AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Andrea Guadalupe Velez, and
Luis Dalhet Hipolito

Defendants.

Case No. 2:25-MJ-03896-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 the date of June 24, 2025 in the county of Los Angeles in the Central District of California, the defendants violated:

Code Section	*Offense Description*
18 U.S.C. § 111(a)(1)	Assault on a Federal Officer

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Joseph Arko, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone. Date: 06/25/2025 at 3:36 p.m.

Judge's signature

City and state: Los Angeles, California

Hon. Michael Kaufman, U.S. Magistrate Judge
Printed name and title

AUSA Shawn Andrews x6104

AFFIDAVIT

I, Joseph Arko, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of criminal complaints against and arrest warrants for Andrea Guadalupe Velez ("VELEZ"), and Luis Dalhet Hipolito ("HIPOLITO"), charging them with violating Title 18, United States Code, Section 111(a)(1) (Assault on a Federal Officer).

2. This affidavit is also made in support of an application for a warrant to search the following digital devices ("SUBJECT DEVICES"), in the custody of the Bureau of Alcohol, Tobacco, Firearms, and Explosives("ATF"), in Los Angeles, California, as described more fully in Attachment A:

a. a white Apple iPhone ("SUBJECT DEVICE 1"), seized from VELEZ following her arrest by federal law enforcement on June 24, 2025;

b. a white Apple iPhone ("SUBJECT DEVICE 2"), seized from HIPOLITO following his arrest by federal law enforcement on June 24, 2025; and

c. a Samsung cellular telephone bearing IMEI number 357861960520959 ("SUBJECT DEVICE 3," and collectively the "SUBJECT DEVICES") seized from HIPOLITO following his arrest by federal law enforcement on June 24, 2025.

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Section 111(a)(1) (Assault on a

Federal Officer) and Title 18, United States Code, Section 372 (Conspiracy to Impede a Federal Officer), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. 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 that there is sufficient probable cause for the requested complaint and warrant and does not purport to set forth all my knowledge of or 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 AGENT

5. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), and have been for over 20 years. Prior to my employment with ATF, I was an Officer with the United States Secret Service for three years.

6. I am currently assigned to the Homeland Security Investigations ("HSI") Integrated Operations Group Task Force (the "Task Force"). As part of this Task Force, I investigate various immigration crimes with Department of Homeland Security agents and analysts, including from HSI and Immigration and Customs Enforcement ("ICE") and Enforcement and Removal Operations.

III. STATEMENT OF PROBABLE CAUSE

7. Based on witness interviews, my review of body worn camera footage, and my knowledge of this investigation, I know the following:

8. At approximately 9:20 a.m. on June 24, 2025, ICE Deportation Officers C.G. ("C.G.") and C.C. ("C.C.") were two of a contingent of federal law enforcement officers driving in a convoy of vehicles down East 9th Street in downtown Los Angeles. As the vehicles passed Main Street, they pulled over to the side of the road so the federal officers could question two individuals about whether they were lawfully present in the United States.

9. C.G. and C.C. exited the cars they were riding in and approached the two individuals. As they approached, however, one of the individuals, a male subject, ran away from the DOs and the DOs gave chase. According to an interview I conducted with C.G. and C.C., they said (in substance and summary):

a. As C.G. ran after the male subject, he saw a woman (later identified as VELEZ) step into his path and extend one of her arms in an apparent effort to prevent him from apprehending the male subject he was chasing;

b. Since VELEZ stepped into C.G.'s path so abruptly, he could not stop his momentum and VELEZ's outstretched arm struck C.G. in the face;

c. C.G. believed that VELEZ was using a cellular phone in her other hand and recording the event as it transpired;

d. When VELEZ made contact with C.G., she knocked him off balance and prevented him from continuing his chase;

e. C.C. was running behind C.G. and C.C. saw VELEZ step into C.G.'s path of travel and extend her arms, striking C.G. in his head and chest.

10. As a result of VELEZ's actions, C.G. and C.C. ended their pursuit and placed VELEZ under arrest. Then, they placed VELEZ into one of the government vehicles on scene in order to transport her for further processing.

11. Then, the government vehicles tried to drive away from the scene, but three individuals (one of whom was later identified as HIPOLITO) stood in front of the lead vehicle and prevented it from driving away. According to the interview I conducted with C.C., he said:

a. He was in the lead government vehicle when he saw HIPOLITO and two compatriots approach the vehicle and stand in front of it in an apparent effort to prevent it from leaving the scene;[1]

b. He exited the vehicle and tried to verbally command HIPOLITO and his two compatriots to leave the scene, but HIPOLITO and his two compatriots refused to move from in front of the government vehicle;

c. Since HIPOLOTO and his two compatriots refused to move, C.C. sprayed all three individuals with O.C. spray.

[1] I have reviewed social media videos that captured this portion of the incident, and based on that review, it appears that HIPOLITO was using one of his cellular phones to record video at this point in the event.

d. After he sprayed the three individuals with pepper spray, HIPOLITO's two compatriots backed away, but HIPOLITO punched C.C. in the face.

12. Eventually, HIPOLITO was arrested and transported for further processing. During that processing, agents seized SUBJECT DEVICE 2 and SUBJECT DEVICE 3 from his person. When VELEZ was being processed following her arrest, agents seized SUBJECT DEVICE 1 and no other digital devices from her person.

IV. TRAINING AND EXPERIENCE ON GROUPS WHO OBSTRUCT LAW ENFORCEMENT

13. Based on my training and experience, as well as my familiarity with investigations conducted by other law enforcement agents into groups who organize in an effort to obstruct federal law enforcement in the execution of their duties, I know the following:

14. Such groups are often organized along ideological lines; for instance, these groups may organize around a shared ideology opposed to the enforcement of federal immigration laws. As such, the members of these groups often communicate with one another to share information about their common ideology. Such sharing is usually conducted via text message, Internet messaging application, and/or social media via digital devices.

15. Such groups typically consist of a large number of participants who are poised to coalesce into action on short notice. For example, should a group that is organized around a shared ideology opposed to the enforcement of federal immigration law learn of what the group believes to be an

immigration law enforcement operation, those members will communicate with each other via digital devices to mobilize group members to hinder law enforcement action.

16. In some instances, such groups have contacts who are privy to non-public law enforcement documents. By having access to such documents, the groups are able to anticipate law enforcement action and mobilize more quickly to hinder such action. Members of these groups often share such non-public information via digital devices.

17. Members of these groups often keep the names, addresses, and telephone numbers of those involved in their activities on their digital devices. Additionally, they often keep records of meetings with associates on their digital devices, including in the form of calendar entries and location data.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

18. As used herein, the term "digital device" includes the SUBJECT DEVICES.

19. 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:

20. 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.

21. 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.

22. 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.

23. 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.

24. 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:

25. 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.

26. 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.

27. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

28. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally

displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

29. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time.

30. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress VELEZ's and/or HIPOLITO's thumb and/or fingers on the device; and (2) hold the device in front of VELEZ's and/or HIPOLITO's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

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

VI. CONCLUSION

32. For all the reasons described above, there is probable cause to believe that VELEZ and HIPOLITO have committed a violation of Title 18, United States Code, Section 111(a)(1) (Assault on a Federal Officer). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES as 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 25 day of June 2025 at 3:36 p.m.

HONORABLE MICHAEL KAUFMAN
UNITED STATES MAGISTRATE JUDGE