

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Cole Ashcraft, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

I am a Special Agent with the Treasury Inspector General for Tax Administration (“TIGTA”) and am assigned to the Federal Bureau of Investigation (“FBI”) Washington Field Office Cyber Task Force as a Task Force Officer. In my duties as both a TIGTA Special Agent and an FBI Task Force Officer, I investigate unlawful activity in connection with computers. As both a TIGTA Special Agent and FBI Task Force Officer, I am authorized by law or by a government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of federal criminal laws.

This affidavit is being submitted in support of a criminal complaint alleging that, over the course of February through April 2021, MIGUEL ZAPATA made false statements to the Federal Bureau of Investigation via its tip line in violation of 18 U.S.C. § 1001(a)(2) and (3), which makes it a crime to, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully make any materially false, fictitious, or fraudulent statement or representation, and knowingly and willfully make or use any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry.

This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents, court-authorized searches, and my training and experience, as well as the training and experience of other law enforcement agents. Where the content of records and the actions, statements, and conversations of others are reported, they are reported in substance and in part, except where otherwise indicated.

Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have only set forth the facts that I believe are necessary to establish probable cause that ZAPATA violated 18 U.S.C. § 1001(a)(2), (3).

Details of Probable Cause***The Attack at the U.S. Capitol on January 6, 2021***

On January 6, 2021, a Joint Session of the United States House of Representatives and the United States Senate (“the Joint Session”) convened in the United States Capitol building (“the Capitol”) to certify the vote of the Electoral College of the 2020 U.S. Presidential Election (“the Electoral College vote”), as required by both the Twelfth Amendment of the United States Constitution and Title 3, United States Code, Section 15.

The Capitol is secured 24 hours a day by United States Capitol Police. The Capitol Police maintain permanent and temporary barriers to restrict access to the Capitol exterior, and only authorized individuals with appropriate identification are allowed inside the Capitol building.

On January 6, 2021, at approximately 1:00 p.m., the Joint Session convened in the Capitol building to certify the Electoral College vote. Vice President Michael R. Pence, in his constitutional duty as President of the Senate, presided over the Joint Session.

A large crowd began to gather outside the Capitol perimeter as the Joint Session got underway. Crowd members eventually forced their way through, up, and over Capitol Police barricades and advanced to the building's exterior façade. Capitol Police officers attempted to maintain order and stop the crowd from entering the Capitol building, to which the doors and windows were locked or otherwise secured. Nonetheless, shortly after 2:00 p.m., crowd members forced entry into the Capitol building by breaking windows, ramming open doors, and assaulting Capitol Police officers. Other crowd members encouraged and otherwise assisted the forced entry. The crowd was not lawfully authorized to enter or remain inside the Capitol, and no crowd member submitted to security screenings or weapons checks by Capitol Police or other security officials.

Shortly thereafter, at approximately 2:20 p.m., members of the House and Senate (including Vice President Pence)—who had withdrawn to separate chambers to resolve an objection—were evacuated from their respective chambers. The Joint Session and the entire official proceeding of the Congress was halted while Capitol Police and other law-enforcement officers worked to restore order and clear the Capitol of the unlawful occupants.

Later that night, law enforcement regained control of the Capitol. At approximately 8:00 p.m., the Joint Session reconvened, presided over by Vice President Pence, who had remained hidden within the Capitol building throughout these events.

