IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN THE MATTER OF THE SEARCH OF **403 2nd Street N, Pflugerville, TX and electronic devices found therein**

Case No. A-18-M-208

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

I, **REYNALDO ALATORRE, JR.**, 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 search warrant authorizing the examination of property described in Attachment A for the items described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), United States Department of Justice, and have been so employed since July 2001. Prior to my employment with the ATF, I was employed as a Border Patrol Agent for approximately four years. As a result of my training and experience, I am familiar with firearms and with Federal Firearms Laws, including Title 26 offenses concerning destructive devices. I have also discussed this investigation with other ATF Special Agents with specialized experience in Destructive Devices (explosive device(s)) and Destructive Device investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The

investigation described below is at its preliminary stages and facts continue to develop. I responded to the scene on March 2, 2018 as well as the scene of the second explosive device on March 12, 2018. I also responded to the scene on March 18, 2018. I am relying on my observations of the scenes as well as the facts and information gathered from other law enforcement described below. All facts are relayed in sum and substance.

4. As a result of my training, my experience relating to these statutes, and the experience of senior Special Agents and investigators, I believe that there is probable cause that evidence of the following offenses will be found in residence and vehicle, as well as the electronic devices found therein, listed in Attachment A:

> Title 26 United States Code § 5861: It is unlawful for any person to possess a firearm (defined as including a Destructive Device) that is required to be registered with the National Firearms Registration and Transfer Record and is not so registered or to transfer a firearm (including a Destructive Device) to a person to whom the firearm is not registered.

5. The applied-for warrant would authorize the search and seizure as described in Attachment B.

PROBABLE CAUSE

6. Your Affiant is familiar with the information contained in this affidavit, either through personal investigation or through reports and discussion with other law enforcement officers, who have participated in and have contributed their investigative efforts in this matter.

7. On March 2, 2018, at approximately 6:55 am, at 1112 Haverford Drive, Austin, Texas 78753 in the Western District of Texas, an explosion occurred on the front porch of the single story brick residence, resulting in the death of Anthony S. House. Preliminary analysis of

the explosive device revealed that it utilized a [redacted] as part of the triggering mechanism.

8. On March 12, 2018 at approximately 6:44 am at 4806 Oldfort Hill Drive, Austin, Texas 78723 in the Western District of Texas, an explosion occurred inside the residence, resulting in the death of a 17-year old victim and injuries to an additional victim. Preliminary analysis of the explosive device revealed that it utilized a [redacted] as part of the triggering mechanism.

9. On March 12, 2018 at approximately 11:50 am at 6706 Galindo Street, Austin, Texas 78741 in the Western District of Texas, an explosion occurred outside of the residence, sending one person to the hospital with injuries. Based on communications from the victim, the package containing the explosive device may have had the address "6705 Galindo" written on it. Preliminary analysis of the explosive device revealed that it utilized a [redacted] as part of the triggering mechanism.

10. On March 18, 2018, sometime before 9:00 pm, an explosion occurred near the block of 4800 Dawn Song Drive and 4721 Eagle Feather Drive, located in the neighborhood of Travis Country, Travis County, Texas—a location within the Western District of Texas. Two individuals were injured. A witness was interviewed who resided in the area of the explosion. [redacted] stated that when [redacted] returned to her home at approximately 8:25 pm [redacted] saw a "Drive Like Your Kids Live Here" yard sign with red backing and white letters that had not been present when [redacted] left her home. Preliminary analysis of the explosive device revealed that it utilized a [redacted] as part of the triggering mechanism. I believe, based on interviews with the witness and the preliminary analysis of the scene, that the sign was utilized to facilitate the concealment of the explosive device.

11. On March 20, 2018, at approximately 12:45 am, at the FedEx processing center in

Schertz, Texas, a package in FedEx custody exploded. At approximately 7:00 am on March 20, 2018, a package was located at the FedEx facility located near the Austin, Texas airport at 4117 McKinney Falls Pkwy. The package was addressed to [redacted] located in Austin, Texas. That package was x-rayed and an explosive device was found inside. Law enforcement was able to render the device safe. Preliminary analysis of the device revealed that it consisted of a PVC pipe casing with a metal pipe inside surrounded by shrapnel. The device utilized a [redacted] trigger. The trigger was designed to ignite the device creating an explosion when a flap of the package was opened.

