AFFIDAVIT IN SUPPORT OF APPLICATION FOR CRIMINAL COMPLAINT, ARREST AND SEARCH WARRANT

I, Casey Biagiotti, being duly sworn, state as follows:

Introduction and Agent Background

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and I have been employed as a Special Agent since January 2021. I am currently assigned to the Joint Terrorism Task Force ("JTTF") of the Boston Division of the FBI. I am currently working in conjunction with the Violent Crimes Task Force ("VCTF") of the Boston Division of the FBI. As an FBI SA, I am responsible for the investigation of federal criminal offenses and have participated in various investigations which include investigative activities such as executing search and arrest warrants, conducting interviews of victims, witnesses, and suspects, issuing and reviewing the returns of subpoenas, and conducting physical and electronic surveillance. I have also received specialized training regarding investigative techniques and evidence collection and preservation.

2. I am currently investigating Marshall Nicholas Fain ("Fain"), DOB: xx/xx/1990, for cyberstalking, in violation of 18 U.S.C. § 2262A, and transmitting a threat in interstate commerce, in violation of 18 U.S.C. § 875(c) (collectively, the "Target Offenses").

3. Based on my training and experience, I am aware that a violation of 18 U.S.C § 875(c) makes it a federal offense for any individual to knowingly transmit in interstate or foreign commerce any communication containing any threat to kidnap or injure the person of another; and that 18 U.S.C. § 2261A(2) makes it a federal offense for any individual, with the intent to injure, harass, or intimidate another person, to use

any electronic communication service or any other facility of interstate or foreign commerce to engage in a course of conduct that places that other person in reasonable fear of the death of or serious bodily injury to a person, or that causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to that other person or that person's immediate family member.

4. The facts stated herein are based on my own involvement with this investigation, as well as from information provided to me by other law enforcement officers involved in the investigation. This affidavit is being submitted for the limited purpose of establishing probable cause to believe that Fain committed the Target Offenses. Therefore, I have not included all facts known to me concerning this investigation.

5. This affidavit is submitted in support of: (1) a criminal complaint charging Fain with the Target Offenses; (2) an arrest warrant for Fain; and (3) a search warrant for the person of Fain, as further described in Attachment A, annexed hereto and incorporated herein by reference. For the reasons detailed herein, there is probable cause to believe that the items described in Attachment A will comprise or contain evidence, instrumentalities, or fruits of the Target Offenses, as more fully described in Attachment B, which is also annexed hereto and incorporated herein by reference.

Probable Cause to Believe that FAIN Committed the Target Offenses

6. On October 7, 2021, M-C D-S ("Victim's mother") DOB: xx/xx/1972, reported to the FBI National Threat Operations Center ("NTOC") that she and her

daughter, J D-T ("Victim") DOB: xx/xx/1994[1], a resident of Massachusetts, had been receiving death threats from the Victim's ex-boyfriend, Fain. The threats were being sent via email, social media, and text message. M-C D-S and the Victim were interviewed by investigators on October 7, 2021 and expressed fear and concern for their lives.

7. Investigators conducted a subsequent interview with the Victim on October 12, 2021. The Victim stated she was in a relationship with Fain for approximately two years, spanning from October 2019 to August 2021. The Victim reported that they broke up in mid-August 2021, and that after she ended the relationship, she began receiving threats. On September 12 and 13, 2021, the Victim reported to Boston Police Department ("BPD") she had received death threats from Fain that made her fear for her life. On September 16, 2021, the Victim was granted an abuse prevention order, docket number 2107RO1062, against Fain from the Dorchester District Court. The Victim filed subsequent reports with local police alleging violations of the abuse prevention order on September 30, 2021 and October 9, 2021 as Fain continued to contact and threaten her via text message, social media, and email. Among other things, the Victim reported she changed her telephone number as a result of Fain's continued contacts.

8. On September 25, 2021, the Victim received a direct message on her Instagram account[2] from Instagram user "@godsun203" stating, "I'll kill you, Joey

[1] The identities of the victim and her mother are known to investigators but are being withheld to protect their privacy.

[2] Instagram is a photo and video sharing social networking service in which users sign up with registered email address and select their username and display name. Users can post photos, stories, and send and receive private direct messages to other Instagram users.

badass and 600 breezy bitch"[3], "I'm back in Boston". A copy of this message was provided to Investigators by the Victim.

9. A subpoena to Facebook Inc. for subscriber records of the "@godsun203" Instagram account revealed that the account had an associated email address of marshallfain2@gmail.com. A subpoena to Google for information about the subscriber of the email address marshallfain2@gmail.com revealed Marshall Fain to be the account owner. The "@godsun203" Instagram account was created on September 25, 2021. Upon receiving this message the Victim filed a report alleging a violation of the abuse prevention order with BPD, specifically referencing the phrase, "I'll kill you."

