UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

v.

TRENT SCHNEIDER

CASE NUMBER: 25 CR 708

~~UNDER SEAL~~

FILED
10/31/2025
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 October 16, 2025, at Lake County, in the Northern District of Illinois, Eastern Division, the defendant(s) violated:

Code Section	*Offense Description*
Title 18, United States Code, Section 875(c)	making a true threat to injure another person in interstate commerce.

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

MICHAEL S RIDINGS
Digitally signed by MICHAEL S RIDINGS
Date: 2025.10.30 21:42:34 -05'00'

MICHAEL RIDINGS
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: October 31, 2025

Judge's signature

City and state: Chicago, Illinois

GABRIEL A. FUENTES, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS

AFFIDAVIT

I, MICHAEL RIDINGS, being duly sworn, state as follows:

1. I am a Special Agent with the United States Secret Service (USSS) and have been so employed for three years. I am currently assigned to the Protective Intelligence Squad in USSS's Chicago Field Office. I am also a Task Force Officer with the Joint Terrorism Task Force in the Federal Bureau of Investigation's (FBI) Chicago Field Office. My current responsibilities include the investigation of threats to life against USSS-protected persons. In my capacity, I have been involved in multiple threat investigations.

2. This affidavit is submitted in support of: (1) a criminal complaint alleging that TRENT SCHNEIDER has violated Title 18, United States Code, Section 875(c) by making threats in interstate commerce to injure another person (the "**Subject Offense**"); (2) an application for a search warrant to search SCHNEIDER's residence, the single-family home and free-standing shed located at 2810 15th St. in Winthrop Harbor, Illinois (the "**Subject Residence**"), as described in Attachment A-1, for evidence and instrumentalities of the **Subject Offense**, as described in Attachment B; (3) an application for a search warrant to search SCHNEIDER's person, as described in Attachment A-2, for evidence and instrumentalities of the **Subject Offense**, as described in Attachment B; (4) an application for a search warrant to search the Instagram account with the username "truthreaper888" that

is subscribed to SCHNEIDER (the "**Subject Account**"), as described in Attachment A-3, for evidence and instrumentalities of the **Subject Offense**, as described in Attachment A-3(III). Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging SCHNEIDER and search warrants for the **Subject Residence**, SCHNEIDER's person, and the **Subject Account**, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe establish probable cause to believe that SCHNEIDER committed the **Subject Offense**, and that evidence and instrumentalities of the **Subject Offense** will be found during a search of the **Subject Residence**, SCHNEIDER's person, and the **Subject Account**.

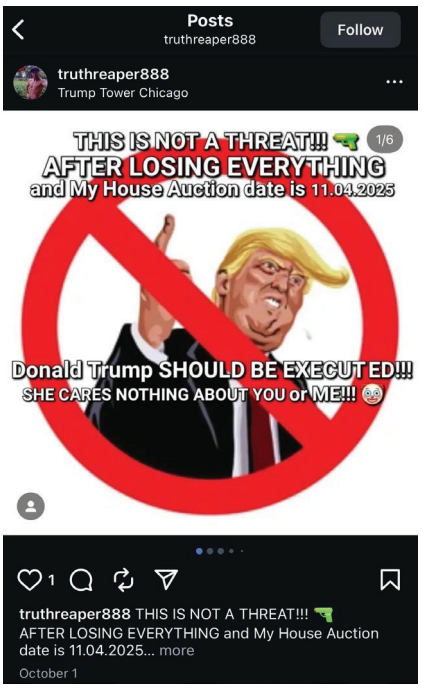
3. This affidavit is based on my personal knowledge, information provided to me by other law enforcement agents, law enforcement reports, interviews of witnesses, my experience and training, and the experience and training of other agents.

