IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF 426 SWAIN ROAD, RUMFORD, MAINE	No. 2:22-mj-00011-JCN

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Emily Spera, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 426 Swain Road, Rumford, Maine, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

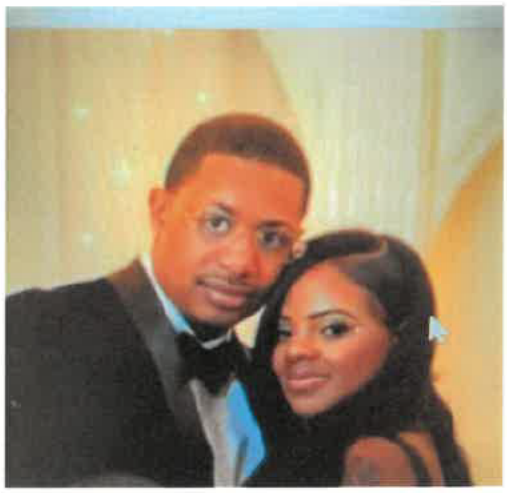
2. I am a U.S. Postal Inspector with the United States Postal Inspection Service assigned to the Boston Division. I have been a Postal Inspector for ten years. Among my assignments are the investigation of violent crimes including robbery of U.S. Postal Service (USPS) employees, assaults, and burglaries of USPS facilities. I have been trained in all aspects of investigations relating to the U.S. mails at the Postal Inspection Service Training Academy in Potomac, Maryland. I have also completed investigative courses sponsored by the U.S. Postal Inspection Service which focused upon violent crime investigations involving postal employees and its facilities.

3. This affidavit is intended to provide the facts necessary for a determination of probable cause for the requested search warrant.

PROBABLE CAUSE

A. Post Office Burglaries

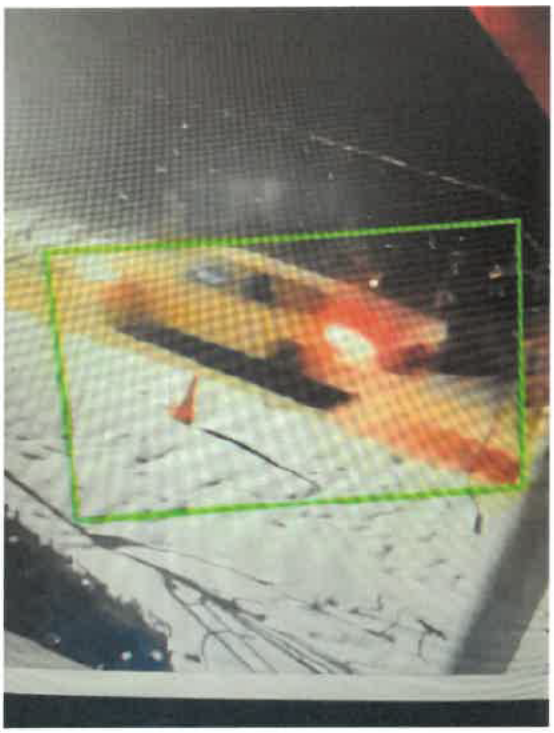
4. I know from my participation in this investigation that on about January 14, 2024, Postal Inspectors were notified of a burglary at the Paris, Maine Post Office located at 39 Tremont St. During law enforcement's investigation of the incident, it was determined that entry was made through a window, and that postal equipment to include keys, mail, and a money order printer were taken. Officers located two Apple iPhones in the snow directly beneath the broken window. Both phones were placed in airplane mode, shut off and placed into evidence. The generic lock screen on one of the iPhones had a photo of a black male and black female. A U.S. Postal Inspection Service (USPIS) analyst was able to use facial recognition software and identified the male pictured on the lock screen as Target Subject Winston MCLEOD. The images pulled from the iPhone are depicted below:



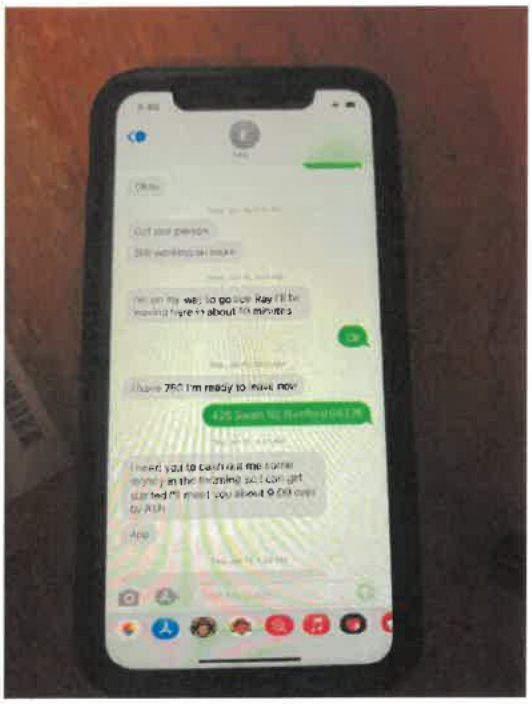
5. I have compared these photographs with my observations of MCLEOD and with a photograph taken of MCLEOD during his detainment at the Rumford Police Department on January 21, 2024 (described herein), and I have concluded that the images recovered from the iPhone depict MCLEOD. A photograph of MCLEOD taken at on January 21, 2024 appears below:

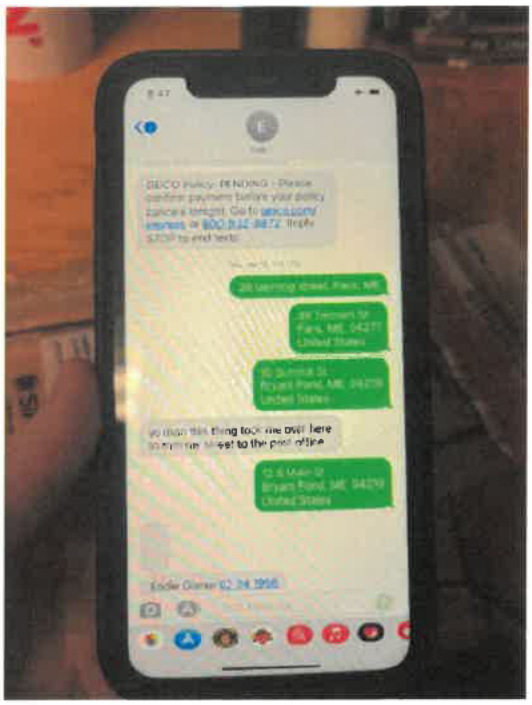
6. Officers were able to recover surveillance video during their investigation of the post office burglary. Appearing on video taken in the neighborhood of the Paris

post office during the approximate time of the burglary depicted a white SUV. An image from the video appears below:



7. Officers obtained judicially authorized search warrants to search both of the cellular phones recovered from the scene of the burglary. During the search of the phones, messages between the owner of the phone (believed to be MCLEOD) and a contact listed as Eddy (believed to be Target Subject Eddie GILMER) were recovered. Screen shots of relevant text messages are depicted below. Among other things, MCLEOD texted "Eddy" the address of the PREMISES when "Eddy" indicated that he was "ready to leave now" on about January 11, 2024. That same day, MCLEOD also appears to have texted "Eddy" the address of the Paris Post Office.





8. I know from my participation in this investigation that just two days after the Paris Post Office robbery, on about January 16, 2024, at approximately 12:10 P.M. Postal Inspectors were notified of a burglary at the North Monmouth Post Office located at 140 N Main St., North Monmouth, Maine. Initial investigation revealed that mail, a laptop, and a money order printer were taken and entry was made through a window.

B. Armed Robberies of Postal Carriers

9. I know from my participation in this investigation that on about January 20, 2024, Postal Inspectors were notified of an armed robbery of two USPS Letter Carriers just minutes apart in Lewiston, Maine. The first robbery occurred at 20 Davis St., and the second robbery occurred at 480 Main St. The 911 call from the letter carrier

of the second robbery was placed at 11:54 A.M. Lewiston Police and Postal Inspectors responded.