10. On October 6, 2021, the Victim received two direct messages on her Instagram account from Instagram user with the identifiers "Sauce Gang Musik" and "@supremenation704" which read, "You gonna get yours if it's the last thing I do. Massachusetts ain't far. Y'all better move from 509 soon. Because I promise ima get you", "I got your mom and [your sister][4] number. Tell them they next to get a number change." A copy of these messages was provided to investigators by the Victim.

11. Facebook Inc., provided Instagram records which indicate, among other things, that this account was accessed on the day of the threat, October 6, 2021, from IP address 2607:fb90:b029:afcb:b146:52e2:9d0f:a422. That IPv6 address is unique and specific to T-Mobile telephone number, XXX-XXX-2473 (hereinafter, "the 2473 number"). T-Mobile records provide the 2473 number is registered to Witness 1, DOB:

[3] The Victim stated, "Joey badass" and "600 Breezy" are rappers who Fain was aware that the Victim found attractive.

[4] Investigators are aware of the identity of the Victim's sister but have withheld her name to protect her identity. The Victim understood "509" to be a reference to her address, which was known to Fain.

XX/XX/1961.[5]

12. On October 5, 2021 at 1:45pm, an individual believed to be Fain telephonically contacted Farm Bureau Insurance to report the Victim for committing insurance fraud regarding a car accident in April of 2021. Fain left a detailed voicemail in which he stated his name and that his contact telephone number is the 2473 number. On October 8, 2021 at approximately 9:40am, Investigator Lane Robinson of Farm Bureau Insurance returned Fain's call at the 2473 number. During the recorded phone call, Fain stated he was currently residing in Connecticut.[6] Farm Bureau Insurance notified the North Carolina Department of Insurance the Victim had allegedly committed insurance fraud.

13. On October 6, 2021 the Victim received an email from "Grim Reaper" at "devilsadvocate704@gmail.com" titled, "You're gonna die", stating, "I'm gonna find you and kill you if it's the last thing I do. Boston isn't far AT ALL. You and [your sister] not safe. Nobody is. Ima get you bitch. And I know you know I'm not playing. By now you know I don't give a fuck about my own life so I really don't mind taking yours." A copy of this message was provided to Investigators by the Victim. Google records show this email account was accessed on October 7, 2021 at 02:02 UTC[7] from IP address 2607:fb90:70eb:a725:c885:9e15:16fc:4c05. T-Mobile records indicate this IPv6 address

[5] Witness 1 is a resident of New Haven, CT whose identity is known to investigators. Investigators are aware that Witness 1 was romantically involved with Fain. Witness 1 has not yet been interviewed.

[6] Special Agent Jessica Smith of the North Carolina Department of Insurance provided this information to investigators in January 2022 after becoming aware of the FBI's investigation into Fain involving the Victim. Investigators are in possession of the recorded voicemail and phone call and interview with Investigator Lane Robinson.

[7] Coordinated Universal Time (UTC) is five hours ahead of Eastern Standard Time.

is unique and specific to T-Mobile telephone number 2473, which I understand to mean that the 2473 number is the device that used the above IP address on October 7, 2021.

14. On October 8, 2021 the Victim received an email from "Haze Blak"[8] at "hazeblak69@gmail.com" titled "Time is ticking" stating, "Nobody can keep you safe 100% of the time. Not your sister, not them n****s, not your parents, not even law enforcement. You will get caught slipping. I know how to track people better than central intelligence lol. When the time is right you gonna be one of the girls going missing. Ima torture the fuck out of you when I catch you. You gonna pay for playing with my emotions bitch. Then you can be a mother to the baby you murdered." A copy of this message was provided to Investigators by the Victim. Google records indicate this email account was accessed on October 8, 2021 from IP address 2607:fb90:b057:fdae:115e:e776:6cd5:be1a. T-Mobile records indicate this IPv6 address is unique and specific to T-Mobile telephone number 2473.

15. On October 9, 2021, due to the messages received on October 6, 2021 and October 8, 2021, the Victim explained to investigators that she feared for her life. The Victim filed an additional report of a violation of the abuse of prevention order with BPD.

