AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

FILED
Oct 08 2026
Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

United States of America
v.
Abdulrahman ALFOZAN

Case No. 3:26-mj-71329 MAG

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 September 28, 2026 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2511(1)(b)	Use of an electronic, mechanical, or other device to intercept oral communications

This criminal complaint is based on these facts:

See attached affidavit of FBI SA Lydia Liang

☑ Continued on the attached sheet.

/s/ Lydia Liang
Complainant's signature

Approved as to form by
AUSA Nicholas Parker

FBI SA Lydia Liang
Printed name and title

Sworn to before me by telephone.

Date: 10/08/2026

Judge's signature

City and state: San Francisco, CA

Hon. Alex G. Tse, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Lydia Liang, a Special Agent of the Federal Bureau of Investigation (FBI), having been duly sworn, hereby declare as follows:

INTRODUCTION AND PURPOSE OF AFFIDAVIT

1. I make this Affidavit in support of an application under Rules 3, 4, and 4.1 of the Federal Rules of Criminal Procedure for a criminal complaint (and accompanying arrest warrant) charging Abdulrahman ALFOZAN with one count of intentionally endeavoring to use an electronic, mechanical, or other device to intercept oral communications, in violation of 18 U.S.C. § 2511(1)(b), beginning on a date unknown but no later than on or about September 28, 2026, and lasting through a date unknown but no earlier than October 5, 2026, in the Northern District of California.

SOURCES OF INFORMATION

2. Because this Affidavit is submitted for the limited purpose of securing a criminal complaint and arrest warrant, I have not included every fact known to me concerning this investigation. Instead, I have set forth only the facts necessary to establish probable cause that the violation of federal law identified above has occurred.

3. I have based my statements in this Affidavit on my training, experience, and research, personal knowledge of the facts and circumstances obtained through my participation in this investigation, information provided by other agents and law enforcement officers, and information provided by records and databases. I believe these sources to be reliable. Where I refer to conversations and events, I refer to them in substance and in relevant part rather than in their entirety or verbatim, unless otherwise noted. This Affidavit also reflects my current understanding of facts relating to this investigation, but my understanding may change in the future as the investigation proceeds.

AFFIANT BACKGROUND

4. I am a Special Agent of the FBI and have been so employed since February 2023. I am currently assigned to the San Francisco Division. Before becoming a Special Agent with the

FBI, I worked at various technology companies as a data analyst and data product manager for more than 10 years. My FBI training included attending a four-month academy at Quantico, Virgina, which included trainings in investigation, interrogation, human intelligence (HUMINT), law, defensive tactics, and firearms. I received advanced HUMINT training in 2024 with a focus in espionage. As an FBI Special Agent, I have investigated a wide array of federal criminal offenses, including matters related to acting as an agent of a foreign government, espionage, counterintelligence, and national security. I have gained additional experience through my training at the FBI and everyday work relating to conducting these types of investigations

5. I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7). That is, I am empowered by statute to conduct investigations of—and to execute warrants and make arrests for—violations of federal law, including violations of the wiretap statute, 18 U.S.C. § 2511, *et seq.*

APPLICABLE LAW

6. Title 18, United States Code, Section 2511(1)(b), makes it unlawful to "intentionally use[], endeavor[] to use, or procure[] any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use

(A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States."

FACTS ESTABLISHING PROBABLE CAUSE

A. Background

7. Since in or around July 2025, ALFOZAN—a foreign national who was educated in, and who since September 2020 has been a legal permanent resident of, the United States—has worked as an engineer at Company 1.

8. Company 1 is a super intelligence (SI), a/k/a artificial intelligence (AI), company headquartered in the Northern District of California. Among other things, Company 1 develops large-scale generative models and provides for a chatbot and virtual assistant that allows users to prompt the platform for a variety of information and responses. Company 1 employs thousands of people.

9. There is an executive conference room ("Conference Room 1") inside one of Company 1's buildings in San Francisco ("Company Building 1") that, according to Company 1 representatives, (i) can be reserved only by executives and executive assistants; and (ii) typically is used for internal leadership meetings and technical and product sessions, as well as external briefings with government officials and business counterparts.

10. According to Company 1 representatives, ALFOZAN had no authority to access, or to participate in meetings occurring in, Conference Room 1. Meetings in Conference Room 1 frequently involve discussions of highly confidential technical, commercial, and strategic information, including proprietary research, product plans, and business-development opportunities, as well as nonpublic information about Company 1's technical progress and strategic decisions, capabilities, priorities, government engagements, and commercial relationships.