10. I know from conferring with law enforcement officers, and from reading their report, that the victim letter carrier ("Carrier-1"), informed officers that the robber was a black male approximately 5'6", thin build, wearing a ski mask, armed with a knife. She described the assailant's vehicle as a small white SUV with a black male driver. She stated the robber instructed her to "give me the mailbox key." The assailant left with her USPS vehicle keys and personal cell phone.

11. I know from interviewing the second victim letter carrier ("Carrier-2") that he was outside of his vehicle at 480 Main St. when he was approached by a black male who stated, "give me your key or I'll kill you." The suspect held a knife at Carrier-2's throat and then his ribs. Carrier-2 described the knife as a black "butterfly" knife, approximately 6" in length. Carrier-2 removed the postal key that was attached to his person and gave it to the robber who fled into the passenger seat of a car parked nearby. Carrier-2 described the assailant's vehicle as a white colored vehicle, possibly a PT Crusier, bearing a Maine license plate.

12. Law enforcement conducted a canvas of the incident locations and were able to recover video of the robbery that occurred at 20 Davis St. That video depicts a

white SUV, later identified as 2010 Jeep Patriot, stopping alongside the USPS vehicle and committing the robbery. Images from that video appear below.[1]

13. Law enforcement conducted a review of other surveillance footage obtained by the Lewiston Police Department. That review shows that the Jeep Patriot

---

[1] Note that the time stamp on the camera from the resident is ahead by approximately one hour.

depicted above traveled throughout Lewiston following the robberies, eventually crossing the bridge into Auburn. I know from debriefing Lewiston officers that during the timeframe of these two incidents, one Lewiston officer observed a white Jeep SUV in the area and noted the first two numbers of the license plate as "85."

C. Traffic Stop of the Ford Mustang

14. I know from my participation in this investigation that on about January 20, 2024, at approximately 3:09 P.M., Rumford Police conducted a traffic stop on U.S. Route 108 of a 2023 Ford Mustang bearing Pennsylvania registration MDK1544. The operator was identified as Target Subject Lance FUNDERBURK, and the front seat passenger was MCLEOD. During the encounter, officers observed that MCLEOD, who gave a fake name, was wearing a black balaclava and a baseball cap. FUNDERBURK was carrying two knives on his person, including a black butterfly knife. During a consensual search, officers recovered a large sum of currency from FUNDERBURK's wallet. A K9 search was conducted on the Mustang, and the K9 alerted to the presence of narcotics. A subsequent search of the Mustang revealed several checks with different names inside a Louis Vuitton case.

15. As the Mustang was being searched, Target Subject Uniah LEIDY and Target Subject Eddie GILMAN arrived at the scene in a white Jeep Patriot bearing Maine registration 8534RD (the "SUBJECT VEHICLE"). GILMAN advised officers that the Mustang was his rental vehicle that he allowed MCLEOD and FUNDERBURK to use.

16. During the investigation, MCLEOD was arrested for an active warrant. Later, at the Rumford Police Department, a custodial search of MCLEOD's person was conducted, revealing $4,382 in U.S. currency in his underwear.

D. Events at the Rumford Police Department

17. While at the Rumford Police Department, law enforcement contacted FUNDERBURK and advised him to pick up MCLEOD. However, LEIDY arrived at the Rumford Police Department to bail MCLEOD and stated she was alone. Officer suspected that LEIDY was not alone; an officer went outside and located the SUBJECT VEHICLE in the post office parking lot next door. In the back seat of the SUBJECT VEHICLE, FUNDERBURK was located laying on the floorboards. He was then detained at the Rumford Police Department.

18. Officers searched FUNDERBURK pursuant to arrest and the following items, among others, were recovered: white gloves dipped with red palms and fingers, lighters, Vaseline jelly, assorted keys, key fob, black mulitfunction tool, $1,005.00 cash, TD Bank card for Eddie GILMER, black matte butterfly knife with 4" silver blade and four cell phones.