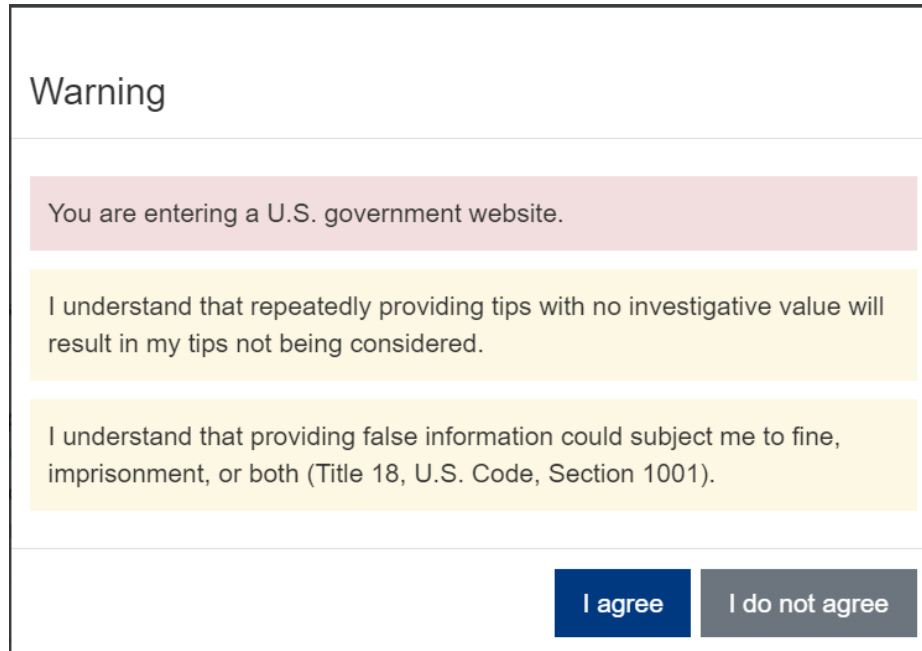
In the course of these events, numerous members of the Capitol Police and the Metropolitan Police Department were assaulted. Additionally, many media members were assaulted and had cameras and other news-gathering equipment destroyed, and the Capitol suffered millions of dollars in damage—including broken windows and doors, graffiti, and residue of various pepper sprays, tear gas, and fire extinguishers deployed both by crowd members who stormed the Capitol and by Capitol Police officers trying to restore order.

The FBI Tip Website

As a result of these events, the FBI began investigating the riot, the actors, and related offenses and made a public appeal for tips related to the unlawful activity at the U.S. Capitol on January 6, 2021. The FBI encouraged members of the public to submit tips via an online portal at tips.fbi.gov.¹

¹ See <https://www.fbi.gov/contact-us/field-offices/washingtondc/news/press-releases/fbi-seeking-information-related-to-violent-activity-at-the-us-capitol-building-010621>.

When members of the public visit tips.fbi.gov to submit a tip, they are shown a warning banner that states, in relevant part, “I understand that providing false information could subject me to fine, imprisonment, or both (Title 18, U.S. Code, Section 1001).” To progress to the tips page, the user must then click “I Agree” to access the tip submission form. This warning banner appears every time an individual attempts to submit a tip, and is displayed in the below screenshot from the publicly available tips.fbi.gov page:



Warning

You are entering a U.S. government website.

I understand that repeatedly providing tips with no investigative value will result in my tips not being considered.

I understand that providing false information could subject me to fine, imprisonment, or both (Title 18, U.S. Code, Section 1001).

I agree I do not agree

Zapata’s Use of a Web Anonymizer to Submit False Tips

On February 10, February 16, February 17, and April 11, 2021, the FBI received at least seven anonymous tips via the tips.fbi.gov portal alleging that seven identified government employees and contractors were involved in unlawful activities at the Capitol on January 6, 2021.

Because of similarities in the wording of the tips, the grouping of the dates the tips were submitted, and the technical tradecraft used to submit them, these tips appeared to be submitted by the same individual. These tips variously alleged that the government employees and contractors were physically present at or involved in the attack at the Capitol or had shared classified information with individuals and groups present at the riot with the intent to assist these groups in overthrowing the United States government.

According to FBI records, all seven tips were submitted from four specific, identified IP addresses. Subscriber information for these IP addresses demonstrated that all four were assigned to a particular provider (hereinafter, “Company A”). Company A provides a service that allows its users to access the Internet via an isolated web browser to help protect users from security threats and for other purposes. In general, when a user of Company A’s services accesses a website through Company A’s product, the website will record an IP address associated with Company A, and not the end user.

According to their published privacy policy, Company A retains records of user activity on their services, including the websites a particular user has visited. Company A also maintains records regarding the identity of users of their platform, including name, username, email, phone number, address, and payment data. Under certain circumstances, they may also collect and maintain information about computers used to access their services, including IP address, operating system, software versions, and other data elements.

According to Company A's logs and records, a single user accessed the FBI's tips portal on each of the dates and at around the times the tips were submitted. Moreover, Company A's logs recorded the user visiting the page that displays the § 1001 banner for each of the seven tips at issue. Based on the design of this page, as shown above, the user must click the "I agree" button to proceed to the tip form. Beyond just the FBI tips portal, the logs recorded some of the web addresses the user visited just before submitting certain tips, including websites related to the government employee or contractor named in the tip that immediately followed.

