*AFFIDAVIT

I, Raymond P. Martinez III, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since March 2009. I am currently assigned to the San Antonio Division and assigned to a squad that is responsible for the investigation of, among other things, Weapons of Mass Destruction. During my career as a SA, I have participated in numerous investigations involving computer-related offenses and assisted in the execution of search warrants involving computers, computer equipment, software, electronically stored information, and instrumentalities of fraud. I have received training from the FBI, both formal and informal, regarding Weapons of Mass Destruction. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with authority to execute federal search warrants.

2. I am familiar with the facts and circumstances described herein, and this affidavit is based upon the personal knowledge I have derived from my participation in this investigation, conclusions I have reached based upon my training and experience, my conversations with other federal and state law enforcement investigators with whom I have discussed this case, and what I believe to be reliable information obtained from the following sources: oral and written reports about this investigation and other investigations which I have received from federal agents and from state law enforcement agencies; law enforcement databases; public records; recorded telephone calls; and physical surveillance conducted by federal agents or local law enforcement agencies which has been reported to me either directly or indirectly.

3. Title 18, United States Code, 1038 makes it a crime for

> Whoever engages in any conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of chapter … 10,… shall be fined under this title or imprisoned not more than 5 years, or both

4. Title 18, United States Code, Section 175, contained in Chapter 10 of Title 18, makes it a crime for

> Whoever knowingly … transfers… any biological agent… for use as a weapon … or attempts, threatens, or conspires to do the same, shall be fined under this title or imprisoned for life or any term of years, or both.

II. PURPOSE OF AFFIDAVIT

5. This affidavit is made in support of:

a. an application for a warrant to search the residence located in San Antonio, TX, 78219 (the "SUBJECT PREMISE");

b. a criminal complaint against and arrest warrant for Christopher Charles Perez ("PEREZ") for a violation of 18 U.S.C. § 1038 (WMD False Information and Hoaxes); and

c. an application for a warrant to search digital devices in the physical possession of PEREZ or in areas within his immediate control at the time of his arrest (the "SUBJECT DEVICES").

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUBJECT PREMISE

7. The premises to be searched is located in San Antonio, Texas.

IV. SUBJECT DEVICES

8. The SUBJECT DEVICES to be searched are digital devices in the physical possession of PEREZ or in areas within his immediate control at the time of the execution of the arrest warrant.

V. SUMMARY OF PROBABLE CAUSE

9. The FBI is investigating PEREZ for his threat made online in which he claimed he paid someone to spread COVID-19 at a Grocery Stores in the San Antonio area. The investigation into PEREZ arose from an anonymous individual who viewed PEREZ's online post and reported it. PEREZ was located and confessed to creating the post in order to scare people.

VI. STATEMENT OF PROBABLE CAUSE

A. Online Post and Identification of SUBJCECT

10. On April 5, 2020 at approximately 00:21 CDT, an online tip was filed with the website www.tip411.com regarding a threat to contaminate and spread COVID-19. A screenshot of the post made by the Facebook moniker "Christopher Robbins" (PEREZ). The post stated "PSA!! Yo rt GROCERY STOREMERCADO!! My homeboys cousin has covid19 and has licked every thing for past 2 days cause we paid him too [4 EMOTICONS]…big difference is we told him not to be these fucking idiots who record and post online…YOU'VE BEEN WARNED!!! GROCERY STORE on nogalitos next ;)"

11. San Antonio Fusion Center Officer #0094 located the Facebook page for PEREZ. The original post had been removed at the time Officer #0094 viewed the page, however, a second post was made linking a news article to www.news4sanantonio.com referencing an article in which a store released a statement that an employee tested positive for COVID-19. The post contained a comment stating the following: "Lol..I did try to warn y'all but my homegirl changed my mind…mercado already is, nogalitos location next…."

12. Through intelligence gathered on SUBJECTS Facebook page and database checks, SUBJECT was identified as:

NAME: CHRISTOPHER CHARLES PEREZ

13. This information was then passed then passed to the FBI San Antonio Division for investigative actions.

B. Interview of the SUBJECT

14. PEREZ was located at the SUBJECT PREMISE and interviewed. PEREZ confirmed ownership of the Facebook account under the name "Christopher Robbins." PEREZ admitted to making a post on his Facebook page about someone intentionally spreading coronavirus, a.k.a. COVID-19, inside a Grocery store in San Antonio. PEREZ claimed it was "shit talking" and he was not aware of anyone actually spreading the virus in a Grocery Store. PEREZ stated he was not sick, none of his family were sick with coronavirus, and he did not know anyone with coronavirus. PEREZ said he "thought it was stupid for people to be out shopping and he was trying scare people from the stores in order to stop them from spreading the virus to keep people safe." PEREZ said too many people were still out shopping in the stores and he wanted them to take things more seriously and reduce the number of people in the stores. PEREZ intended "in a way" to stop people from going to GROCERY STORE so he could keep people from getting sick. PEREZ did not intend to cause a mass panic, but prevent the spread of coronavirus by keeping people at home because he believes people are out there intentionally spreading the virus. When asked if he was happy a GROCERY STOREclosed as a result of his threat, PEREZ stated he was "50/50."