12. Information from FedEx revealed that both packages discovered on March 20, 2018 were sent by the same individual at a FedEx location in Austin, Texas on Brodie Ln on March 18, 2018. Video footage was recovered from the FedEx and revealed that a single white male individual shipped both packages. He was wearing gloves and a hat in the store. He paid in cash. It appeared that he was wearing a wig. The FedEx clerk was interviewed by law enforcement who dealt with the customer who sent the packages. The clerk stated that the customer was in his mid 20s, wearing gloves, pasty white complexion, wearing a green shirt and blue jeans, wearing a hat and a wig. When the customer left, the clerk saw him get into a red truck. The clerk was shown a stock photograph of a 2002 red Ford pickup truck and the clerk said it was consistent with the vehicle that the customer got into. A [redacted] store in the same shopping center as the FedEx had exterior cameras that showed a red pickup truck with extended cab similar in appearance to a Ford Ranger in the parking lot approximately 10 minutes prior to the time the customer was in the FedEx.

13. The investigation is continuing for all of these incidents and this information continues to develop as the investigation continues, but law enforcement believes these

explosions were likely caused by Destructive Devices. Law enforcement has assessed that the explosive devices shared commonalities, such as the delivery method, contents of the explosive device, and the manner of detonation. All six explosive devices used shrapnel. Law enforcement believes all six devices are linked.

14. Multiple other individuals were investigated for potential links to these Destructive Devices. None of those persons were deemed likely to be involved. Our investigation is ongoing.

15. On or about February 27, 2018, a customer purchased several items at Frye's Electronics store located at 12707 N MOPAC Expressway, Austin, TX 78727. The items included [redacted] 4xAA Battery Holder With Snap Connector. Preliminary analysis of the explosive devices revealed that all six explosive devices utilized a [redacted] 4xAA Battery Holder With Snap Connector. The customer utilized a U.S. Bank credit card issued to Mark Conditt, who according to Texas Department of Public Safety driver's license records, resides at 403 2nd Street N, Pflugerville, TX 78660. Conditt has a 2002 Red Ford Ranger with an extended cab registered to him. Video footage recovered from Frye's showed that the customer looked to be Mark Conditt.

16. On or about March 13, 2018, at approximately 6:30 pm a red truck arrived at a Home Depot in Round Rock, Texas. A white male walked into the store and purchased several signs, including a "Drive Like Your Kids Live Here" sign consistent with the sign the witness reported seeing related to the March 18, 2018 explosion. Also, the person purchased a 6 pack of work gloves consistent with the gloves seen in the FedEx video from March 18, 2018. The white male seen on Home Depot video footage is similar in appearance to a photograph I have viewed of Mark Conditt. That customer paid with cash.

17. A Confidential Source (CS1)[1] with multiple contacts with Mark Conditt was interviewed on March 20, 2018. CS1 was shown a single photo of Mark Conditt and [redacted] identified the photograph to be Mark Conditt. CS1 was then shown the Home Depot video footage from March 13, 2018, discussed in detail above. CS1 told law enforcement that the photograph looked like Mark Conditt when asked how confident he/she was, CS1 said he/she was "98%" confident that the customer in the Home Depot footage was Mark Conditt. CS1 was shown the [redacted] footage of the red pickup truck, discussed above, and told law enforcement that the truck looks like Conditt's truck. When asked how confident he/she was, CS1 replied "70%."

18. According to Facebook pages viewed by other agents, [redacted] "liked" the [redacted] Facebook page—the same [redacted] where the explosive device discussed above was addressed to.

19. Law enforcement took [redacted] photographs of 403 2nd Street N, Pflugerville, Texas on March 20, 2018. Law enforcement also conducted physical surveillance of the address. A red 2002 Ford Ranger pickup truck was observed at the home. The [redacted] footage revealed multiple items in the bed of the pickup truck. I have seen the [redacted] exterior camera footage of the red pickup truck and I believe that the items in the bed of the truck in that footage are consistent with the items captured in the [redacted] photographs of the truck at 403 2nd Street N, discussed above.