According to Company A's records, the billing name for the user is "Mike Zapata." ZAPATA created the Company A account in 2017. The contact email address on the account matches one used by "Michael Zapata" on various accounts and records, including a previous loan application. According to U.S. government personnel security records, ZAPATA has used the first names "Michael" and "Miguel." As detailed below, ZAPATA previously worked in the government and, at one time or another, worked with all seven of the government employees or contractors ZAPATA named in the false tips to the FBI.

Zapata's False Tips Regarding the January 6 Attack at the Capitol

None of the seven government employees and contractors were in Washington, D.C., on January 6 or attacked the Capitol.

Below are relevant portions of all seven false tips ZAPATA submitted to the FBI from February through April 2021:

1. February 10, 2021 – Victim 1 and Victim 2

On February 10, 2021, ZAPATA submitted the following tip to the FBI about Victim 1:

[Victim 1] . . . was actively engaged in attempting to overthrow the government of the United States. [He/she] actively took part in the riot on January 6 2021, that lead to the deaths of 6 people.

Additional Info: *Has espoused [...] conspiracy theories and actively retaliates against colleagues that do not share [his/her] political views.*

What was the exact crime that occurred? *Involvement in the Capitol riot and insurrection.*

When did the crime/incident occur? *January 6 2021*

Where did the crime/incident occur? *Washington, DC*

This tip listed Victim 2 as a witness and contained the following additional information in the witness information section of the tip form:

Additional Info: [T]ook part in the Capitol riot and insurrection alongside [Victim 1].

Also on February 10, 2021, ZAPATA reported the following tip to the FBI about Victim 2:

[Victim 2] . . . was actively engaged in attempting to overthrow the government of the United States. [He/she] actively took part in the riot and insurrection on January 6 2021, that lead to the deaths of 6 people.

Additional Info: Has espoused [...] conspiracy theories and aligns with colleagues that share similar views.

What was the exact crime that occurred?: Actively took part in the riot and insurrection at the Capitol.

When did the crime/incident occur? January 6 2021

Where did the crime/incident occur? Washington, DC

This tip listed Victim 1 as a witness.

ZAPATA also included additional details about Victim 1 and Victim 2, including their full names, ages, parts of their addresses, current employers, and security clearance levels.

From around March 2020 until early 2021, ZAPATA worked at the same workplace with both Victim 1 and Victim 2. According to interviews with Victim 1 and Victim 2, and records from their employer at that time, both Victim 1 and Victim 2 were physically at work in Virginia on January 6, 2021.

Company A's logs in February 2021 indicate that ZAPATA visited a section of Victim 1's and Victim 2's employer's website related to reporting activity of concern by employees. On or around February 1, 2021, the employer received an anonymous report regarding Victim 1. According to both the employer and Victim 1, the employer received an anonymous report that Victim 1 had taken part in the attack at the Capitol and bragged about Victim 1's actions to colleagues. The anonymous reporter quoted Victim 1 as having stated, "we're going to hang those dirty politicians and keep President Trump in office for 4 more years." The employer's investigators contacted the anonymous reporter through their online reporting portal, and the reporter responded with additional details including an allegation that Victim 2 also attended the attack at the Capitol.

2. February 16, 2021 – Victim 3 and Victim 5

i. Victim 3

On February 16, 2021, ZAPATA submitted the following tip to the FBI about Victim 3:

[Victim 3] attended the US capitol riot and insurrection and was present when storming the capitol.

What was the exact crime that occurred?: *Took part in insurrection at the US capitol*

When did the crime/incident occur? *January 6 2021*

Where did the crime/incident occur? *US Capitol*

How is Contact Known: *Colleague*

ZAPATA also included additional details about Victim 3, including their full name, age, address, current employer, and security clearance level. The address provided in the tip is a virtual office address publicly available on the internet, and no one works at that location. Victim 3's name, job title, and description are also all available on the company's website.

In and around 2014 and 2015, ZAPATA and Victim 3 worked together. The FBI has interviewed Victim 3, who reported that Victim 3 was physically present at work in Virginia on January 6, 2021.

ii. Victim 5²

Also on February 16, 2021, ZAPATA reported the following tip to the FBI about Victim 5:

[Victim 5] attended the US Capitol riot and insurrection. [He/she] took an active role in leading the riot and storming the US Captiol [sic] to hunt for politicians and execute them.

