

**FILED**

**TD**

**4/1/2026**

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

THOMAS G. BRUTON  
CLERK, U.S. DISTRICT COURT

UNITED STATES OF AMERICA

v.

MICHAEL KOVCO

CASE NUMBER: 26 CR 143  
UNDER SEAL

**FILED**

**LM**

**4/3/2026**

THOMAS G. BRUTON  
CLERK, U.S. DISTRICT COURT

**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 March 19, 2026, at Chicago, Illinois, in the Northern District of Illinois, Eastern Division, the defendant violated:

*Code Section*

*Offense Description*

Title 18, United States Code, Section 875(c)

Transmitting threats in interstate commerce

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

wchrones

Digitally signed by wchrones  
Date: 2026.04.01 15:28:19  
-05'00'

William Chrones  
Special Agent, United States Secret Service  
(USSS)

Pursuant to Fed. R. Crim. P. 4.1, this Complaint is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the Complaint and Affidavit by telephone.

Date: April 1, 2026



*Judge's signature*

City and state: Chicago, Illinois

YOUNG B. Kim, U.S. Magistrate Judge  
*Printed name and title*

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS

**AFFIDAVIT**

I, William Chrones, being duly sworn, state as follows:

1. I am a Special Agent with the United States Secret Service (USSS), and have been so employed since November 13, 2006. My current responsibilities include investigations concerning threats to life against United States Secret Service protected persons (“protectees”) and I am currently assigned to the Protective Intelligence Squad in the USSS Chicago Field Office. I have been involved in dozens of threat investigations.

2. This affidavit is submitted in support of (1) a criminal complaint alleging that MICHAEL KOVCO has violated Title 18, United States Code, Section 875(c); (2) an application for a search warrant to search KOVCO’s residence, the apartment located at 53 [REDACTED] North Cumberland Avenue Apartment [REDACTED] Chicago, Illinois, 60656 (the **Subject Residence**), as described in Attachment A-1, for evidence, contraband, and instrumentalities of the **Subject Offense**, as described in Attachment B; and (3) an application for a search warrant to search KOVCO’s person, as described in Attachment A-2, for evidence, contraband, and instrumentalities of the **Subject Offense**, as described in Attachment B. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging KOVCO and for search warrants for the **Subject Residence** and KOVCO’s person, I have not included each and every fact known to me concerning this

investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint.<sup>1</sup>

3. This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents, law enforcement reports, interviews of witnesses, my experience and training, and the experience of other agents. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part and are not verbatim, except where otherwise indicated, e.g. by quotation marks.

#### **I. SUMMARY OF PROBABLE CAUSE**

4. As detailed below, on March 19, 2026 at 11:27 AM, 29-year-old MICHAEL KOVCO sent a message, via the official White House website, threatening to “hunt” with a firearm USSS Agent 1, who came to his door earlier that day to inquire about a threat message that KOVCO had sent two days earlier. Specifically, on March 19, 2026, KOVCO wrote:

I'm gonna hunt the secret service agent that comes to my door's family so he better not tell me any identifying information at all like first or last name or pet name or address or place of work because im going to buy a small concealable firearm and go shoot up his place of work immediately if he tells me anything

---

A large black rectangular redaction box covering the bottom portion of the page.

(The “March 19 Threat”). The message was posted using an IP address registered to KOVCO at his home, 53 [REDACTED] North Cumberland Avenue Apartment [REDACTED] Chicago, Illinois, 60656 (the “**Subject Residence**”). The message was sent approximately two hours after USSS Agent 1 and two USSS task force officers visited the **Subject Residence** to inquire about a threat KOVCO sent on March 17, 2026 and, receiving no answer, left USSS Agent 1’s contact information on the door knocker of the door of the **Subject Residence**.