SUMMARY OF PROBABLE CAUSE

4. As further described below, on or about October 16, 2025, SCHNEIDER publicly posted to the **Subject Account** a video of himself in which he, in part, stated: "I'm going to get some guns. I know where I can get a lot of fucking guns and I am going to take care of business myself. I'm tired of all you fucking frauds. People need to fucking die and people are going to die. Fuck all of you, especially you Trump. You should be executed." The video also included a caption stating, in part: "THIS IS

NOT A THREAT!!! 🔫 AFTER LOSING EVERYTHING and My House Auction date is 11.04.2025 @realDonaldTrump SHOULD BE EXECUTED!!! 🔫 SHE IS A #FRAUD and a #COWARD!!! 🤓 SHE CARES NOTHING ABOUT YOU or ME!!!" SCHNEIDER posted this same video and caption on the **Subject Account** approximately 18 times between October 16, 2025 and October 21, 2025.

5. SCHNEIDER also posted the below picture approximately 20 times to the **Subject Account** between September 26, 2025 and October 21, 2025. In several instances, the picture was included in the same post as the aforementioned video. Many of the posts also included the tagged geolocation of Trump Tower in Chicago, Illinois.



6. Based on my training and experience, I know that public posts to the **Subject Account** are viewable via the internet to persons anywhere in the United States. I am specifically aware that, on or about October 16, 2025, a concerned citizen

in Florida viewed the October 16, 2025 video posted by the **Subject Account** and reported it.

BACKGROUND

Background on Meta and Instagram[1]

7. Based on my training and experience, I have learned the following about Meta and Instagram:

a. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A-3, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

b. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code),

[1] The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Privacy Policy," https://privacycenter.instagram.com/policy/; "Information for Law Enforcement," https://help.instagram.com/494561080557017; and "Help Center," https://help.instagram.com.

telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

c. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

d. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

e. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records

of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

f. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

g. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

h. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the

user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

i. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

j. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

k. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

l. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

m. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

n. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

o. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag.

Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

p. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

q. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

r. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

s. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user

(including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

t. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

u. The stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, voice messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

8. The servers of Meta are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, transaction information, and account application. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Meta, to protect the rights of the subjects of the investigation and to effectively pursue this investigation, authority is sought to allow Meta to make a digital copy of the entire contents of the information subject to seizure specified in Section II of Attachment A-3. That copy will be provided to me or to any authorized federal agent. The contents

will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A-3.

Background on SCHNEIDER

9. SCHNEIDER is a 57-year-old male who lives alone in Winthrop Harbor, Illinois. According to law enforcement databases, law enforcement reports, and law enforcement contacts, SCHNEIDER resides at 2810 15th St. in Winthrop Harbor, Illinois 60096 (the "**Subject Residence**").

10. According to court records, SCHNEIDER is the defendant in a pending foreclosure action. According to open-source databases, the **Subject Residence** will be presented at a foreclosure auction on November 4, 2025.

11. According to law enforcement reports, SCHNEIDER posted multiple violent messages about public officials on various social media accounts in 2022. In response, federal and local law enforcement officers interviewed SCHNEIDER at the **Subject Residence** in March 2022.

12. According to law enforcement reports, in December 2022, law enforcement officers arrested SCHNEIDER based on a report that SCHNEIDER made threats to "shoot up" a T-Mobile store. When law enforcement officers attempted to stop SCHNEIDER, SCHNEIDER fled and continued to resist arrest when apprehended by law enforcement thereafter. Following this incident, law enforcement officers executed a search of the **Subject Residence**. No firearms or ammunition were found during the search, but law enforcement officers did observe and photograph a crossbow at the **Subject Residence**.

13. On March 21, 2023, according to law enforcement databases, SCHNEIDER was found unfit to stand trial for charges related to the December 2022 arrest.

Identification of SCHNEIDER as User of the Subject Account

14. The **Subject Account** is an Instagram account with the username "truthreaper888." The display name on the account is "'Trent Schneider." According to subscriber records from Meta, the registered name and date of birth for the **Subject Account** match SCHNEIDER's name and date of birth as reflected in law enforcement databases.

15. I have compared the photograph from SCHNEIDER's Illinois State Identification card to the **Subject Account**'s profile photo and videos posted by the **Subject Account**. Based on this visual comparison, I believe the photos and videos posted on the **Subject Account** depict SCHNEIDER. Specifically, I believe the individual depicted in the aforementioned October 16, 2025 video posted to the **Subject Account** is SCHNEIDER.