16. On October 12, 2021 the Victim received an email from king.james653@yahoo.com stating, "Watch your mouth on Facebook. You must really wanna speed up your death. I'm tryna take my time and let you live a little but you keep it up and I'll be there sooner than later. I don't give a fuck about being embarrassed. You

[8] According to the victim, "HAZE BLAK" was a nickname for the Victim's father and Fain was aware of that. The victim also informed Investigators that the email did not come from her father.

gonna be dead. You and your sister. Stupid broke bitch. Always calling someone a bum but you sleep on your sisters couch and you broke as fuck. Stop it. You depending on a lawsuit that you lied about lol. You're a loser bitch." A copy of this message was provided to investigators by the Victim.

17. Yahoo records produced in response to a subpoena show this email account listed the 2473 number as the verified recovery phone number.[9] This Yahoo email account was created on October 12, 2021.

18. On October 12, 2021 the Victim received an email from god_your@yahoo.com stating, "…What can you do to me when NOBODY KNOWS WHERE I AM? On the other hand tho. You're the one exposed. I know your address and where family members and certain friends live at. Checkmate. P.S. N****s don't spend their life in jail for stalking threats and harassment and shit. The cops ain't gonna protect you anyway. All these missing bitches and they ain't doing shit."[10] A copy of this message was provided to Investigators by the Victim.

19. Yahoo records produced in response to subpoena show this Yahoo email account also lists the 2473 number as the recovery phone number. This Yahoo email account was created on October 12, 2021.

20. On October 15, 2021 during an interview of Witness 2, an associate of Fain, who reports having known Fain for approximately eight to nine years, Witness 2

[9] When a user creates a Yahoo email account, a recovery phone number is an optional entry for the user to give, in the event the user is locked out of their account. A code or link will be sent to the phone to authenticate that the user signing up for the email account is the same user of the telephone number. When the telephone number is, "verified" it means that the user authenticated their phone number via the code or link during account creation.

[10] This is a truncated version of the full email to depict only relevant statements.

stated Fain had contacted them from the 2473 number to apologize for his recent behavior.[11] Witness 2 stated Fain had not previously used the 2473 number.

21. On November 3, 2021 the Victim received an email from marshallfain2@gmail.com titled "Shits hard…" stating, "I miss you so much man I can't even lie this shit hurts so bad…I only said the mean things recently because of my broken-hearted anger…But I'm not gonna harasss you, post things, and threaten you anymore or bother your family. Been 3 weeks since I did that and I'm honestly done. That shit got tiring and pointless…"[12] A copy of this message was provided to investigators by the Victim.

22. On December 26, 2021 the Victim received an email from marshallfain2@gmail.com stating, "I can't wait to catch you. Ima cut you up and then light your hair on fire. Ima record you burning to death with a no attempts hoody on. Ima pee on you and choke you until you die." A copy of this message was provided to investigators by the Victim.

23. As outlined above in Paragraph 12, in October 2021, Fain lodged complaints about the Victim with an insurance agency in North Carolina, where the Victim and Fain had at one time lived, and the insurance agency referred the matter to the North Carolina Department of Insurance. On January 3, 2022, Special Agent Jessica Smith of the North Carolina Department of Insurance attempted to contact Fain at the 2473 number. An unidentified male answered the phone and stated Fain had a new number. Special Agent Smith, based on her familiarity with Fain's voice as it was

[11] The identity of Witness 2 is known to investigators.
[12] This is a truncated version of the full email to depict only relevant statements.

recorded by the Farm Bureau Insurance, believed that this male was indeed Fain. Special Agent Jessica Smith relayed this information to Investigators.

24. On January 18, 2022, Fain contacted Special Agent Jessica Smith via the 2473 number and confirmed the 2473 number is his current telephone number and provided his current address in, Hamden, CT. Special Agent Jessica Smith relayed this information to Investigators.

25. Based upon interviews conducted with the Victim on October 7, 12, and 21, 2021, November 18, 2021, and January 4, 2022, investigators believe the Victim was fearful for her life as the Victim had expressed serious concern for her safety regarding the threats she received from Fain. The Victim stated she was afraid of Fain and described his demeanor as threatening and aggressive. During interviews, the Victim displayed signs of emotional distress, such as crying, when discussing Fain's threats.

