IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF 1909 WASHINGTON AVENUE, PORTLAND, MAINE	Magistrate No.: 2:25-mj-00176-KFW Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Andrew M. Allaire, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for 1909 Washington Avenue, Portland, Maine 04103. The location to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant for the home described in Attachment A for the evidence of the crimes committed further described in Attachment B.

2. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 419(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. I am a Special Agent with the FBI and have been so employed since May 2017. I am currently assigned to the Portland, Maine Resident Agency in the Boston Field Office. I have primarily investigated violations of federal law, including but not limited to, carjackings, robberies of banks, robberies of businesses that affect interstate commerce (also known as Hobbs Act robberies), kidnappings and crimes against children. Furthermore, I have received training and experience as a police officer in the City of Biddeford, State of Maine, for approximately six years prior to my current position as a Special Agent.

4. I have participated in numerous violent-crime investigations and have debriefed or participated in debriefings of numerous defendants, informants, and witnesses who had personal knowledge regarding crimes of violence.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that ALICE JONES, date of birth July 2, 1985, has violated Title 18, United States Code, Sections 871 and 875(c). As set forth below, JONES is believed to reside at 1909 Washington Avenue, Portland, Maine (the "SUBJECT PREMISES"). There is probable cause to search the SUBJECT PREMISES, further described in Attachment A, for the evidence further described in Attachment B.

PROBABLE CAUSE

7. On May 12, 2025, a member of the Wells Police Department ("Wells PD") contacted the FBI in Portland, Maine concerning threatening communications being made toward their officers. It was reported that a call was received on May 11, 2025, at 2:03 AM by the Wells PD Police Chief (the "Chief") on her cell phone. The call was made from telephone number (508) 377-6705 (hereinafter, "SUBJECT TELEPHONE"). The unknown caller, a female, called the Chief a "nazi."

8. About five minutes after to the call to the Chief, the Wells Dispatch Center received a telephone call from the SUBJECT TELEPHONE. This call to the dispatcher is summarized as follows:

a. The female caller called the dispatcher a "fucking nazi" and ridiculed Wells Police for being the first in the State of Maine to work alongside Immigration and Customs Enforcement;

b. The caller stated to the dispatcher, "let me know if you want to get slit all the way through your throat, bitch, cause you're a fucking nazi."

c. The caller referenced the level of armor ICE agents wear, threatened that there are going to be dead ICE agents, and referred to the Chief as a "[d]ead nazi cunt walking."

d. The caller stated that she just got her first gun, has received extensive training, and that this is what the Second Amendment is for.

e. The caller took credit for doxing police officers in Worcester and Nashville, stating that they would do the same to Wells PD.

9. On May 11, 2025, at about 2:15 AM, the same female called the dispatch center again from the SUBJECT TELEPHONE and threatened to go sit outside of the Wells Police Station and follow the dispatcher home from her shift. The caller claimed to be a member of Antifa New England.[1] The dispatcher received another call on May 11, 2025 at approximately 2:17 AM, in which the female caller stated, "If you nazi cunts do anything here like what happened in Worcester, you are going to have some dead ICE agents."

10. On May 11, 2025 at approximately 2:20 AM, a Wells PD Officer ("Officer 1") received a call from the SUBJECT TELEPHONE on her personal cell phone. The female caller

[1] I understand "Antifa" to refer to a loose collection of persons and groups who claim to oppose fascism.

recited Officer 1's home address where Officer 1's child was then home. Officer 1 feared for her child's safety and contacted local police there to check her residence.

11. On May 11, 2025, at approximately 2:30 AM the mother of a Wells PD Sergeant ("Sergeant 1") received a call from the SUBJECT TELEPHONE on her home phone number. The female caller stated that that Sergeant 1's mother would end up dead if she was supporting ICE. The caller called Sergeant 1's mother a nazi, at which point Sergeant 1's mother ended the call and blocked the number.

12. On May 11, 2025, at approximately 1:40 a.m. Central Daylight Time, the mother of another Wells PD Sergeant ("Sergeant 2") who lives outside the District of Maine received a call from the SUBJECT TELEPHONE. The female caller stated, "You are a fucking nazi. You will die because you are a fucking nazi." Sergeant 2's mother ended the call and continued to receive six more calls in succession from the SUBJECT TELEPHONE. The threatening calls were reported to local police.

13. On May 11, 2025, at approximately 6:16 PM, Wells PD Dispatch received a call from the SUBJECT TELEPHONE in which the female caller demanded to know what was going on with Wells Officers being deputized as ICE agents. The call was forwarded to a Wells PD Corporal ("Corporal") who continued the call from a desk phone. The female caller recited a list of all of the Wells Police Officers. She claimed to know what level of protection their vests were rated for. The female repeatedly called the Corporal a nazi and stated that all nazi's are going to be murdered. The Corporal asked the female if she was done, and she stated that she will be done when President Trump is dead. She stated that she has wanted him dead since the early 2000s. The Corporal asked whether caller wanted President Trump dead, and she replied, "I want to slit his throat, I want to be the one to do it." The caller stated that she and Antifa militias

are real and that she is a researcher for the militia, not a field worker. During the call, the female caller referenced a police interaction she had last Thanksgiving involving revenge porn where the Portland Police did not help her.

