AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Eric Devon Lazenby

Case No. 5:26-mj-1026-PRL

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of January 15 and January 16, 2026 in the county of Lake in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. Sec. 875(c)	Interstate Communications of Threats

This criminal complaint is based on these facts:

See attached affidavit.

☑ Continued on the attached sheet.

Todd Myers
Complainant's signature

SA Todd Myers, FBI
Printed name and title

Sworn to before me over the telephone or other reliable electronic means and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: January 30, 2026

P. Lammens
Judge's signature

City and state: Ocala, Florida

Philip R. Lammens, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
OCALA DIVISION

IN THE MATTER OF THE ISSUANCE OF A CRIMINAL COMPLAINT AGAINST ERIC LAZENBY AND THE SEARCHES OF A SAMSUNG GALAXY CELLULAR PHONE AND THE PREMISES LOCATED AT 21810 SUNSET DRIVE, ASTOR, FLORIDA 32102	Case Nos.: 5:26-mj-1026-PRL 5:26-mj-1027-PRL 5:26-mj-1028-PRL **FILED UNDER SEAL**

MASTER AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND SEARCH WARRANTS

I, Todd Myers, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of a criminal complaint for **Eric Devon Lazenby** and applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search property (a cellular telephone more fully described in Attachment A-1), and the extraction from that property of electronically stored information described in Attachment B, and the premises located at 21810 Sunset Drive, Astor, Florida 32102, hereinafter "**PREMISES**," further described in Attachment A2.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since March 2017. I am currently assigned to the Jacksonville Field Office, Daytona Beach Resident Agency, and I have been assigned to this position since

August 2017. For nine years before I joined the FBI, I served as a police officer in the State of Ohio, and prior to that I served in the United States Army.

3. I have completed FBI training at the FBI Academy in Quantico, Virginia. During my employment with the FBI, I have received specialized training and have gained experience in the investigation of violent crime, violent criminal enterprises, gangs, international terrorism, domestic terrorism, weapons of mass destruction and violent crimes against children. I have received specialized training and am a Firearms Instructor for the FBI and a member of the Jacksonville Division SWAT team.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

FACTS SUPPORTING PROBABLE CAUSE

Background

5. On January 14, 2026, a Homeland Security Investigations (HSI) federal agent with Immigration and Customs Enforcement (ICE), Enforcement Removal Operations (ERO) was involved in a shooting that occurred in the area of the 600-block of 24th Avenue North, in Hennepin County, Minneapolis, Minnesota, while conducting an immigration enforcement action. Agents from the FBI Minneapolis Violent Crime Squad and personnel from the FBI Evidence Response Team (ERT) responded to the scene to investigate the incident and to gather evidence.

6. After collecting evidence from the scene and during the course of their investigation, a large group of individuals began to gather. Due to the number of individuals and the increasing tension, law enforcement personnel in the area were

unable to maintain a perimeter, and FBI agents and ERT personnel were forced to evacuate the area on foot for their personal safety with the help of other law enforcement officers and agents who responded to the scene. FBI agents were forced to leave two government-owned vehicles parked near the scene.

7. Several individuals attacked, vandalized, damaged, and broke into the two government-owned vehicles left at the scene. FBI-issued equipment and materials, including a rifle, rifle suppressor, a handgun, tactical vests, FBI IDs and building access badges, as well as FBI and other personal documents were stolen from the vehicles. Some of the documents stolen contained rosters with employees' phone numbers, email addresses, and home addresses, as well as driver's licenses.

8. After the employees' personal information and documentation was compromised, several of the documents, including residential addresses, phone numbers, and emails, were posted publicly online on social media. Shortly thereafter, approximately 10 to 15 FBI Agents and employees began receiving multiple harassing and threatening phone calls, text messages and emails. Other suspicious occurrences included "drive-bys" of the employees' residences where vehicles would slow down as they passed before driving away.