5. The USSS investigators went to the **Subject Residence** because two days earlier, on March 17, 2026, KOVCO sent a message to the official White House website threatening President Donald J. Trump and one of his sons (the “March 19 Threat”). KOVCO addressed that message as being from “Mr. I’m going to fucking kill your child Kovco” and included his own contact information, including telephone number [REDACTED]-8560 (the “Subject Phone Number”), his city and area code, and an email address he identified as one of his email addresses. This message was also sent using the IP Address registered to KOVCO at the **Subject Residence**.

6. As detailed below, in addition to the March 19 Threat against USSS Agent 1, KOVCO also sent several additional threat messages via the official White House website on March 19, 2026. These messages were also sent using KOVCO’s registered IP address at the **Subject Residence**, and included identifying information for KOVCO, including his name, the **Subject Residence**, the Subject Phone Number, and his self-identified email address. These messages threatened President Trump, one of his sons, and others.

7. In addition, KOVCO previously sent a message via the Central Intelligence Agency's ("CIA") public website on August 18, 2025 that threatened to kill President Trump. He also included his own contact information with that message, namely the Subject Phone Number and his email address, and sent the message using the IP address registered to him at the **Subject Residence**.

***A. Background Information on KOVCO***

8. According to public record sources, KOVCO is 29 years old and resides at the **Subject Residence** with two adult family members. According to public record sources, and USSS visits to the **Subject Residence**, the **Subject Residence** is a 2-bedroom, 2-bathroom apartment located on the 2<sup>nd</sup> floor of an apartment building, accessible via a common hallway.

9. According to open-source information, IP Address: 73.8.44.67 is registered with Comcast Cable Communications LLC.

10. According to Comcast records, as of March 25, 2026, IP Address 73.8.44.67 is registered to KOVCO at the **Subject Residence**. The telephone number attached to the Comcast account is the Subject Phone Number.

***B. August 15, 2025 Threat Message and Subsequent Interviews***

11. Based on my training and experience, it is my knowledge that many governmental bodies allow individuals to report any suspicious activity or make statements using website comment portals made available on their official government websites. Based on my review of the websites, both CIA.gov and

Whitehouse.gov have contact features that allow for the submission of public comments or messages.

12. As detailed below, during the incidents described in this affidavit, KOVCO utilized official government websites to submit online comment forms making threatening statements, specifically through both the CIA.gov and Whitehouse.gov official public websites.

13. According to the CIA, on or about August 15, 2025, the following message was sent via the CIA's public website: "I am plotting to kill the president of the united states in an ambush with a heavy caliber anti material rifle. Please make a clear line of fire from the white house to marine one on the presidents next departure from the garden." The message provided the following contact information: email address mrmcwaffles@gmail.com and the Subject Phone Number, and self-identified a location of Parkridge, Illinois. The message was associated with IP Address 73.8.44.67, which as stated above, is currently registered to KOVCO at the **Subject Residence**.

14. Based on information provided by the CIA to USSS, USSS identified KOVCO at the **Subject Residence** as the likely author of the August 15, 2025 message. Based on law enforcement databases, USSS determined that KOVCO resided at the **Subject Residence**.

15. On or about August 20, 2025, a USSS investigators went to the **Subject Residence** to attempt to interview KOVCO. First, they encountered and spoke with Individual A, KOVCO's relative who resides with KOVCO, in the hallway outside

their apartment. Investigators asked Individual A if s/he recognized the Subject Phone Number, and s/he stated that it was KOVCO's telephone number.

16. The investigators then spoke with KOVCO. KOVCO stated the following relevant information:

a. Investigators asked KOVCO if he had posted anything threatening in nature on the CIA.gov website. In substance, KOVCO denied posting any threats and claimed others could have posted his information on the website with the threat. KOVCO admitted the Subject Phone Number used to belong to him but claimed he had sold the **Subject Phone** a few months earlier to Store 1. Using google.com, USSS Agents later determined that there was only one known location for Store 1.<sup>2</sup>

b. KOVCO also volunteered that mrmcwaffles@gmail.com was one of his email addresses. At the time KOVCO said this, investigators had not yet indicated that the email address mrmcwaffles@gmail.com was provided in the August 15, 2025 message. When investigators pointed this out to KOVCO, he responded, in substance, "oh well I just assumed" that either that email address would have been used or his other email address.