16. I and two other law enforcement officers attempted to interview SCHNEIDER at the **Subject Residence** on October 22, 2025. I observed cameras set up on tripods in the driveway as I approached the door. An individual matching SCHNEIDER's appearance exited the residence as we approached. I compared the appearance of the individual with the photograph from SCHNEIDER's Illinois State Identification card and the videos on the **Subject Account**. Based on this visual comparison, I believe the videos posted on the **Subject Account** depict SCHNEIDER

and that I encountered SCHNEIDER on October 22, 2025. I asked SCHNEIDER if he had posted threats online. In response, SCHNEIDER became irate and started yelling for the officers to get off his property. Approximately one hour of after I left the **Subject Residence**, the **Subject Account** posted a video of myself and the two other law enforcement officers who attempted to interview SCHNEIDER walking down his driveway. The post contained the same threatening caption as the previously described video posted by the **Subject Account** on October 16, 2025; in relevant part, the caption stated, "THIS IS NOT A THREAT!!! 🔫 AFTER LOSING EVERYTHING and My House Auction date is 11.04.2025 @realDonaldTrump SHOULD BE EXECUTED!!! 🔫"

17. According to open-source databases, the **Subject Residence**, where SCHNEIDER resides, will be presented at a foreclosure auction on November 4, 2025. Numerous posts on the **Subject Account** state, "My House Auction date is 11.04.2025."

18. In 2022, USSS interviewed SCHNEIDER at the **Subject Residence** in response to his violent social media posts regarding government officials. According to a photograph taken during the interview, SCHNEIDER was wearing a black baseball hat that depicted a white "Punisher" style skull with yellow hair. SCHNEIDER is wearing the same hat in all the aforementioned videos posted on the **Subject Account**.

SCHNEIDER'S THREATS TO PUBLIC FIGURES

19. On October 16, 2025, SCHNEIDER posted a "selfie" style video to the **Subject Account** in which he is speaking directly to the camera. In this video, SCHNEIDER, in part, stated:

> People like me have suffered real fucking crimes from fucking judges, doctors, lawyers, police. They all should be killed. All of them should be executed for what they've done. They need to be killed. They need to be executed, ok? They are frauds, ok? *I think it's time. I've waited long enough. I'm going to get some guns. I know where I can get a lot of fucking guns and I am going to take care of business myself. I'm tired of all you fucking frauds. People need to fucking die and people are going to die*. Fuck all of you, especially you Trump. You should be executed. (emphasis added)

20. The video included a caption stating, in part: "THIS IS NOT A THREAT!!! 🔫 AFTER LOSING EVERYTHING and My House Auction date is 11.04.2025 @realDonaldTrump SHOULD BE EXECUTED!!! 🔫 SHE IS A #FRAUD and a #COWARD!!! 😇 SHE CARES NOTHING ABOUT YOU or ME!!!"

21. SCHNEIDER posted this video on the **Subject Account** as a standalone post 7 times on or about October 16, 2025. Multiple of these posts included a tagged geolocation of the Trump Tower in Chicago, Illinois.

22. On or about October 16, 2025, a concerned citizen in Florida viewed this video posted on the **Subject Account** and reported it to law enforcement.

23. In addition, SCHNEIDER has repeatedly posted on the **Subject Account** a photo of the likeness of President Donald Trump superimposed with a red

circle with a line drawn through it and the statement, in part, "Donald Trump SHOULD BE EXECUTED!!!" This post included a caption stating, in part, "THIS IS NOT A THREAT!!! 🔫 AFTER LOSING EVERYTHING and My House Auction date is 11.04.2025 @realDonaldTrump SHOULD BE EXECUTED!!! 🔫 SHE IS A #FRAUD and a #COWARD!!! 😇 SHE CARES NOTHING ABOUT YOU or ME!!!" Many of the posts also included a tagged geolocation of the Trump Tower in Chicago, Illinois. SCHNEIDER posted this photo as a standalone post on the **Subject Account** on the following dates: September 26, September 27, September 28, September 29, October 1, two times on October 15, and two times on October 16, 2025.