20. Information from social media revealed that Mark Conditt was utilizing a cellular telephone with number [redacted]. Records revealed that [redacted] is registered to Mark

[1] There is no criminal history for CS1.

Conditt's father. Cellular data for [redacted] showed that there was no call activity on the number during the following dates and times: March 12, 2018 from midnight until approximately 8:13 pm; on March 13, 2018, from 4:16 pm until March 14, 2018 at 9:06 am; on March 18, 2018 from 4:32 pm until March 19, 2018 at 8:41 am. Therefore, there is no currently available data placing the phone utilizing number [redacted] at either at the scene of the explosions or at Home Depot—nor is their data placing the phone utilizing number [redacted] at locations other than the scene of the explosions or Home Depot. Phone call records for [redacted] show that between March 12, 2018 and March 20, 2018 the phone utilizing number [redacted] made calls to a garage door company—preliminary analysis of the explosive devices revealed that wiring utilized in the device was consistent with wiring used on [redacted].

21. The Government has not found any information of a registered Destructive Device for any of the victims of these Destructive Devices or locations of the explosions, making the possession or transfer to them unlawful. ATF conducted a query on March 20, 2018 and confirmed that Mark Conditt does not have a registered Destructive Device in his name nor is one registered to his address; his possession of a Destructive Device would therefore be unlawful.

22. The address of Mark Conditt on his driver's license and vehicle registration differ between 402 N 2nd St and 402 2nd Street N. Investigators have determined that they are the same location.

23. In my training and experience and that of other experienced ATF agents with expertise in Destructive Device making and explosives, I know and have learned that Destructive Device manufacturers often research their targets using the internet and electronic means.

Destructive Device-makers often research methods of constructing Destructive Devices, as well as information related to motive for using explosives, using the internet and other electronic devices. Furthermore, I have learned that in this case there is some evidence that Mark Conditt has used the internet to look up the FedEx location where two of the devices were mailed from, as described above. Additionally, I know that electronic devices often contain records of location and that information would be relevant evidence in this case.

24. Based on my training and experience, I know that anyone who manufactures or deals in explosives must be licensed by ATF to do so, and that the storage of explosives in a residence or vehicle is in violation of licensing and storage requirements defined by law. Furthermore, I know that due to the volatile nature of explosive materials, their improper manufacture and storage poses an extreme danger to the individual/dealer, as well as nearby residents and their property. Finally, there have been numerous documented instances of similar clandestine unlawful explosive operations in buildings wherein there have been fatalities and substantial property damage.

25. Based on the above, I respectfully submit that there is probable cause to believe that contained on premises described in Attachment A is evidence related to violations of 26 U.S.C. §5861.

TECHNICAL TERMS

26. Based on my training and experience and discussions with other law enforcement, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication

through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is 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 computer 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.

g. 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.

h. Flash drive: A USB flash drive, also variously known as a thumb drive, pen drive, jump drive, disk key, disk on key, flash-drive, memory stick or USB memory, is a data storage device that includes flash memory with an integrated USB interface.

i. SD Card: An SD memory card, flash card or memory cartridge is an electronic flash memory data storage device used for storing digital information. These are commonly used in portable electronic devices, such as digital cameras, mobile phones, laptop computers, tablets, or other digital devices.

27. Based on my training, experience, discussions with other agents, and research, I know that the Devices at issue have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and digital storage device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device as well as location information.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

j. 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.

k. 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.

l. 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.

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

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

n. 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.

o. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

p. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

q. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic 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.

r. Further, in finding evidence of how a device 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.

s. I know that when an individual uses an electronic device to utilize fraudulently obtained PII or create access devices, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic

device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of any electronic devices seized consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks permission to search for evidence of Destructive Devices involved in an ongoing series of explosions, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the search of the Premises described in Attachment A and the contents of any electronic devices recovered therein, as described in Attachment B.

REQUEST FOR SEALING

34. 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 warrant is

relevant to an ongoing investigation into the suspects 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.

Respectfully submitted,

REYNALDO ALATORRE, JR.
Special Agent
ATF

Subscribed and sworn to before me
on March 20, 2018:

HON. MARK LANE
UNITED STATES MAGISTRATE JUDGE