14. On May 13, 2025, I researched the SUBJECT TELEPHONE in FBI systems and identified a connection to an FBI Jacksonville case opened on May 10, 2025. FBI records indicate that on May 10, 2025, a Supervisory Border Patrol Agent ("Border Patrol Agent") began receiving threatening and harassing calls from the SUBJECT TELEPHONE. The Border Patrol Agent believed the calls were prompted by a video posted on the internet which showed his participation in a May 2025 traffic stop in Florida.

15. The Border Patrol agent received a call from the SUBJECT TELEPHONEon May 10 at approximately 6:20 PM. At the time of the call, the Border Patrol Agent was not in Maine. During this call, which was not recorded, a female caller told the Border Patrol Agent that he was the reason the second amendment existed and that she was coming for him. The caller called two additional times and the Border Patrol recorded these additional calls. In the recorded calls, the female caller referred to the Border Patrol Agent as a nazi. She told him that Americans murder nazis. She stated, "If you keep fucking with citizens you're going to die. This is what the Second Amendment is for." The Border Patrol Agent asked the female for her name and the female caller challenged him to figure it out. The female caller recited the Border Patrol Agent's name and date of birth. The female caller's statements caused the Border Patrol Agent to fear for his and his family's safety.

16. A complaint was made to the FBI in Jacksonville regarding the threatening communications. FBI Jacksonville identified the SUBJECT TELEPHONE as a Pinger/TextFree number. An emergency disclosure request (EDR) was sent to Pinger. The

response from Pinger identified two recent IP addresses used by the number an Apple ID, Apple push token, and an advertising ID. Pinger records showed that the account associated with the SUBJECT TELEPHONE was created on May 9, 2025 at 11:11 PM (UTC). Pinger provided two last known IP address associated with the account. IP address 67.244.32.113 was last captured on 05/11/25 at 2:39 AM UTC and IP address 174.196.202.162 on 05/10/25 at 10:18 PM UTC.

17. FBI Jacksonville issued an EDR to Apple, Inc., for subscriber information associated with the Apple ID, push token, and advertising ID that Pinger had provided with respect to the SUBJECT TELEPHONE. Apple responded and identified the subscriber as ALICE JONES of 1909 Washington Avenue, Portland, Maine. Associated email addresses, forms of payment, registered devices were all in the name of ALICE JONES and address of 1909 Washington Avenue.

18. FBI Jacksonville submitted an EDR to Charter Communications with one of the IP addresses utilized by the SUBJECT TELEPHONE. Charter identified the subscriber as Carolyn Ramm of 1909 Washington Avenue, Portland, ME. Based on open-source checks, Ramm also resides at 1909 Washington Avenue. In addition, Cumberland County records indicate that both Carolyn Ramm and Alice Jones are listed on the Deed to 1909 Washington Ave, Portland, Maine.

19. On May 13, 2025, I learned that the Worcester, Massachusetts police department contacted the Portland, Maine police department requesting information on JONES. Police Officers in Worcester had also reported receiving threatening calls believed to originate from JONES. I further learned that Worcester Police contacted Pinger and were provided with recent IP Addresses associated with the SUBJECT TELEPHONE, which included 67.244.32.113, 174.196.195.97.

20. Maine Bureau of Motor Vehicles records indicate that ALICE JONES has a valid Maine driver's license with an address listed of 1909 Washington Avenue, Portland, ME 04103. She has one active vehicle registration, also with 1909 Washington Avenue as the listed address.

Similar Conduct to Current Activities

21. In February 2025, a Texas Fusion Center observed a post on X in which the user of X account @Jenen6616071188 was posting threats including threats to kill Elon Musk. A series of court orders were served in an attempt to identify the user of the account. Subsequently, I learned that agents believed that Alice Jones may be the user of the X account, and I was asked to visit Jones' residence at the SUBJECT PREMISES.

22. On April 2, 2025, I went to the SUBJECT PREMISES to attempt to speak to JONES. Upon arriving at her residence, there were no vehicles in the driveway and a large spray painting reading, "BOMB BOOMERS" was displayed at the entrance to the driveway. Painted onto the window was a Ukraine flag with a math equation over the flag. The equation began with "Elon=…" I knocked on the front door for several minutes and heard at least one dog barking just inside the front door, but never got an answer. In the following weeks, I made several telephone calls and a second in person visit to the residence, but never got an answer or call back from JONES.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet Protocol Address: An Internet Protocol address ("IP address") is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP

address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers ("ISPs"). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets ("octets") of numbers, each ranging from 0 to 255, separated by periods (e.g., 149.101.82.209). An IPv6 address has eight groups ("segments") of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (e.g., 2607:f330:5fa1:1020:0000:0000:0000:00d1).

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

24. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files and information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes

how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of 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. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated

into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought,

computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to transmit communications threatening to injure another, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how

the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

g. Based on the facts alleged in this affidavit, I believe it is likely that the Target of this investigation used a computer to conduct internet searches to identify and target victims, to identify victim's addresses and phone numbers, and to obtain personal identifying information of the victims, such as dates of birth. While such information might be obtained through non-computer and non-internet sources, such information is, based on my training and experience, most readily available through searches of internet databases.

27. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily

viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

29. Because it is possible that more than one person shares the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

30. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock 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 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. 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. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is

the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

31. 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 any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals 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.

CONCLUSION

32. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

33. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

ANDREW M. ALLAIRE
Special Agent
Federal Bureau of Investigation

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: May 14 2025

City and state: Portland, Maine

Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title