Probable Cause to Believe that Evidence, Fruits, and Instrumentalities of the Target Offenses Will Be Located on FAIN's Person

26. Based on my training and experience as an FBI Special Agent, as well as through conversations with other members of law enforcement, I know that people engaged in criminal activity, especially criminal activity that involves phone calls and text messages, frequently possess evidence of that criminal activity on their cell phones. Data relating to such communications, as well as myriad types of additional evidence, including online banking records, internet search history, and social media activity is frequently stored on a cell phone. I also understand that people regularly possess their cell phones on their person. In this case, Fain is believed to have used multiple forms of electronic communication to, among other things, threaten and harass the Victim. The evidence shows that the 2473 number, which is serviced by cellular carrier T-Mobile, is

associated with various Google, Yahoo, and Instagram accounts that Fain has used to harass and threaten the Victim. Furthermore, Fain has been identified by multiple individuals as using the 2473 number, including by a law enforcement agency as recently as January 2022. For these reasons, and based on the information outlined below, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the Target Offenses will be located on Fain's person.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

27. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

28. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

29. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

30. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after 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, which might not occur for long periods of time. 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 the computer has been used, what it has been used for, and who has used it. This 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. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a 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, email 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.

f. 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).

g. 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.

h. 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.

i. 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.

31. Based on my knowledge and training and the experience of other agents

with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence C storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on site.

b. Technical requirements C analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise 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. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the

system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

c. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

BIOMETRIC UNLOCKING

32. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

33. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used

instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

34. The passcode that would unlock the device(s) found during the search of Fain's person is not currently known to law enforcement. Thus, it may be useful to press his finger(s) to the device's fingerprint sensor or to hold the device up to Fain's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

35. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of Fain to the sensor of the device(s) found on his person or place the device(s) in front of his face for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Conclusion

36. Based on the aforementioned information, I respectfully submit there is probable cause to believe that on various dates from in or about September 2021 through in or about December of 2021:

a. Fain knowingly transmitted in interstate or foreign commerce any

communication containing any threat to injure the person of another, in violation of 18 U.S.C § 875(c); and

b. Fain, with the intent to injure, harass, or intimidate another person, used any electronic communication service or any other facility of interstate or foreign commerce to engage in a course of conduct that placed that other person in reasonable fear of the death of or serious bodily injury to a person, and that caused, attempted to cause, and would be reasonably expected to cause substantial emotional distress to that other person or that person's immediate family member, in violation of 18 U.S.C. § 2261A(2).

37. I also submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the Target Offenses, as described in Attachment B, will be found on Fain's person, as described in Attachment A.

Respectfully Submitted,

Casey Biagiotti
Special Agent, FBI

Date and time: ~~February~~ _____, ~~2022~~ at **6:31 PM, Feb 1, 2022**

Notice is hereby provided that, pursuant to Fed. R. Crim. P. 4.1, the affiant was sworn by telephone on the date and time indicated above and on the search warrants and criminal complaint issued by the court.

HONORABLE JENNIFER C. BOAL
UNITED STATES MAGISTRATE JUDGE

PERSON TO BE SEARCHED

MARSHALL FAIN, year of birth 1990, is pictured below:

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 875(c) and 18 U.S.C. § 2261A, for the period from March 12, 2021 to present including:

A. Records (including communications) and tangible objects pertaining to the following people, entities, addresses, telephone numbers, websites, email addresses and electronic identifiers, IP address:

1. The Victim;

2. The Victim's family, including her mother and sister;

3. The 2473 number;

4. IP addresses:

2607:fb90:b029:afcb:b146:52e2:9d0f:a422;
2607:fb90:70eb:a725:c885:9e15:16fc:4c05;
2607:fb90:b057:fdae:115e:e776:6cd5:be1a;

5. Email accounts:
marshallfain2@gmail.com;
devilsadvocate704@gmail.com;
hazeblak69@gmail.com;
king.james653@yahoo.com;
god_your@yahoo.com;

6. Instagram accounts identified by:

"@godsun20";
"Sauce Gang Musik",
"@supremenation704";

7. Farm Bureau Insurance; North Carolina Department of Insurance;

8. The Victim's sister's address;

B. Records and tangible objects pertaining to the travel or whereabouts of Fain;

C. Records and tangible objects pertaining to the existence and identity of co-conspirators;

D. For any computer hardware, computer software, mobile phones, or storage media

called for by this warrant or that might contain things otherwise called for by this warrant (the computer equipment):

1. Evidence who used, owned, or controlled the computer equipment;

2. Evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

3. Evidence of the attachment of other computer hardware or storage media;

4. Evidence of counter-forensic programs and associated data that are designed to eliminate data

5. Evidence of when the computer equipment was used;

6. Passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

7. Records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage; and

8. Serial numbers and any electronic identifiers that serve to identify the equipment.

II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for items described in paragraph I.

III. During the execution of the search of the person described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of Marshall Fain to the sensor of the subject device(s) and/or to hold the device(s) in front of his face.

DEFINITIONS

For the purpose of this warrant:

A. "Equipment" means any hardware, software, storage media, and data.

B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such

as electronic data security hardware and physical locks and keys).

C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.