B. Discovery of Recording Device 1

11. On or about September 30, 2026, Company 1 personnel discovered a surreptitious audio recording device inserted into a USB port on the back of a television in Conference Room 1 ("Recording Device 1").

12. The device was a Seeed XIAO ESP32-S3 Sense[1]—a thumb-sized development board with a detachable camera sensor, digital microphone, and microSD storage—and had been concealed in toilet paper, as reflected in Figure 1, below (red circle added for identification). Company 1 personnel removed the device from the television and unwrapped it. Figure 2, below, shows the unwrapped device.

Figure 1

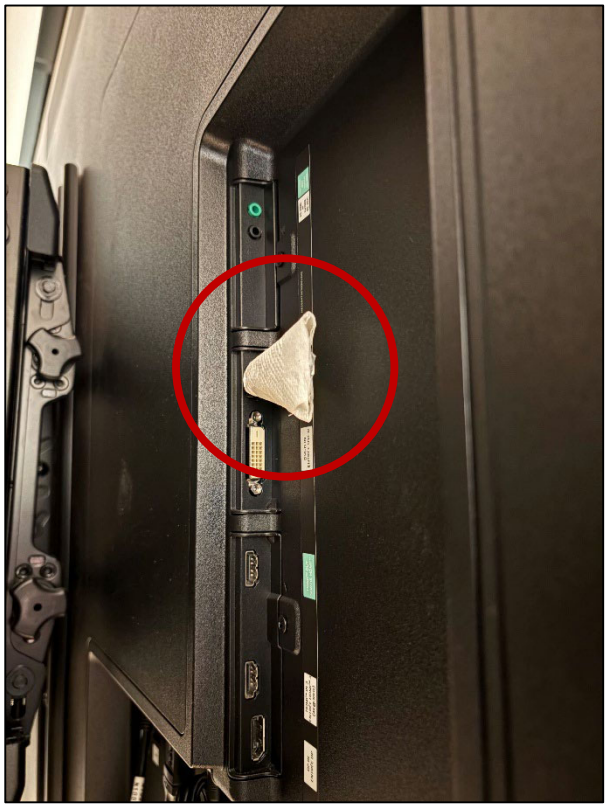


Figure 2 (Recording Device 1)

[1] According to its website, Seeed is a company based in Shenzhen, People's Republic of China, with manufacturing based in Asia and offices throughout the world.

13. A subsequent investigation by Company 1 personnel determined that (i) the USB adapter on Recording Device 1 may have been modified to prevent data transfer between Recording Device 1 and the television; and (ii) the contents of the microSD card may have been encrypted. Specifically, when Company 1 personnel made a forensic image of the microSD card, none of the files on it could be recovered or decrypted, but the limited information that could be recovered included a MAC address[2] and a custom header ("NANOVOL1") for the microSD card that—based on my training, experience, and research—is a layout consistent with a potentially encrypted file system. Company 1 also determined that the firmware for Recording Device 1 appeared to have been compiled on September 28, 2026, suggesting it was installed on or about that date.

C. Attribution of Recording Device 1 to ALFOZAN

14. Company 1 did not have a camera within Conference Room 1 at the time Recording Device 1 was installed on or about September 28, 2026. However, closed-circuit television (CCTV) footage inside Company 1's offices reveals that ALFOZAN was near Conference Room 1 on the following dates at the following times:

Date	Time
September 8, 2026	4:35 pm – 7:01 pm
September 9, 2026	12:11 pm – 12:12 pm
September 14, 2026	12:08 pm – 12:09 pm
September 15, 2026	12:30 pm – 12:31 pm
September 16, 2026	12:36 pm – 6:51 pm
September 21, 2026	11:31 am – 6:12 pm
September 22, 2026	12:14 pm – 7:22 pm
September 23, 2026	12:35 pm – 7:27 pm

[2] Based on my training, experience, and research, a MAC address is a unique physical hardware identifier assigned to a device's network adapter, typically by the manufacturer.

September 28, 2026	2:18 pm – 6:30 pm
September 29, 2026	3:35 pm – 3:37 pm

15. Furthermore, between on or about August 17, 2026, and on or about September 16, 2026, ALFOZAN used a productivity agent to inquire about Company 1's building addresses, meeting rooms, meeting-room capacities and calendars, and external-partner meeting venues. Specifically, ALFOZAN submitted the following queries, among others:

Date	ALFOZAN Query
August 17, 2026	what meeting was this presented at and when was it recorded
August 18, 2026	how to send USPS to [Company Building 1]? \ it's not [Company Building 1] front desk
September 16, 2026	list meeting rooms in [Company Building 1] that are 6+
September 16, 2026	can you list today's meeting in this room
September 16, 2026	where did you find room's calener? [*sic*]
September 16, 2026	so is [a different Company 1 building] the mailing building now? how about leadership and exec?
September 16, 2026	how about external partners, where would those usually meet with [Company 1] at?

