

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of Indiana

United States of America)

v.)

John Andrew Smriga III)

Case No.)

2:25-MJ-170)

FILED UNDER SEAL

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 9, 2025 in the county of Lake in the Northern District of Indiana, the defendant(s) violated:

Code Section 18 U.S.C. § 875(c) Offense Description Interstate Communications with a Threat to Injure

This criminal complaint is based on these facts:

See Attached Affidavit

Continued on the attached sheet.

Complainant's signature

SA Jacob Kerwin, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 9/11/2025

s/Abizer Zanzi

Judge's signature

City and state: Hammond, IN

Hon. Abizer Zanzi, US Magistrate Judge

Printed name and title



AFFIDAVIT FOR CRIMINAL COMPLAINT AND ARREST WARRANT:

John Andrew Smriga III

I, Jacob Kerwin, being duly sworn upon oath, state as follows:

1. I am a Special Agent for the Federal Bureau of Investigation and have been so since approximately January of 2018. As part of my duties as a Federal Bureau of Investigation Special Agent, I investigate criminal violations relating to violent crime, such as threats, weapons and drug offenses, and other criminal offenses.

2. The information about the following events, all of which occurred on September 9, 2025, is based upon my personal knowledge, information provided to me by other law enforcement personnel, public records, and records provided by communications companies regarding **John Andrew Smriga III** (hereinafter **SMRIGA**). Based on my training and experience in the investigation of violations of federal laws and my investigation of the facts outlined below, I have probable cause to believe that **SMRIGA** violated **Title 18, United States Code, Section 875(c), Interstate Communications with a Threat to Injure**.

3. On September 9, 2025, an FBI Special Agent put me into contact with Deputy Prosecutor 1 at Prosecutor's Office A. Deputy Prosecutor 1 advised that her supervisor, the elected Prosecuting Attorney in charge of Prosecutor's Office A, had received a threatening text message and picture to

his personal cell phone. I received a picture of the text message sent from the phone number 708-435-2145 (hereinafter **subject phone number 1**). The text message read “Ayo, [Prosecuting Attorney], we know exactly where you lay your head at. Tomorrow, we rollin’ through to grab what’s yours, so you better be set. Ain’t no playin’ around. 🇸🇨” The message included a picture of masked men, some of whom appeared to be gesturing gang signs with their hands, and others of whom appeared to be mimicking guns with their arms and hands. See Figure 1 below.¹



Figure 1

¹ At this time, it is not believed that those depicted in the photo are involved in sending the threat. Instead, based on information provided to me by another FBI Special Agent, I believe that image is associated with a musician known as “Unknown Rdb” and was obtained from the internet.

4. Utilizing law enforcement databases, I determined the carrier for **subject phone number 1** was Sinch Voice. I contacted Sinch Voice via their law enforcement portal “Exigent Circumstances” form. Sinch Voice, which is also known as Inteliquent, provided the following response via email: “Inteliquent/Sinch Voice and its subsidiaries primarily provide wholesale telecommunications services to other telecommunications carriers, resellers and service providers. As a wholesale provider of services, Inteliquent generally does not provide service to or have information on file regarding end user subscribers of telephone numbers. The telephone number is assigned to the following wholesale customer: TextNow, Inc. 420 Wes Graham Way, 2nd Floor, Waterloo, Ontario N2L 0J6 Canada Phone: 202.888.4004 Email: lawenforcement@textnow.com. You must contact TextNow, Inc. to obtain end user/subscriber information.”

5. The following is a summary of TextNow’s services from their website: “TextNow is a voice over Internet Protocol (VoIP) service that allows its users to text and call any number in Canada and the United States. We provide users with a real 10-digit phone number that can be used on a smartphone, tablet, or desktop computer with an internet connection. Users can be logged in to the same account on multiple devices at the same time.”

6. I contacted TextNow via their law enforcement portal and submitted an Emergency Disclosure Request (hereinafter EDR) regarding

subject phone number 1. TextNow responded with subscriber information, which included as a registration IP address of 108.214.186.46 (hereinafter **IP address 1**) and a registration email address of makeadeliverydriverjobharder@gmail.com (hereinafter **email account 1**).

7. I performed an open-source database search of the IP address and learned it was hosted by AT&T Enterprises LLC (hereinafter **ATT**). Subsequently, I called **ATT** and submitted an EDR for the IP address with an origination date of July 30, 2024. **ATT** advised **IP address 1** is currently in use by, and has been since approximately 2021, the customers Debbie and David Niezgoda, with a service address of 5816 W 249th Ave., Lowell, IN 46356-9721 (hereinafter **subject address 1**).