Review of Victim A's Cellphone Messages

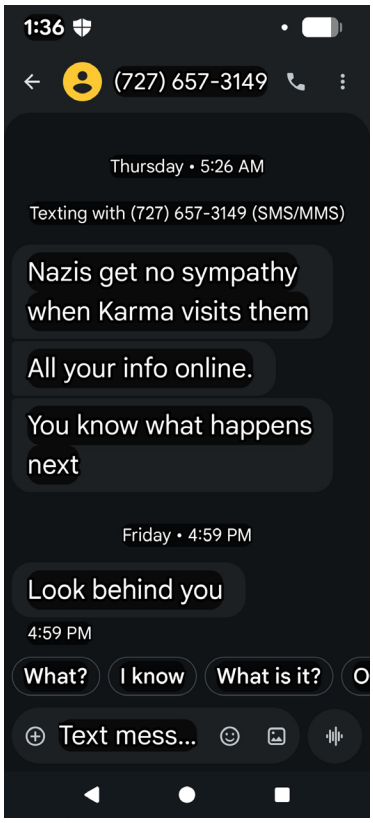
9. Victim A is an FBI SA with the Minneapolis Field Office who has received multiple threatening phone calls and text messages after the January 14, 2026 incident described above, and whose information was contained on some of the documents stolen from the two government-owned vehicles that were damaged.

10. On Thursday, January 15, 2026, at 6:25 a.m. Eastern Standard Time (EST)[1], Victim A received a voicemail from **727-657-3149** (**Subject Phone**) that stated, "Hey [Victim A's first name], I just wanted to thank you for your vehicle, and all your belongings. You guys really got your asses beat tonight. Now your face and your family, everything has been leaked on the internet. So [Victim A's first name], you have a great rest of your week, while we ya know, do what we do best, and um, you suck a big dick. You took fifty grand to be a class traitor and now all your info is online, Have a great night."

11. On the same date at 6:26 a.m. EST, Victim A received a threatening text message from the **Subject Phone**. The message read, "Nazis get no sympathy when Karma visits them All your info online. You know what happens next."

12. On Friday, January 16, 2026, at 5:59 p.m. EST. Victim A received another text message from the **Subject Phone** that stated, "Look behind you." A photograph of the messages is below:

[1] Victim A and Victim B (described below) were located in the Central Time Zone (Minnesota) when the call and messages were received from the **Subject Phone**, which is why the texts message times in the photographs below are one hour behind the EST times in this affidavit.



Interviews with Victim A

13. During an interview by investigating agents, Victim A confirmed having received the above text messages. Victim A stated the text messages were "definitely threatening." Victim A has changed their behavior as a result of the threatening communications. For example, Victim A parked their official bureau vehicle at a friend's house in his garage. When Victim A has to go to work, they will drive a privately owned vehicle (POV) to a friend's house and take their official bureau vehicle to work from there. Victim A conducts surveillance detection routes to and from work. Initially after January 14, 2026, Victim A sent their family to different locations so they would not be found. Victim A has ordered multiple surveillance cameras for their house after this event.

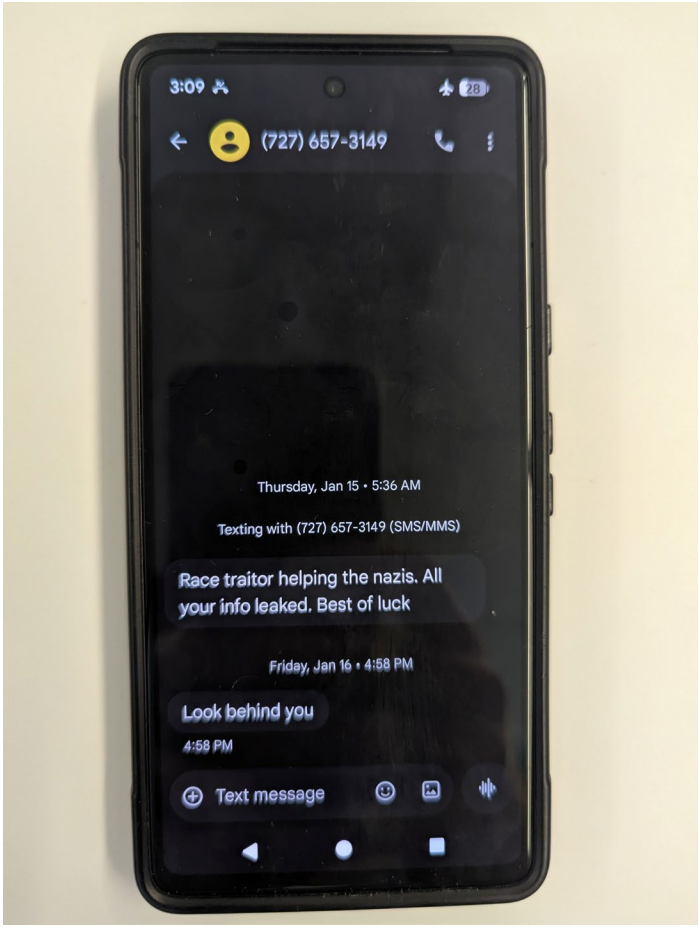
14. Victim A stays armed at all times while they are at home and has staged firearms around the house out of fear of potential intruders who have learned about their residential address. Victim A stands outside armed while Victim A's pet goes outside to use the bathroom. Victim A is worried about their family while at work, and Victim A's family is worried about this situation. Victim A is worried about their own life and safety and the life and safety of Victim A's family as a result of the threatening communications Victim A has received, including those described above.

