

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND SEARCH WARRANT**

I, TERRENCE DUPONT, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since April 2013. I am currently assigned to the Economic Crimes squad with the Boston Division of the FBI. Prior to this assignment, I spent two years on the Health Care Fraud squad and four and a half years on the Philadelphia Division’s Public Corruption squad. During my time in the FBI, I have participated in investigations relating to mail and wire fraud, money laundering, and aggravated identity theft. I have also been the affiant on numerous complaint and search warrant applications.

2. I am currently investigating WEMERSON DUTRA AGUIAR for various federal crimes, including mail fraud, wire fraud, and conspiracy to commit those crimes, in violation of Title 18, United States Code, Sections 1341, 1343 and 1349, respectively; aggravated identity theft, in violation of Title 18, United States Code, Section 1028A; and money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957 (collectively, the “TARGET OFFENSES”).

3. I make this affidavit in support of a criminal complaint charging WEMERSON DUTRA AGUIAR with conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349. As set forth below, I have probable cause to believe that AGUIAR conspired with others known and unknown: (1) to open driver accounts with various rideshare and delivery service companies using stolen identities and/or falsified documents and (2) to make money by renting or selling those fraudulent accounts to individual drivers who might not otherwise qualify to drive for those services, and by exploiting referral bonus programs offered by the companies.

4. I also make this affidavit in support of an application for a search warrant for the carry-on bag located in AGUIAR's possession when special agents from the FBI arrested AGUIAR on May 5, 2021 (the "Premises"), including but not limited to the mobile phone assigned number 857-231-3814, used by AGUIAR, for which Sprint is the service provider (the "AGUIAR TELEPHONE") and laptop located in the Premises, as described in Attachment A, because there is probable cause to believe that it contains the fruits, evidence, and instrumentalities of the TARGET OFFENSES, as described in Attachment B.

5. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents and witnesses, and my review of documents—including bank records, text messages and "chats" between the defendant and his co-conspirators, and other materials obtained through legal process and Court-authorized search warrants. This affidavit is intended to show simply that there is sufficient probable cause for the requested complaints and does not set forth all of my knowledge about this matter.

**PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED**

**Overview of the Conspiracy**

6. Beginning by at least 2019 and continuing through at least April 2021, in the District of Massachusetts and elsewhere, AGUIAR conspired with others known and unknown to create fraudulent driver accounts with multiple rideshare and delivery companies (the "Rideshare/Delivery Companies"), and to rent or sell the accounts to individuals who might not otherwise qualify to drive for those services. The evidence I have reviewed indicates that the scheme included the following:

- a. Obtaining images of victims' driver's licenses, or the information on victims' driver's licenses, and Social Security Numbers, from various sources including the DarkNet<sup>1</sup>;
- b. Creating accounts to drive for the Rideshare/Delivery Companies using those stolen identifiers;
- c. Renting or selling those accounts, including to people who might not otherwise qualify to drive for the Rideshare/Delivery Companies;
- d. Coordinating on prices charged to rent and sell accounts so as not to undercut each other's business;
- e. Sharing tips on how to circumvent the Rideshare/Delivery Companies' fraud detection systems;
- f. Causing the Rideshare/Delivery Companies to generate Internal Revenue Service Forms 1099 in the names of identity theft victims for income they never earned from the Rideshare/Delivery Companies, and attempting to divert those Forms 1099 from being sent to the victims;
- g. Using driver accounts for the purpose of referring other drivers to the Rideshare/Delivery Companies, and then collecting referral bonuses from the companies for additional fake accounts that the conspirators created;

---

<sup>1</sup> The DarkNet is part of the Internet that is not indexed and consists of overlaying networks that use the public Internet but require unique software, configuration, or authorization to access, which is predominately designed to hide the identity of the user. Payment for goods and services on the DarkNet is usually through virtual currency like bitcoin, which is also designed to be anonymous.

h. Utilizing global positioning system (“GPS”) “spoofing” applications to “cut the line” for rides or deliveries, or to make it appear that trips were longer than they actually were, in order to obtain increased fares from the Rideshare/Delivery Companies, and selling this technology to clients.