Additional Info: *In addition to attending the riot and insurrection at the US Captiol,[sic] [he/she] espouses extremist ideology in the work place and has bragged about [his/her] association with the Boogaloo Bois, ProudBoys and Oath Keepers. While serving as a contractor at [an intelligence agency], [he/she] has accessed classified Agency resources to foment terror and incite violence by sharing this information with other conspiracy theory based personalities [...] [He/she] has often talked about "sharing classified information with these groups and individuals as being a [sic] [his/her] duty to ensure the United States Constitution is protected."*

² The designation "Victim 4" is purposefully omitted.

What was the exact crime that occurred?: [Victim 5] attended the US Capitol riot and insurrection

When did the crime/incident occur? January 6 2021

Where did the crime/incident occur? US Capitol

How is Contact Known: Colleague

ZAPATA also included additional details about Victim 5, including their full name, age, current employer, previous employment, and security clearance level.

From approximately 2017 to 2019, ZAPATA worked with Victim 5. The FBI has interviewed Victim 5. According to Victim 5 and supporting documentation, Victim 5 was working in Virginia at the time of the attack on the Capitol on January 6, 2021.

3. February 17, 2021 – Victim 6

On February 17, 2021, ZAPATA submitted the following tip to the FBI about Victim 6:

[Victim 6] attended the capitol riot insurrection. [He/she] was directly involved in coordination of the riot that lead [sic] to the deaths of 6 people.

Additional Info: [...] [he/she] uses [his/her] clearance to continue supporting [an intelligence agency] and accesses classified information.

What was the exact crime that occurred?: [Victim 6] attended the capitol riot insurrection.

When did the crime/incident occur? January 6 2021

Where did the crime/incident occur? Washington DC

How is Contact Known: Colleague

ZAPATA also included additional details about Victim 6, including their full name and nickname, age, current employer, previous employment, security clearance level, and an active hyperlink to Victim 6's LinkedIn page.

In or around 2015 through 2017, ZAPATA previously worked with Victim 6, who had interviewed and hired ZAPATA and then served as ZAPATA's program manager. The FBI has interviewed Victim 6, who reported that Victim 6 was working from their Virginia home during the attack at the Capitol on January 6, 2021. Victim 6's employer provided information related to Victim 6's activity on their virtual private network that demonstrated Victim 6 was working remotely on January 6. Victim 6 denied coordinating any of the January 6 attack at the Capitol.

Company A's logs indicate that on or around February 17, 2021 ZAPATA conducted a Google search for Victim 6, viewed Victim 6's LinkedIn profile that ZAPATA included in his false tip, and viewed a profile for Victim 6 on a website that provides contact and profile information from across the internet—all in the approximately 40 minutes immediately prior to submitting the tip on Victim 6.

4. April 11, 2021 – Victim 7 and Victim 8

i. Victim 7

On April 11, 2021, ZAPATA submitted the following tip to the FBI about Victim 7:

[Victim 7] attended the riot insurrection at the Capitol that lead [sic] to the death of multiple people and the wounding of multiple police officers. [He/she] also provided support to domestic terrorist groups like the OathKeepers, Proud Boys and Boogaloos. [He/she] used [his/her] position of trust in the intelligence community to share classified information with these groups in an effort to assist them succeed in overthrowing the government. [He/she] currently works for [an intelligence agency][...] and is actively engaged in leadership meetings that grant [him/her] higher than normally expected access to classified information. [His/her] actions on January 6 directly lead [sic] to and actively contributed to the successful breach of Capitol police barricades through his encrypted communication techniques used on that day.

What was the exact crime that occurred?: Attended and provided support to the January 6 insurrection riot

When did the crime/incident occur? January 6 2021

Where did the crime/incident occur? Washington DC, Capitol

How is Contact Known: Colleague

ZAPATA also included additional details about Victim 7, including their full name and nickname, age, part of their address, phone number, and current employer.

In approximately 2020, ZAPATA previously worked with Victim 7. The FBI has interviewed Victim 7 and another individual related to Victim 7. According to both Victim 7 and the other individual, Victim 7 was at Victim 7's Virginia home during the attack at the Capitol on January 6, 2021.

