19. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

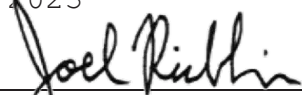
b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

20. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

## **VII. CONCLUSION**

21. For all of the reasons described above, there is probable cause to believe that OCHIGAVA violated Title 18, United States Code, Section 2199 (Stowaway on Aircraft) and that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE described in Attachment A.

Attested to by the applicant in  
accordance with the requirements  
of Fed. R. Crim. P. 4.1 by  
telephone on this 6 day of  
November, 2023

Handwritten signature of Joel Richlin in blue ink, written over a horizontal line.

HONORABLE A. JOEL RICHLIN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

PROPERTY TO BE SEARCHED

A black iPhone SE with a silver back, IMEI number 356609082196518, including any and all subscriber identity modules (aka "SIM" cards) found within the case of said phone (collectively, the "SUBJECT DEVICE"), which is currently CBP's possession.

**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Section 2199 (Stowaway on Aircraft) (the "Subject Offense"), namely:

- a. All international travel-related documents, including boarding passes and airline tickets;
- b. All documents and records related to immigration, including visas, passports, applications for visas, and other forms;
- c. All records pertaining to the purchase of airline tickets or other forms of transportation;
- d. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;
- e. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;
- f. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook,

Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

g. Contents of any calendar or date book;

h. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

i. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

j. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;



iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal

digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## **II. SEARCH PROCEDURE FOR DIGITAL DEVICES**

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

**ATTACHMENT**

FINDING RE PROBABLE CAUSE

On November 6, 2023, at 12:50 ~~a~~/p.m., Special Agent Caroline Walling of the Federal Bureau of Investigation appeared before me regarding the probable cause arrest of defendant SERGEY VLADIMIROVICH OCHIGAVA, occurring on November 4, 2023, at Los Angeles, California.

Having reviewed the agent's statement of probable cause, a copy of which is attached hereto, the Court finds that there **exists/~~does not exist~~** probable cause to arrest the defendant for a violation of Title 18, United States Code, Section 2199.

/ X / It is ordered that defendant SERGEY VLADIMIROVICH OCHIGAVA be held to answer for proceedings under Federal Rule of Criminal Procedure 5 ~~7-40~~ on November 6, 2023, at 12:50pm.

/     / It is ordered that defendant SERGEY VLADIMIROVICH OCHIGAVA be discharged from custody on this charge forthwith.

DATED: November 6, 2023 , at 12:50 ~~a.m.~~/p.m.



\_\_\_\_\_  
HON. A. JOEL RICHLIN  
UNITED STATES MAGISTRATE JUDGE