---

<sup>2</sup> During the interview, KOVCO indicated he sold the phone to the Store 1, which he described as down the street from where he lived in July. Based on information currently known to me, KOVCO had not resided anywhere other than the **Subject Residence** during the time period of August 2025 to present. According to public source information, including Google.com, Store 1 has only one location, which is in Norridge, Illinois and, according to Google Maps, is approximately a 3 minute drive or 16 minute walk away from the **Subject Residence**. Therefore, I believe that KOVCO misspoke about Store 1's location.

c. KOVCO also told investigators that he had previously been [REDACTED] and hospitalized for approximately one week.<sup>3</sup> KOVCO stated that while he was admitted to the hospital, he was prescribed certain medications, which he no longer takes. KOVCO also stated that he is unemployed and has little money.

17. During the interview, investigators then called the Subject Phone Number, and it went straight to voicemail with the recorded message, “This is Mike, please leave a message.” Additionally, it appeared to investigators, based on their observations of KOVCO and experience, that the voice on the voicemail message was consistent with KOVCO’s voice, who they were speaking with at that same time.

18. After interviewing KOVCO, USSS investigators went to Store 1 to inquire about the phone that KOVCO said he had sold to them. Individual B, the store manager, stated they do not buy phones from individual people and stated that he has not bought a phone from an individual in about 3 years.

***C. March 17, 2026 Threat Message***

19. Based on my training and experience, and the training and experience of other law enforcement officers, and review of Whitehouse.gov, I know many

---

<sup>3</sup> During the August 20, 2025 interview, KOVCO voluntarily signed an SSF 1945 form authorizing USSS to obtain his medical records. [REDACTED]

governmental bodies allow individuals to report any suspicious activity or make statements using website comment portals made available on their official government websites. Specifically, the “Contact Us” page located at <https://www.whitehouse.gov/contact/> requires the individual fill in a prefix, first and last name, country, full address, phone number, and email address to submit a comment.

20. On or about March 17, 2026, the following message was sent via the White House public website (the “March 17 Threat”):

I'm going to take a serrated knife and saw Barron Trump's head off after I successfully stake out the president of the united states with a high caliber sniper rifle permanently aimed at the White House Lawn from a local vantage point. I have absolutely every intent of plotting and carrying out an active assassination attempt against the President of the United States of America. This is a serious threat.

The message provided the following contact information:

From: Mr. I'm going to fucking kill your child Kovco  
Address: GOD Chicago, IL 60656  
Email: mrmcwaffles@gmail.com  
Phone: [the Subject Phone Number]

This message was sent using IP Address: 73.8.44.67.

21. Based on the message’s IP address and the provided contact information, USSS believes KOVCO submitted the March 17 Threat. Namely, it states it is from “Mr. [ ] Kovco,” it list the **Subject Residence**’s city and area code, and KOVCO’s self-identified phone number, the Subject Phone Number, and self-identified email address. Additionally, it was sent using the IP address registered to KOVCO at the **Subject Residence**.

#### *D. March 19, 2026 Threats and Interviews*

22. On March 19, 2026, USSS Agent 1 and two USSS task force officers went to the **Subject Residence** to attempt to interview KOVCO about the March 17 Threat. At approximately 9:30 AM CT, USSS Agent 1 and two USSS task force officers visited the Subject Residence and knocked on the door. After receiving no answer, USSS Agent 1 left a card with his contact information on the door knocker of the door of the **Subject Residence**.

23. At approximately 9:42 AM CT, investigators called Individual A, who resides with KOVCO, asking if s/he would be home in the near future.<sup>4</sup> S/he responded that s/he would be home around noon and agreed to meet with investigators at the residence at that time.

24. According to information received from the USSS Protective Intelligent Division, located in Washington D.C., the following messages were sent via the White House public website on or about March 19, 2026 between approximately 10:26 AM and 11:30 AM CT:

a. At 11:26 AM CT From: "Admiral Michael Kovco": "I intend to purchase a high caliber assault rifle with a large magazine and assemble several improvised explosive devices within my home at [the North Cumberland Residence] and leave them in several key places around Washington DC until I get justice for my rape from the US government."