7. To date, investigators have identified more than 2,000 individuals whose identities were stolen and used as part of the scheme.

### **Background on the Rideshare/Delivery Companies**

8. Rideshare Company A is a ride-hailing company that connects drivers with riders via a mobile phone application (“app”). To become a driver for Rideshare Company A in Massachusetts, applicants must be at least 21 years old, have at least one year of driving history (three years if under age 23), and pass a motor vehicle and criminal background check. Drivers apply through Rideshare Company A’s app or its website and provide, among other things, their name, date of birth, Social Security number, an image of their driver’s license, automobile registration and insurance information, and a profile photo. Drivers must also pass a separate background check run by the Massachusetts Department of Public Utilities (“DPU”). Rideshare Company A stores the information applicants enter on servers which are located outside the District of Massachusetts.

9. Delivery Company B is an online food ordering and delivery service. To become a driver for Delivery Company B in Massachusetts, drivers applying to deliver via automobile must be at least 18 years old, have at least one year of driving history, and pass a motor vehicle and criminal background check.<sup>2</sup> Drivers apply through Delivery Company B’s app or its website

---

<sup>2</sup> Some of the Delivery Companies allow drivers to deliver via bicycle or on foot in certain locations.

and provide, among other things, their name, date of birth, Social Security number, and profile photo. Drivers applying to deliver via automobile must also provide an image of their driver's license. Delivery Company B stores the information applicants enter on servers which are located outside the District of Massachusetts.

10. Rideshare Company C is a ride-hailing company that connects drivers with riders via a mobile phone app. To become a driver for Rideshare Company C in Massachusetts, applicants must be at least 25 years old, possess a valid driver's license, Social Security number, and vehicle insurance, have at least one year of driving history, and pass a motor vehicle and criminal background check. Drivers apply through Rideshare Company C's app or its website and provide, among other things, their name, date of birth, Social Security number, an image of their driver's license, their automobile insurance information, and a photo of themselves ("selfie"). Drivers must also pass a separate background check run by the DPU. Rideshare Company C stores the information applicants enter on servers located outside the District of Massachusetts and operated by Amazon Web Services.

11. Delivery Company D is an online food ordering and delivery platform. To become a driver for Delivery Company D in Massachusetts, drivers applying to deliver via automobile must be at least 18 years old, have a valid Social Security number, and pass a motor vehicle and criminal background check. Drivers apply through Delivery Company D's website and provide, among other things, their name, date of birth, and Social Security number. Drivers applying to deliver via automobile must also provide their driver's license number (but not an image of their license). Delivery Company D stores the information applicants enter on servers located outside the District of Massachusetts and operated by Amazon Web Services.

12. Delivery Company E is an online grocery delivery and pick-up service platform. To become a driver for Delivery Company E in Massachusetts, drivers must be at least 18 years old and pass a motor vehicle and criminal background check. Drivers apply through Delivery Company E's website and provide, among other things, their name, date of birth, Social Security number, image of their driver's license, and a "selfie" photo. Delivery Company E stores the information applicants enter on servers located outside the District of Massachusetts and operated by Amazon Web Services.

13. When a driver account is opened, the Rideshare/Delivery Companies generally collect metadata concerning, among other things, the device used to open the account, its location, the IP address used to submit the applicant's information, and whether the account was referred by another driver.

14. Each of the Rideshare/Delivery Companies uses a third-party company to complete the motor vehicle and criminal background check on driver applicants. This company runs the motor vehicle and criminal background check based on the name, date of birth, and Social Security number provided by the driver applicant.

15. The DPU also completes a two-part background check for rideshare drivers in Massachusetts. The DPU runs its background check based on the name, date of birth, driver's license number, and last six digits of the Social Security number provided to Rideshare Company A and Rideshare Company C by the driver applicant. The DPU completes follow-up background checks on all Rideshare Company A and Rideshare Company B drivers in Massachusetts every six months based on this same information.

16. None of the Rideshare/Delivery Companies requires that the vehicles used for rides or deliveries be registered to the driver. It is not uncommon for drivers to use a vehicle registered to someone else.