16. Based on my training and experience, these queries suggest ALFOZAN was researching Company 1's conference rooms, meeting calendars, and potential attendees to identify where he should place Recording Device 1.

17. Between on or about September 27, 2026, and September 28, 2026, an AI chatbot account associated with ALFOZAN's spouse—an account that shared installation identifiers, logged IP usage, and user path name references with ALFOZAN's own AI chatbot account—

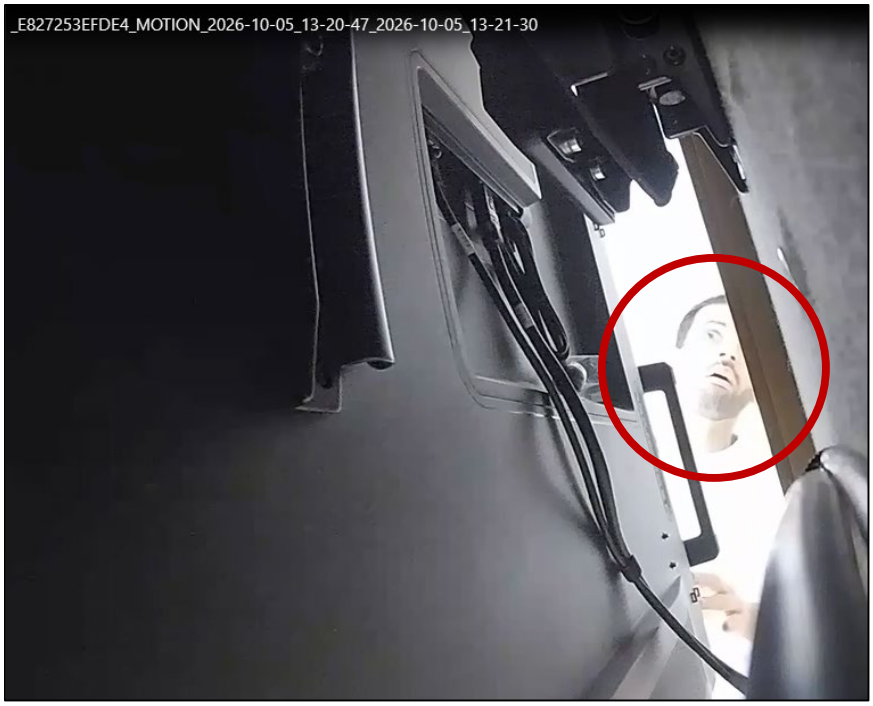
submitted user prompts containing the aforementioned custom "NANOVOL1" header and the unique MAC address of Recording Device 1. The account associated with ALFOZAN's spouse also submitted additional relevant prompts between on or about September 24, 2026, and September 30, 2026, including the following:

- To build a continuous audio recorder (e.g., capturing microphone audio and save compressed WAV recordings to an SD card, generally in one-hour files);
- To add browser access and controls (e.g., adding timestamped filenames, downloading/deleting recordings, stop/resume, reboot, live listening, and adjustable microphone gain);
- To customize Wi-Fi identity and connectivity (e.g., assigning hostnames and custom MAC addresses, use passive scanning and repeated connection attempts, then introduce iPhone hotspot profiles);
- To improve audio and live listening;
- To test recording reliability;
- To encrypt the SD card (e.g., implementing NanoVol encryption, testing interrupted power, and decrypting and recovering recordings from the removed card);
- To protect firmware and restrict USB output (e.g., USB power-only change, enabling Secure Boot and firmware encryption, disabling serial logging, and configuring the first unit for USB power-only during normal operation);
- To develop a second unit and speech-triggered recording;
- To develop a third unit and refine everyday use; and
- To apply final protection and silence boot output.

18. My training and experience, the specificity and configuration of Recording Device 1, and these written prompts attributable to ALFOZAN and/or his spouse, indicate that ALFOZAN inserted Recording Device 1 into the television in Conference Room 1 and was interested in building, customizing, installing, audio recording, testing, obfuscating, and remote accessing, among other things, a surreptitious audio listening and recording device.