Company A's logs for April 11, 2021, indicate that ZAPATA conducted a Google search for Victim 7, viewed a LinkedIn profile for Victim 7, and viewed a Facebook profile for Victim 7 shortly before submitting the tip on Victim 7.

ii. Victim 8

Also on April 11, 2021, ZAPATA submitted the following tip to the FBI about Victim 8:

[Victim 8] provided material support and coordination by way of [his/her] position of trust with access to classified information to domestic terrorist groups like the Proud Boys, Oathkeepers, and Boogaloos. [...] [he/she] shared classified information with terrorist groups in hopes that this information would lead to the overthrow of the United States government. [His/her] position of trust within the intelligence community led to these groups breaching police barricades by

encouraging a flanking maneuver on the barricade that resulted in the overrun of police lines on January 6 2021. [...] [he/she] has maintained access to classified data, senior executive service employees and managers with connections to [an intelligence agency] and grown a social network of classified personnel from which [he/she] has exploited to support insurrection. For over a decade [he/she] has quietly plotted a "change in government" leading to the downfall of United States government and other institutions through [his/her] legacy position of trust and access.

What was the exact crime that occurred?: January 6 insurrection riot at the Capitol

When did the crime/incident occur? January 6 2021

Where did the crime/incident occur? Capitol, Washington DC

How is Contact Known: Colleague

ZAPATA also included additional details about Victim 8, including their full name, age, home phone number, cell phone number, and current employer and a related website hyperlink.

From approximately December 2019 to February 2020, ZAPATA worked with Victim 8. The FBI has interviewed Victim 8, who reported that Victim 8 was working from their Virginia home during the week of the attack on the Capitol on January 6, 2021. Victim 8 did not participate in the attack at the Capitol, did not coordinate groups such as the Oath Keepers or Proud Boys, and has never provided classified information to members of these groups. Victim 8 did not attempt to overthrow the United States government.

ZAPATA's tip included information that Victim 8 would have only provided to coworkers. Specifically, the phone number ZAPATA listed as Victim 8's home phone number is actually Victim 8's spouse's number. Victim 8 reported that Victim 8 only uses that number as a contact number at work, and coworkers would have received a call card with the colleagues' phone numbers to take home.

Company A's logs on April 11, 2021 indicate ZAPATA conducted a Google search for Victim 8, viewed a profile for Victim 8 on a website providing a directory of business contacts (the same hyperlink he included in his false tip), and viewed a LinkedIn profile for Victim 8 just minutes prior to submitting the tip on Victim 8.

According to Company A's logs, web activity for ZAPATA's user account on the dates when the account was used to submit tips was primarily or exclusively related to submitting tips. For example, on February 10, 2021, the FBI's tip site was the only site that the account accessed. On February 16, 2021, the account accessed the FBI's tips site and conducted a Google search for a comic book character but had no other activity. On February 17, 2021³, logs showed ZAPATA's account conducting research -- for example, Google searches or accessing social media or

³ According to Company A's logs, this activity occurred late at night on February 17, 2021, and continued into the early morning on February 18, 2021.

commercial database sites -- on Victim 6 and accessing disposable⁴ email and phone number services in addition to accessing the FBI's tips site; after accessing the tips site, ZAPATA's account accessed a variety of technology-related sites apparently unrelated to the victims or the activity under investigation. On April 11, 2021, Company A's logs showed ZAPATA's user account accessed the FBI's tips site, conducted research on Victims 7 and 8, conducted a Google search for the term "fbi mole," accessed a disposable email service, and accessed the website of an Office of Inspector General for an IC agency.

* * *

Based on the foregoing, I submit that there is probable cause to believe that MIGUEL ZAPATA violated 18 U.S.C. § 1001(a)(2) and (3), which makes it a crime to, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully make any materially false, fictitious, or fraudulent statement or representation, and knowingly and willfully make or use any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry.



Cole Ashcraft
Task Force Officer, FBI Washington Field
Office Cyber Task Force
Special Agent, Treasury Inspector General
for Tax Administration

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this 1st day of May 2024.

G. MICHAEL HARVEY
U.S. MAGISTRATE JUDGE

⁴ Disposable – sometimes called “burner” – email and phone services provide users with short-term access to email addresses and phone numbers that can be used for online or other activity, like sending an email or signing up for an account. By using these services, users can avoid exposing their true phone number or email to entities with whom they are communicating.