Review of Victim B's Phone

15. Victim B is an FBI SA with the Minneapolis Field Office who received multiple phone calls and text messages after the January 14, 2026 incident described above, and whose information was contained in some of the documents stolen from the two government-owned vehicles that were damaged.

16. On January 15, 2026, at 6:36 a.m. EST, Victim B received a text message from the **Subject Phone** that stated, "Race traitor helping nazis. All your info leaked. Best of luck."

17. On January 16, 2026, at 5:58 p.m. EST, Victim B received a text message that stated, "Look behind you." A photograph of the messages is below:



Interview With Victim B

18. On January 21, 2026, FBI investigating agents interviewed Victim B. Victim B received a phone call on January 14, 2026, from an unknown person. Upon answering the phone, the unknown person asked, "is this [Victim B's first name]?" The unknown caller then stated, "you are on live stream, and all of your information is leaked." Victim B began receiving consistent text messages, voicemails, and phone calls from January 14, 2026 onward, after this particular call, including the texts from the **Subject Phone**, described above. Victim B perceived these specific threats from the **Subject Phone** to be extremely serious. Victim B stated that the threats sounded

"crazy" at first, until an unknown individual showed up to Victim B's residence while his family was present at home.

Identification of **Lazenby** as the User of the **Subject Phone**

19. On January 26, 2026, FBI Agents submitted an emergency disclosure request (EDR) to T-Mobile for location/subscriber data for the **Subject Phone**. The information received from the EDR identified **Eric Lazenby** as the subscribed user of the phone, a Samsung Galaxy S10E. The following information was obtained through the request:

a. Mobile Station International Subscriber Directory Number (MSISDN) Name: **Eric Lazenby**

b. Billing address: 3601 ROCKLEDGE, COLUMBUS, OH 43223-3429

c. Contact phone: (727) 657-3149

d. IMSI: 310260352698993

e. IMEI: 354764100148249

f. Begin Service Date: 08/04/2017

20. Open-source databases also indicated the registered owner of the **Subject Phone** was **Lazenby**.

21. A review of **Lazenby's** criminal history shows that he has a felony conviction for kidnapping and false imprisonment.