17. The Rideshare/Delivery Companies occasionally offer referral bonuses depending on market conditions. To earn a referral bonus, existing drivers who are in good standing can refer another person to become a driver for the company. Once the referred driver completes a set number of trips, which varies by company and market, the referring driver (and, at some companies, the referred driver) can earn a bonus. The amount of the bonus depends on the company and the market and can be greater than \$1,000.

18. One way that the Rideshare/Delivery Companies pay their drivers is via direct deposit.<sup>3</sup> Payments generally, but not always, appear on bank statements with the name of the driver who purportedly completed the trip or delivery.

**WEMERSON DUTRA AGUIAR**

19. The investigation has revealed that, as part of the scheme, AGUIAR rented and sold fraudulent driver accounts; prepared and submitted driver applications using fraudulent identifiers; rented his own vehicles to drivers to use while driving under fraudulent accounts; purchased and traded driver's licenses and Social Security numbers; and exchanged information with other co-conspirators on how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

20. For example, on or about November 23, 2019, a driver account in the name of Victim 1 ("Account 1") was created with Rideshare Company A using an Apple iPhone, on the Sprint mobile network, from a location having latitude 42.4742431640625 and longitude

---

<sup>3</sup> Some of the companies also offer a debit card option for payment.

-70.95612752697879, which is in the vicinity of an apartment complex at 196 Locust Street in Lynn, Massachusetts. The account appears to have been set up using Victim 1's name, Social Security number, and driver's license, but the photo on the driver's license was of another individual, Co-Conspirator 1 ("CC-1"). The vehicle associated with Account 1 in Rideshare Company A's system was registered in the name of CC-1, and the bank account linked to Account 1 was a Bank of America account in the name of CC-1. Between December 7, 2019 and December 18, 2019, 38 trips were completed using Victim 1's identity before Rideshare Company A closed Account 1 for suspected fraud.

21. Metadata associated with the Apple iPhone used to create Account 1 matches metadata linked to (a) an Apple iCloud account with Apple ID "[REDACTED]@icloud.org" (the "AGUIAR iCloud Account"), which is registered to AGUIAR at 196 Locust Street, Apt. 207, Lynn, Massachusetts, and (b) the AGUIAR TELEPHONE, which is registered to a subscriber whose last name matches the last name of AGUIAR'S then-domestic partner and is associated with AGUIAR'S iCloud Account and with a Zelle account used by AGUIAR.<sup>4</sup> Based on my investigation, I am aware that until February 2021, AGUIAR resided at the Locust Street address. In addition, Rideshare Company A's records reflect a rider account in AGUIAR's own name that had pick-ups at or near 196 Locust Street.

22. I have reviewed the AGUIAR iCloud Account pursuant to a Court-authorized search warrant. Among other items, I located an image of Victim 1's driver's license, altered to reflect CC-1's picture—the same image that was submitted to Rideshare Company A in connection

---

<sup>4</sup> Zelle is a digital payment network owned by a group of banks, including Bank of America and Wells Fargo, among others. Zelle allows users to send and receive money, typically over a mobile device, directly from their bank accounts at participating banks.



with Account 1. I have also reviewed WhatsApp chats between AGUIAR and CC-1 discussing Account 1, which appears to have been created after Rideshare Company B suspended a driver account in the name of another victim that CC-1 was using.<sup>5</sup>

23. Location data Rideshare Company A collected indicates that multiple other suspected fraudulent accounts were likewise created in the vicinity of 196 Locust Street, and metadata from Rideshare Company A's records reflect that the individual or individuals who set up Account 1 were also associated with hundreds of other driver accounts.

24. AGUIAR's picture appears to be "Photoshopped" onto the driver's licenses of at least three different fraudulent driver accounts with Rideshare Company A that were created in the vicinity of 196 Locust Street. In total, investigators have identified at least nine driver accounts, in different names, with AGUIAR's picture on the driver's license (the "AGUIAR Accounts"). The vehicle associated with each of these Accounts is registered to AGUIAR.<sup>6</sup> In total, Rideshare Company A identified more than 180 other driver accounts linked to the same device that created Account 1 and the AGUIAR Accounts.