---

<sup>4</sup> USSS Investigations obtained the cellular telephone number of Individual A through a TLO query.

b. At 11:27 AM CT from “Mr. Michael Kovco”: “I’m gonna hunt the secret service agent that comes to my door’s family so he better not tell me any identifying information at all like first or last name or pet name or address or place of work because im going to buy a small concealable firearm and go shoot up his place of work immediately if he tells me anything”

c. At 11:29 AM CT from “Mr. Michael Kovco”: “I’m going to leave improvised explosive devices which i do not currently have the means to manufacture but can purchase with relatively little resources and assemble with relatively little effort at some point in the future as a punitive action against any secret service agent who comes to respond to these clear and apparent threats.”

d. At 11:28 AM CT, from “Mr. Michael Kovco”: “I’m literally gonna find out how Barron Trump walks around in NYC or DC or wherever the fuck he is and run at him with a serrated bread knife and saw that motherfuckers head off”

e. At 11:30 AM CT from “Mr. Michael Kovco”: “You’re never going to get another courtesy call with the Chicago Police Department ever again =)” “it’ll just take about two years (if you last that long) (Barney/Kenny Williams/Michael Kovco Child Porn/Defend the President at all costs/how does he know/you’re all going to fucking die. it’s VULCAN”

25. All of the above messages were sent via the IP Address registered to KOVCO at the **Subject Residence**. KOVCO also filled in his name, Subject Phone Number, email, and the **Subject Residence**.

26. At approximately 12:00 PM CT, USSS Agent 1 and investigators returned to the **Subject Residence** and met with Individual A in the hallway outside the **Subject Residence**.<sup>5</sup> One of the investigators was equipped with body-worn camera that recorded their interactions. In substance, Individual A denied knowledge about the March 17 Threat. S/he stated that KOVCO was not presently compliant with his [REDACTED] medication, he was unemployed, and rarely left the **Subject Residence**.

27. Then, KOVCO exited the **Subject Residence** and spoke briefly with investigators in the hallway. As captured on one investigator's body-worn camera footage, KOVCO became very agitated when USSS Agent 1 identified himself and explained he was there about a comment that someone posted to the White House website that Monday. KOVCO interrupted and said "That's fucking hilarious. It wasn't me. Go Fuck yourself. Go get a warrant for my arrest." After briefly stepping back into the apartment and slamming the door behind him, KOVCO returned to the hallway and asked USSS Agent 1, in substance, why he was there. After USSS Agent 1 responded that he investigates threats against the President, KOVCO said "Ok, I posted four more. I'm gonna get money from your ass. Go check it out." KOVCO then went back into the **Subject Residence** and the investigators left.

---

<sup>5</sup> USSS Agent 1 and the investigators were not aware of the March 19, 2026 threats messages at the time of their interview with Individual A or KOVCO. Specifically, USSS received the March 19, 2026 threat messages on or about March 25, 2026 from the USSS Protective Intelligence Operation Center (PIOC) in Washington D.C.

28. As discussed in paragraphs 22 to 25, the five message KOVCO sent on March 19, 2026 were sent after USSS Agent 1 left his contact information on the door of the **Subject Residence** and approximately 30 minutes before he told USSS Agent 1 that he had “posted four more” threats.

### ***The Subject Phone***

29. Based on my training and experience, there is probable cause to believe that KOVCO has used and continues to use the **Subject Phone** because: (1) Individual A, his relative, identified the Subject Phone Number as his phone number in August 2025; (2) the **Subject Phone** Number is associated with a Comcast account registered in KOVCO at the **Subject Residence** as recently as March 26, 2026; (3) KOVCO that it was previously his phone number; (4) the voicemail message for the **Subject Phone Number** as of August 20, 2025 identified the user as “Mike,” KOVCO’s first name, and according to USSS investigators who were speaking to KOVCO, the voice on the message was consistent with KOVCO’s voice; and (5) Individual B, the manager of the cell phone store that KOVCO claimed to have sold his phone to a few months earlier, Store 1, told Investigators that they do not buy phones from individuals and had not done so in 3 years.