CAST Analysis

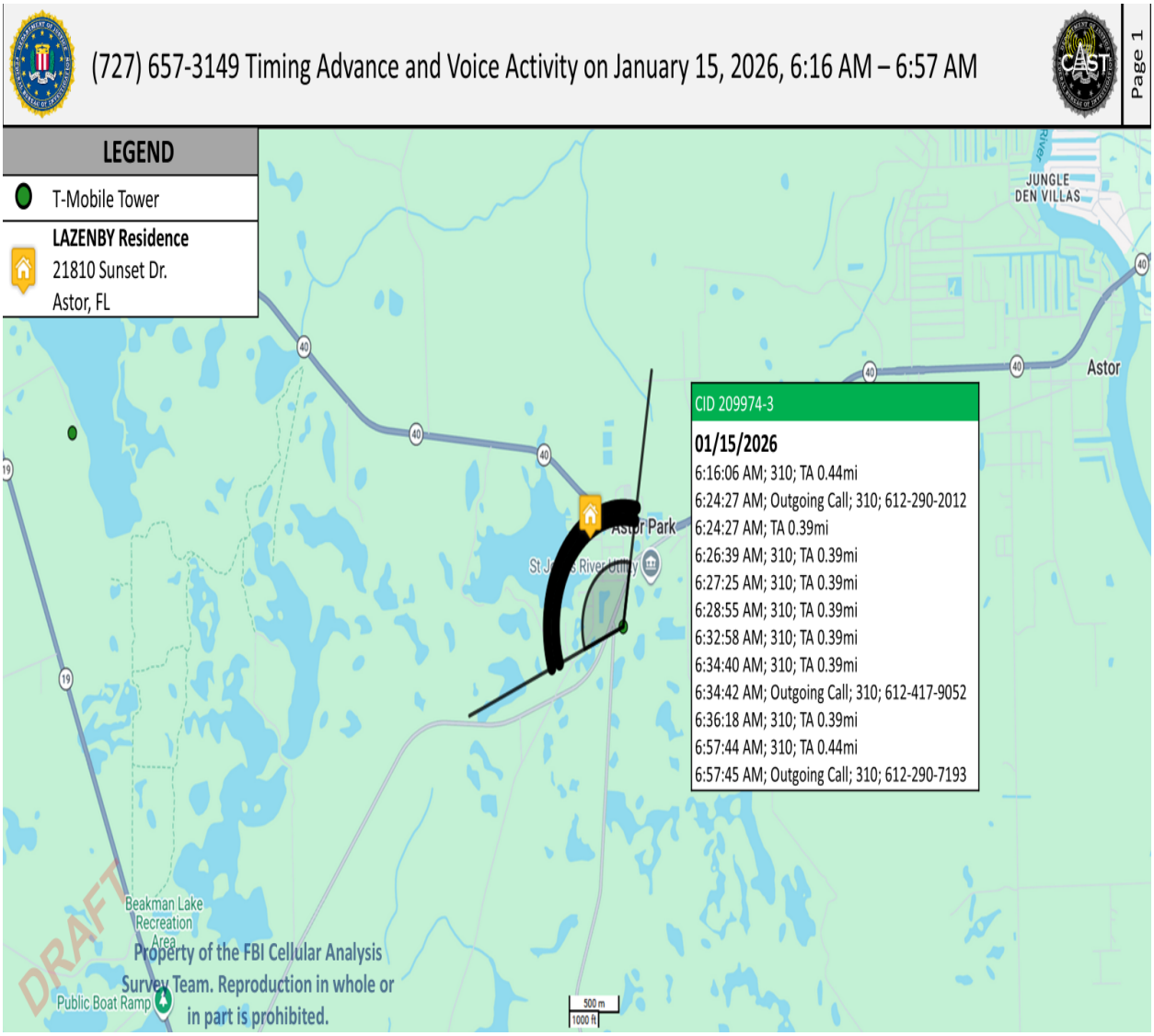
22. FBI SAs and Cellular Analysis Survey Team (CAST) team members Nicole Lopez and Robert W. Blythe reviewed historical cell-site location information for the **Subject Phone** from January 15, 2026 through January 16, 2026.[2] The device remained in the vicinity of Astor Park (Lake County) and Barberville, Florida (Volusia County) (both within the Middle District of Florida) during the entirety of the time frame.