8. During this time, other FBI Special Agents with whom I regularly work submitted an EDR to Google for **email account 1**. Google provided device information from which **email account 1** was created and/or accessed. Within the device information was the device's International Mobile Equipment Identification (IMEI) number, 350318406271397 (hereinafter **IMEI 1**).

9. A subsequent EDR was sent to Verizon with the IMEI, seeking information related to the usage of the device between September 2, 2025 and September 9, 2025. Verizon advised the IMEI of the device, a Samsung Galaxy a15x (hereinafter **device 1**), was utilizing the Verizon phone number 219-789-

3884 (hereinafter **subject phone number 2**). Verizon did not provide subscriber information for the phone number in response to the EDR.

10. In summary, the above information provided me with evidence that the TextNow account associated with the phone number that sent the threat was associated with **subject address 1**, and with **subject phone 2**.

11. I spoke with Indiana State Police Detective Christopher Champione to discuss the investigation. Det. Champione had also been notified of the threat made against the Prosecuting Attorney and was performing his own independent investigation. Det. Champione performed a law enforcement database query of the **subject address 1** which showed SMRIGA (along with Debbie and David Niezgoda) as being associated to the residence. SMRIGA was also associated with a previous complaint made to the FBI National Threat Operations Center in 2021, indicating that he had been the victim of a crime within the area covered by Prosecutor's Office A, and that the matter had not been taken seriously. This complaint was associated with **IP address 1**, which was also used to create the TextNow account discussed above.

12. Det. Champione and I, as well as other members of the Indiana State Police (hereinafter ISP) and FBI, traveled to **subject address 1** and were met by a male, later identified as the homeowner, David Niezgoda (hereinafter DAVID). DAVID advised that SMRIGA was inside the residence.

DAVID allowed law enforcement personnel to enter his residence to speak with SMRIGA.

13. Det. Champione and I spoke with SMRIGA inside **subject address 1**. SMRIGA denied having his phone with him and denied making any threats. However, SMRIGA provided his phone number as **subject phone number 2**, which is the number associated with the TextNow account from which the threat was made. Based on this information, ISP made a probable cause arrest of SMRIGA for violation of Indiana Criminal Code 35-45-2-1, Intimidation, a class 5 felony due to the threat against the Prosecuting Attorney. Det. Champione obtained a search warrant for SMRIGA's electronic devices suspected to be within his bedroom in **subject address 1**.

14. Law enforcement personnel searched SMRIGA's bedroom and located three phones, a desktop computer, and thumb drives. One of the phones, located under SMRIGA's mattress was a Samsung phone which bore **IMEI 1** on the rear cover. Investigators called **subject phone number 2** and the Samsung phone screen illuminated and displayed the incoming call. The phone is currently being analyzed to determine if other evidence may be found on the device.

15. Based on my training and experience, and based on information obtained from other FBI Special Agents with whom I regularly work, text messages and images sent through the TextNow service are transmitted over

the Internet in such a way that generates a wire communication with servers outside of Indiana and therefore any use of the TextNow service creates an interstate wire communication

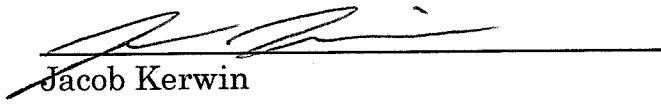
16. In summary, the threatening communication was sent directly to the personal phone of an elected official. The language included statements including claiming knowing where the official lived, that on a specific day they were going to “roll through” and that the official better be ready. It was accompanied by a photo that involved potential gang signs and finger pointing suggesting firearms. This evidence suggests a true threat to the person of another communicated directly to the intended victim. The TextNow account associated with the threat came back to an IP address associated with SMIRGA’s residence. The phone associated with the TextNow account was found in SMIRGA’s bedroom. SMIRGA stated that this was his phone number and when law enforcement called the phone number associated with the TextNow account, that same phone rang.

17. Based on my training and experience, and based on the facts discussed above, I believe that there is probable cause to conclude that **SMRIGA** used **device 1** to transmit the threatening text message and image discussed above to the Prosecuting Attorney using the TextNow service, and that the threatening text message and image were sent in interstate and/or foreign commerce. Accordingly, I believe that there is probable cause to

conclude that **SMRIGA** violated **Title 18, United States Code, Section 875(c), Interstate Communications with a Threat to Injure.**

18. I further request that the Court order all papers in support of this criminal complaint, including the affidavit, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation.

FURTHER SAYETH AFFIANT NAUGHT.



Jacob Kerwin
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me by telephone and transmission of this affidavit by reliable electronic means pursuant to Federal Rules of Criminal Procedure 41(d)(3) and 4.1 on September 11, 2025.

s/Abizer Zanzi

HONORABLE ABIZER ZANZI
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF INDIANA