24. On October 17, 2025, SCHNEIDER combined this video and photo in one post on the **Subject Account**, with the first slide as the photo of the likeness of President Donald Trump described and included above and the second slide as the video in which SCHNEIDER threatens to "get a lot of fucking guns" and "take care of business himself." SCHNEIDER made these combined posts on the **Subject Account** on the following dates: October 17, five times on October 19, and five times on October 21, 2025.

25. On October 21, 2025, according to law enforcement officers, SCHNEIDER appeared in court and at one point stated to the judge that he would "burn this castle down." When asked by the judge if it was a threat, SCHNEIDER said it was not.

PROBABLE CAUSE TO SEARCH

26. 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.

27. Based on my training and experience, users of social media websites and applications, such as Instagram, frequently access their accounts from multiple devices, including personal cell phones, computers, and tablets.

28. 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, garages, sheds, and storage lockers.

29. Based on my training and experience, I believe that a search of social media accounts 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.

SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

30. 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.

31. 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).

32. 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.

33. Based on my training and experience, and my involvement in this matter, individuals, like SCHNEIDER, who commit the **Subject Offense** do so often using electronic means, and individuals who are active social-media users, like SCHNEIDER is, are likely to have such social-media accounts on their cellphones and other devices. 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** and/or on SCHNEIDER's person, as they will likely contain evidence of the **Subject Offense**, including items related to threats made by SCHNEIDER, items reflecting his ownership of the **Subject Account**, items related to SCHNEIDER's use or possession of weapons, and items related to any attack planning or research.

34. The warrant I am applying for would permit law enforcement to obtain from SCHNEIDER 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 SCHNEIDER, if found at the **Subject Premises** and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device;[2] (2) hold the device in front of the face of SCHNEIDER 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.

PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA AND AUTHORIZATION REQUEST

35. 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 **Subject Premises** described in Attachment A-1 and on SCHNEIDER's person, as described in Attachment A-2, 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.

36. The review of electronically stored information and electronic storage media removed from the **Subject Premises** described in Attachment A-1 and on SCHNEIDER's person, as described in Attachment A-2, may include the following techniques (the following is a non-exclusive list, and the government may use other

[2] Law enforcement will select the fingers to depress to the fingerprint scanner to avoid compelling the user of the device to disclose information about his or her knowledge of how to access the device.

procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the 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 (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above;

c. surveying file directories and the individual files they contain 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 searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

37. The government will return any electronic storage media removed from the **Subject Premises** described in Attachment A-1 and from SCHNEIDER's person, as described in Attachment A-2, within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic

storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

PROCEDURES TO BE FOLLOWED IN SEARCHING THE SUBJECT ACCOUNT

38. In order to facilitate seizure by law enforcement of the records and information described in Attachment A-3, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Meta Platforms, Inc. to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Meta Platforms, Inc. personnel who will be directed to the information described in Section II of Attachment A-3;

b. In order to minimize any disruption of computer service to innocent third parties, Meta Platforms, Inc. employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A-3, including an exact duplicate of all information stored in the computer accounts and files described therein.

39. Meta Platforms, Inc. employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A-3 and all information stored in those accounts and files to the agent who serves this search warrant; and

40. Following the protocol set out in the Addendum to Attachment A-3, law enforcement personnel will thereafter review all information and records received from Meta Platforms, Inc. employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A-3.

CONCLUSION

41. Based on the information above, I submit that there is probable cause to believe that SCHNEIDER committed the **Subject Offense**, namely, making threats in interstate commerce, and that evidence and instrumentalities of the **Subject Offense**, described more fully in Attachments B and A-3(III), are likely to be found in the **Subject Residence**, on SCHNEIDER's person, and in the **Subject Account**.

FURTHER AFFIANT SAYETH NOT.

MICHAEL S RIDINGS Digitally signed by MICHAEL S RIDINGS Date: 2025.10.30 21:43:17 -05'00'

MICHAEL RIDINGS
Special Agent
United States Secret Service (USSS)

SWORN TO AND AFFIRMED by telephone October 31, 2025.

Honorable GABRIEL A. FUENTES
United States Magistrate Judge