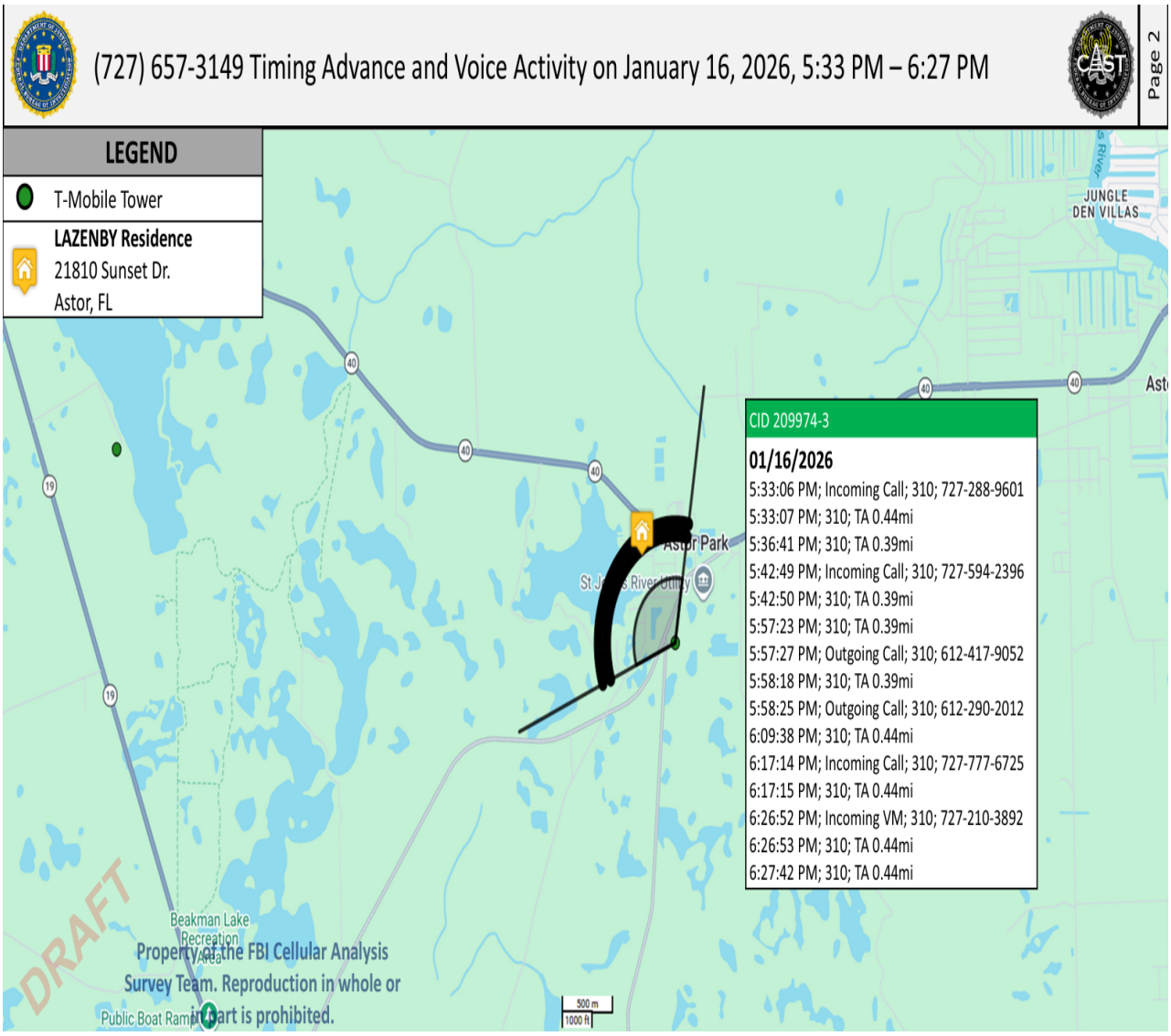
23. On January 15, 2016, between 6:16 a.m. EST and 6:57 a.m. EST (the time period during which the initial call and texts to Victim A and Victim B occurred), the **Subject Phone** used the closest T-Mobile tower to the **PREMISES** (which is located in Lake County) and the sector facing the **PREMISES** for voice and timing advance signaling. The timing advance signaling indicate the **Subject Phone** was calculated to be approximately the same distance from the tower as the **PREMISES** is from the tower.

24. On January 16, 2026, the **Subject Phone** used the closest tower to the **PREMISES** and the sector facing the **PREMISES** between 5:33 p.m. EST and 6:27 p.m. EST (the time period during which the latter texts were sent to Victim A and Victim B). The timing advance signaling indicate the **Subject Phone** was approximately the same distance from the tower as the **PREMISES** is from the tower. Thus, the cell-site location information shows that the **Subject Phone** was located

[2] This information was received from a state search warrant executed in Minnesota.

within the Middle District of Florida (and likely at the **PREMISES**) during the times it sent the phone call and messages to Victim A and Victim B. Below are two maps of this information:





DAVID Results

25. On January 29, 2026, I reviewed the Florida Driver and Vehicle Information Database (DAVID) associated with **Lazenby**. DAVID results revealed the **PREMISES** as **Lazenby's** current mailing address. Florida license plate LEHL05 is reported to be registered to **Lazenby**. As of January 26, 2026, LEHL05 was registered to a 2003 Toyota, four-door, silver vehicle, which is solely registered to **Lazenby**.

Surveillance

26. On January 29, 2026, physical surveillance was conducted by FBI Personnel at the **PREMISES**, and the following was observed:[3]

a. At approximately 11:21 a.m. EST, a silver Toyota sedan bearing Florida license plate LEHL05 was parked in the driveway of the **PREMISES**.