19. On or about October 5, 2026, by which point a camera had been placed in Conference Room 1, ALFOZAN was observed entering Company Building 1. CCTV footage from that date shows ALFOZAN entering Conference Room 1 at about 1:20 pm and checking behind the television into which Recording Device 1 had been inserted. Figure 3 below is a screenshot from the CCTV footage showing ALFOZAN checking behind the television in Conference Room 1 on or about October 5, 2026 (red circle added for identification).

Figure 3

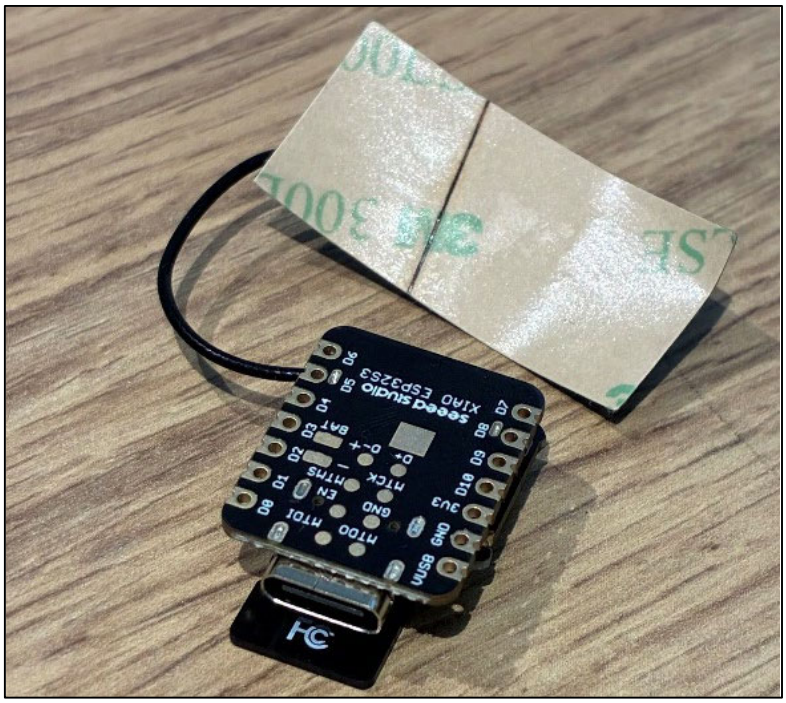


D. Discovery of Recording Device 2 and Attribution to ALFOZAN

20. Also on or about October 5, 2026, according to Company 1 representatives, ALFOZAN left a bag unattended in a printer room in Company Building 1. Company 1 security personnel opened the bag and discovered—among other things, including ALFOZAN's wallet, ID, and other personal items—another recording device ("Recording Device 2"). Like Recording Device 1, Recording Device 2, which is depicted in Figure 4 below, is manufactured by Seeed. And as it had for Recording Device 1, Company 1 assessed that Recording Device 2 (i) had a recording microcontroller; and (ii) had been customized to obfuscate anything stored on the

device, such as potentially intercepted audio communications. ALFOZAN reported to Company 1 that he had lost his bag.

Figure 4 (Recording Device 2)



21. On or about October 6, 2026, at about 12:00 pm, ALFOZAN retrieved his bag—which no longer contained Recording Device 2, among other items—from Company 1's centralized Lost and Found. After retrieving his bag, ALFOZAN asked Company 1 personnel about certain items he said were missing from his bag but did not inquire about Recording Device 2 (or Recording Device 1). ALFOZAN submitted a written update shortly thereafter: "Update: picked up bag from [a Company 1 building], but a few items were stolen: one credit card, cash (~$500), 2 airpods, 1 headphone, sunglasses, powerbank." CCTV footage showed that, after retrieving his bag from Company 1's Lost and Found, ALFOZAN put it down and transferred items into it from a Target shopping bag.

CONCLUSION

22. Based on the facts and circumstances set forth above, and on my training and experience, I submit there is probable cause to believe that, beginning on a date unknown but no

later than on or about September 28, 2026, and lasting through a date unknown but no earlier than October 5, 2026, in the Northern District of California, the defendant, Abdulrahman ALFOZAN, used or endeavored to use an electronic, mechanical, or other device to intercept any oral communication, in violation of 18 U.S.C. § 2511(1)(b). Accordingly, I respectfully request that the Court issue (i) a criminal complaint charging the defendant with that offense; and (ii) a warrant for the defendant's arrest.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

/s/ *Lydia Liang*
LYDIA LIANG
Special Agent
Federal Bureau of Investigation

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) on this 8th day of October 2026.

HON. ALEX G. TSE
United States Magistrate Judge