15. PEREZ stated he only made one post and this post was on his page for a minute. He claimed he took down this post after another individual commented and told him to take it down because he could get into trouble. This statement was not true in that based on the information on the post, it was up for at least 16 minutes. PEREZ never mentioned his second post in the interview that threatened "mercado already is, nogalitos location next." Based on the information on contained the second post, this post was up for at least 23 hours.

16. PEREZ stated he lost his job as a result of the shelter in place orders.

C. Victim's Response

17. I interviewed VICTIM's Vice President of Loss Prevention, Darrell Taylor ("TAYLOR"). TAYLOR stated after he was made aware of the threat, he notified VICTIM's Vice President of Risk Management Abel Martinez. The grocery store took these threats seriously, however, they were awaiting confirmation on the validity of the threat as well as what stores may have been affected to initiate their planned response. Taylor stated no stores were closed as they were unaware of what store or stores would have been affected by the threat. Also, they did not know the date and time the possible contamination would have occurred. Taylor stated if the grocery stores would have started to close for these threats, it could have caused a panic response by the public in the current state due to the COVID-19 pandemic.

18. Based on PEREZ's two posted threats, I believe there is probable cause to believe he engaged conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of 18 U.S.C. 175, that is conspiring to weapondize a biological agent, that is coronavirus a.k.a. COVID-19.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

19. From my experience, I know processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and

that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons. 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).

20. *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."

22. *Forensic evidence.* 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.

23. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

a. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

b. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive 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 digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and

innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

24. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I know from my training and experience and my review of publicly available materials that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor or, facial recognition. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device. In my training and experience, users of devices with a fingerprint sensor feature often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security. Likewise, some devices can be unlocked through the use of facial recognition software. If the device recognizes the preprogrammed face, the device will unlock. In my training and experience, users of devices with facial recognition software features often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

25. In some circumstances, fingerprint sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple's Touch ID feature, these circumstances include: (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; and (3) five unsuccessful attempts to unlock the device via Touch ID are made. Other brands have similar restrictions. I do not know the passcodes of the devices likely to be found at the SUBJECT PREMISE or the SUBJECT DEVICES. Likewise, Apple and other manufacturers who also use facial recognition software set similar limits to unlock a device.

26. For these reasons, while executing the warrant, agents will likely need to use the fingerprints or thumbprints of any user(s) of any fingerprint sensor-enabled device(s) to attempt to gain access to that device while executing the search warrant. Additionally, if the device is enabled to unlock the device, agents will need to hold the device in front of any and all user's faces. The warrant seeks the authority to compel the use of the fingerprint and/or thumbprint and/or face of: (a) every person who is located at the SUBJECT PREMISE during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint and/or facial recognition sensor-enabled device that is located at the SUBJECT PREMISE and falls within the scope of the warrant; and (b) PEREZ with respect to the SUBJECT DEVICES. The government may not be able to obtain the contents of the devices if those fingerprints are not used to access the devices by depressing them against the fingerprint sensor at the time of the search. Although I do not know which of the fingers are authorized to access on any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password, for which passcode or password the government does not seek to compel.

VIII. ITEMS TO BE SEIZED

27. Based on the foregoing, I respectfully submit that there is probable cause to believe that the items which constitute evidence of violations of the Subject Offenses, will be found at the SUBJECT PREMISE, and that the items which constitute evidence of violations of the Subject Offenses, will be found in the SUBJECT DEVICES.

IX. CONCLUSION

28. For all the reasons described above, there is probable cause to believe that: (a) evidence of violations of the Subject Offenses, this affidavit, will be found in a search of the SUBJECT PREMISE and the SUBJECT DEVICES, respectively, (b) PEREZ has committed a violation of 18 U.S.C. § 1038 (Hoaxes Involving Biological Agents).

REQUEST FOR SEALING

29. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court.

These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Raymond P. Martinez III, Special Agent
Federal Bureau of Investigation

Subscribed and sworn telephonically and signed electronically on the 7th day of April, 2020

HONORABLE RICHARD B. FARRER
UNITED STATES MAGISTRATE JUDGE