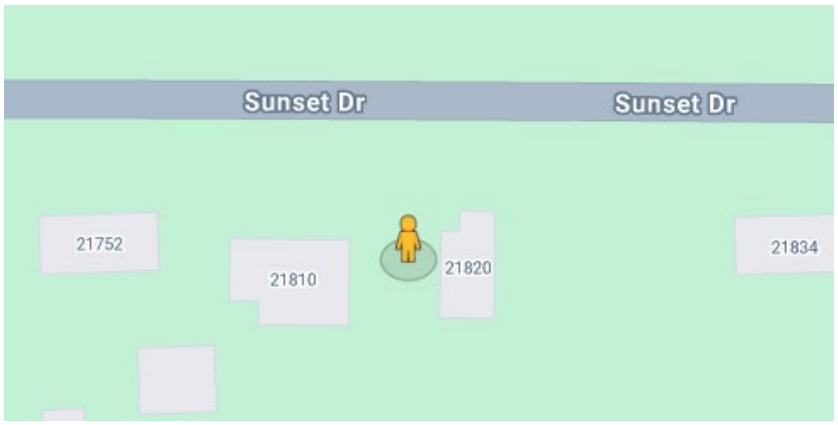
b. At approximately 12:33 p.m. EST, the silver Toyota sedan was parked under an awning at the **PREMISES**.

[3] The location of the residence makes it difficult for law enforcement to surveil without the risk of detection by **Lazenby**.

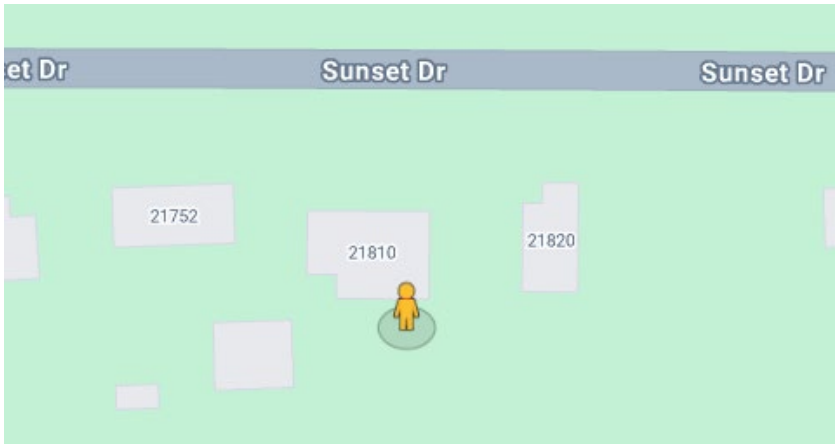
Current Location Information

27. The FBI is currently receiving location information ("pings") for the **Subject Phone** as a result of a state search warrant issued in Minnesota. Below is a list of the most recent locations associated with the **Subject Phone**. All three of the below pings identify the **Subject Phone** being at or very near the **PREMISES**:

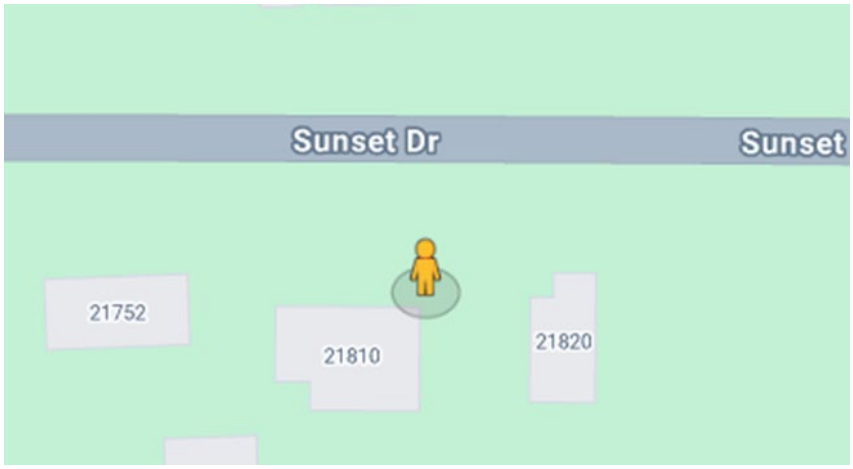
a. Local Date/Time: 1/30/2026 at 7:54:32 a.m. EST