## **II. PROBABLE CAUSE TO SEARCH**

30. Based on my training and experience, individuals transmitting threats via the internet on social media, do so utilizing electronic devices including but not limited to cell phones, tablets, computers, and “smart” watches.

31. Based on my training and experience, I believe that a search of

electronic devices of individuals engaged in transmitting threats yields investigative leads relating to:

- a. the transmitted threats themselves;
- b. the identities of participants engaged in and witnesses to the threat;
- c. the contact information of participants engaged in and witnesses to the threat;
- d. discussions regarding planning and implementing the threat;
- e. the location of participants engaged in making the threat; and
- f. the methods and techniques used to promote or carry out the threat.

32. Based on my training and experience, individuals who commit, or threaten to commit, acts of violence often possess weapons, firearms, ammunition, magazines, and weapons of mass destruction to include incendiary or explosive devices. These weapons can be stored anywhere that is readily accessible to the individuals, including in residences.

### **III. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA**

33. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (e.g. computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a

qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

34. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications

software which may have been used to create the data (whether stored on hard disk drives or on external media).

35. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain evidence or were used to carry out criminal activity.

36. Based on my training and experience, and my involvement in this matter, individuals, like KOVCO, who commit the Subject Offense do so often using electronic means. In addition, individuals who plan to carry out violent threats are likely to have evidence of the Subject Offense on their devices, including Internet searches, notes, and messages associated with the threats. Therefore, I submit that there is probable cause to search any electronic devices found within the Subject Residence that is reasonably believed to be used or possessed by KOVCO and/or on KOVCO's person, as they will likely contain evidence of the Subject Offense, including items related to threats made by KOVCO, as well as other criminal violations, items reflecting his ownership of the Subject Phone Number or email address, items related to KOVCO's use or possession of weapons, and items related to any attack planning or research.

37. The warrant I am applying for would permit law enforcement to obtain from KOVCO the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock electronic devices subject to

search and seizure pursuant to this warrant. I seek this authority based on the following:

a. 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 and laptops, 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 and facial 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.

b. 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 fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. 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, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then

analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. 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.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For

example, Apple devices cannot be unlocked using Touch ID when (1) more than a certain number of hours have elapsed since the device was last unlocked or (2) when, within a certain number of hours, the device has not been unlocked using a fingerprint and the passcode or password has not been entered. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of MICHAEL KOVCO, if found at the **Subject Residence** and reasonably believed by law enforcement to be a user of a device found at the residence or on KOVCO's person, to the fingerprint scanner of the device; (2) hold the device in front of the face of KOVCO and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

#### IV. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

38. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the residence described in Attachment A

so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

39. The review of electronically stored information and electronic storage media removed from the residence described in Attachment A-1 may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures if those procedures are designed to minimize the review of information not within the list of items to be seized as set forth in Attachment B:

a. examination of categories of data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;

c. surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word or concept searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B; and

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment B.

40. The government will return any electronic storage media removed from the residence described in Attachment A within 60 days of the removal unless, pursuant to Rule 41(c)(1), (2), or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains evidence or contraband, or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

**V. CONCLUSION**

41. Based on the information above, Affiant submits that there is probable cause that MICHAEL KOVCO transmitted threats in interstate commerce, in violation of Title 18, United States Code, Section 875(c).

FURTHER AFFIANT SAYETH NOT.

**wchrones** Digitally signed by wchrones  
Date: 2026.04.01 15:09:11  
-05'00'  
\_\_\_\_\_  
William Chrones  
Special Agent, United States Secret Service  
(USSS)

SWORN TO AND AFFIRMED by telephone April 1, 2026.

\_\_\_\_\_  
Honorable YOUNG B. KIM  
United States Magistrate Judge