19. Officers placed the keys recovered from the search of FUNDERBURK on the desk in the room in which he was being detained. Surveillance video of the interrogation room in which FUNDERBURK was detained shows that FUNDERBURK stood up while handcuffed and approached the keys, picked up a key, and then appeared to place the key into his pants. FUNDERBURK can be seen moving his hand around the rear of his buttocks. Police later conducted a strip search and the key was not located

inside FUNDERBURK's pants or between his buttocks. It is believed that FUNDERBURK pushed the key inside the rectum to prevent the key from being obtained. Images from the surveillance video appear below.

20. Following these events, officers drove to the PREMISES and made contact with GILMER. GILMER was subsequently detained and transported to the Rumford Police Department. All four individuals were searched and, as of this writing, are being detained by law enforcement.

E. Pole Camera Footage of the PREMISES

21. I know from conferring with Rumford Police that they have been independently investigating the PREMISES for drug trafficking activity. Pursuant to that investigation, they have utilized covert surveillance to identify vehicles and visitors to the PREMISES. I have reviewed pole camera footage of the PREMISES captured pursuant to this independent investigation. On about January 20, 2024, at approximately 12:55 P.M., FUNDERBURK was seen entering the PREMISES. He was wearing a dark colored sweatshirt and dark pants. At approximately 1:10 P.M.

FUNDERBURK was seen taking items from the Ford Mustang into the PREMISES, this time with a brown jacket over the sweatshirt. Still images isolated from the pole camera footage appear below.

22. I have reviewed additional pole camera footage of the PREMISES showing the SUBJECT VEHICLE leaving the PREMISES at approximately 10:00 A.M. on about January 20, 2024. At approximately 12:03 P.M., GILMER arrived at the PREMISES in the Mustang. At approximately 12:55 P.M., the SUBJECT VEHICLE returned to the

PREMISES, approximately one hour following the robberies of the Postal Carriers described above.

23. Following her arrest, LEIDY waived her *Miranda* rights and stated to law enforcement that she had allowed FUNDERBURK and MCLEOD to use her vehicle, the SUBJECT VEHICLE, and that they had been staying at her residence, the PREMISES. LEIDY further stated that FUNDERBURK and MCLEOD were at the PREMISES on the afternoon of January 20, 2024.

24. The Mustang and a mobile home are both located at the PREMISES. I also seek authority to search the Mustang and mobile home pursuant to the instant warrant. In my training and experience, thieves often store contraband and stolen merchandise in outbuildings and other structures on their property in order to secure the contraband, and in order to avoid its detection by visitors to the main living quarters on the property. Furthermore, law enforcement has already recovered evidence of the postal robberies in the Mustang, as described further above.

25. Because LEIDY who resides at the PREMISES is currently in custody, but will presently be released from custody following the completion of her interview with law enforcement, and because LEIDY is aware of this instant investigation, the PREMISES must be searched as soon as possible in order to prevent LEIDY or her coconspirators from returning to the residence and effectuating the destruction of evidence. It is anticipated that the release of the suspect will happen presently; as a result, the undersigned requests authority to effectuate the search authorized by this warrant during nighttime hours in order to avoid the destruction/spoilation of evidence.

TECHNICAL TERMS

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

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

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

27. As described above and in Attachment B, this application seeks permission to search for records that might be found on the 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).

28. *Probable cause.* I submit that if a computer or storage medium is found on the 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."

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files 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). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. 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.

30. *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.

31. *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.

32. Because it is currently unknown whether the Target Subjects are the only individuals to reside at the PREMISES, it is possible that the 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 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.

CONCLUSION

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

Respectfully submitted,

Emily Spera
U.S. Postal Inspector
United States Postal Inspection Service

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

Date: Jan 21 2024

City and state: Bangor, ME

Judge's signature

John C Nivison U.S. Magistrate Judge

Printed name and title