b. Local Date/Time: 1/30/2026 at 8:04:33 a.m. EST



c. Local Date/Time: 1/30/2026 8:24:26 a.m. EST



28. Based on the above, I believe there is probable cause that **Lazenby** 1) sent threatening communications to Victim A and Victim B, 2) used the **Subject Phone** to do so, and 3) is living at the **PREMISES** where law enforcement expects to execute the anticipated arrest warrant. Likewise, I know that because the communications were sent using a cellular telephone, and because the victims were located in Minnesota while the **Subject Phone** was located in Florida at the times of the communications, these communications were transmitted in interstate commerce. Because law enforcement expects to arrest **Lazenby** at or near the **PREMISES**, I am seeking a search warrant for the **PREMISES** for the limited purpose of seizing the **Subject Phone** if and only if **Lazenby** does not have the **Subject Phone** on his person at the time of his arrest. Law enforcement would then enter the **PREMISES** to attempt to locate the **Subject Phone**.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital

cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's

latitude, longitude, and sometimes altitude with a high level of precision.

d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. Based on my training and experience, I know that the **Subject Phone** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Subject Phone** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Subject Phone** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise

copying the **Subject Phone**, and would authorize a later review of the **Subject Phone** or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire **Subject Phone**, that might expose many parts of the data to human inspection in order to determine whether it is evidence described by the warrant.

34. *Manner of execution.* Because this warrant seeks permission to examine a device that will be taken into law enforcement's possession, and because the analysis of the device may take place during all hours of the day within a secure law enforcement facility, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

AUTHORIZATION TO USE BIOMETRIC FEATURES TO UNLOCK DEVICE

35. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

36. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that

can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require.

37. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, if the device is equipped with an operating system that is earlier than version 9.3, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. If the operating system is version 9.3 or later, that time frame shrinks to 8 hours.

38. Similarly, Touch ID will not allow access if the device has been turned on or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary to use the fingerprints and thumbprints of any device's users to attempt to gain access to the device while executing the search warrant. The government may not be able to obtain the contents of the **Subject Phone** if those fingerprints are not used to access the device

by depressing them against the Touch ID button. Although I do not know which of the ten finger or fingers are authorized to access on any given device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID, and in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

39. In addition, I know from my training and experience that many other mobile device manufactures have their own version of Touch ID—that is, a fingerprint recognition feature that the device's user can program and use to unlock the device. For instance, I know that Google Pixel phones and Google Pixel XL phones have a fingerprint sensor that can be used to unlock the device. Similarly, Samsung, LG, HTC, and other manufacturers also have devices with fingerprint sensors.

40. Similarly, in my training and experience I know that some applications loaded onto mobile devices or other electronic devices may be secured by the user with a thumbprint or fingerprint. Common among these types of applications are applications such as mobile banking apps or other financial applications, password storage applications, and secure communications apps, among others.

41. Further, if a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the

user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

42. Similarly, if a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

43. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

44. As discussed in this Affidavit, I have reason to believe that the **Subject Phone** will be found on **Lazenby**. The passcode or password that would unlock the

Subject Phone currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the **Subject Phone**, making the use of biometric features necessary to the execution of the search authorized by this warrant.

45. Due to the foregoing, I request this that this warrant authorize the **Subject Phone** to be unlocked using one of the aforementioned biometric features. Law enforcement personnel would obtain from **Lazenby** the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the **Subject Phone**, including to (1) press or swipe the fingers (including thumbs) of **Lazenby** to the fingerprint scanner of the Subject Phone; (2) hold the **Subject Phone** in front of the face of **Lazenby** to activate the facial recognition feature; and/or (3) hold the **Subject Phone** in front of the face of **Lazenby** to activate the iris recognition feature, for the purpose of unlocking the **Subject Phone** in order to search the contents as authorized by this warrant.

CONCLUSION

46. Based on the above, I respectfully request the issuance of 1) a complaint against **Eric Lazenby**, 2) a search warrant for the **Subject Phone**, and 3) a search warrant for the **PREMISES**.

Respectfully submitted,

Todd Myers
Special Agent, FBI

Affidavit submitted to me by reliable electronic means and attested to me as true and accurate by telephone or other reliable electronic means consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) before me this 30th day of January 2026.

PHILIP R. LAMMENS
United States Magistrate Judge