25. Based on my investigation, including review of summary draft translations of WhatsApp chats between AGUIAR and others, I am aware that AGUIAR was not driving under

---

<sup>5</sup> WhatsApp is a text messaging application that provides users with end-to-end encryption, which means that a WhatsApp message is visible only to the sender and receiver of the message. WhatsApp also allows users to send and receive voice recordings. WhatsApp users typically use their phone number as their WhatsApp account number to send and receive messages through the application.

<sup>6</sup> Based on my investigation, I am aware that AGUIAR does not have a valid Massachusetts driver's license. However, in Massachusetts, residents are allowed to register vehicles without a driver's license.

each of the AGUIAR accounts, but rather was renting some of the accounts to other drivers, including CC-1.<sup>7</sup>

26. For example, AGUIAR was a member of several WhatsApp chat groups targeted to Brazilian nationals residing in Massachusetts. AGUIAR regularly posted in these chats that he had rideshare and delivery accounts for sale or rent. For example, on or about April 20, 2020, AGUIAR posted a message in a chat with hundreds of other members advertising male and female accounts with Delivery Company D for a “good price.” AGUIAR posted a similar message on or about September 24, 2020.

27. In addition to the aforementioned chats, the records from the AGUIAR iCloud Account obtained pursuant to a Court-authorized search warrant include hundreds of WhatsApp chats, all in Portuguese, in which AGUIAR corresponded with individuals seeking to rent or buy driver accounts. As detailed further herein, the AGUIAR iCloud Account also included WhatsApp messages with co-conspirators discussing the creation of driver accounts and ways to secure such accounts by circumventing fraud prevention controls imposed by the Rideshare/Delivery Companies. Further, the iCloud Account contained thousands of images of driver’s licenses, as well as lists of names and Social Security Numbers.

28. In reviewing the hundreds of suspected fraudulent accounts associated with Account 1 and the AGUIAR Accounts, investigators discovered that many of the driver’s license images are stock photos that were altered to insert different license images. For example, many of the photos show the altered driver’s license resting on a wallet. It appears that the same

---

<sup>7</sup> Many of the WhatsApp communications I have reviewed were summaries of draft translations of messages written in Portuguese.

background image was used in each of the photos, and the images were edited to make it appear as though different driver's licenses were resting on the wallet. Rideshare Company A identified more than 30 driver accounts that appear to use the identical image of a driver's license resting on a wallet, but with different driver's licenses inserted into the image. Some of these accounts were linked to AGUIAR because the device used to open the account had the same device identifiers as Account 1 and the AGUIAR accounts.

29. Based on my review of draft summary translations of WhatsApp chats between AGUIAR and various co-conspirators, I have learned that the conspirators had templates of various states' driver's licenses, in which they edited victims' information and customers' photos. For example, on or about October 22, 2019, Co-Conspirator 2 ("CC-2") told AGUIAR via WhatsApp that he had obtained more than 50 driver's licenses, and shared a photo of a printout containing victims' names, dates of birth, addresses, and driver's license numbers, but without the images of any licenses.

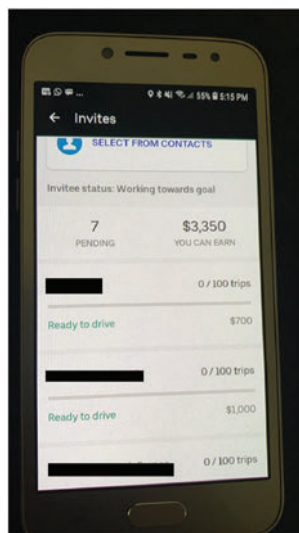
30. I reviewed additional WhatsApp text and voice messages in which AGUIAR and CC-2 discussed driver applications for the Rideshare/Delivery Companies in the names of other people, as well as payments, including referral bonuses, and ways to launder money. The messages, which are in Portuguese, began in or about October 2019 and include images of driver's licenses, as well as screen shots and video captures of AGUIAR's and CC-2's computers and phones.

31. For example, in or about October 2019, CC-2 sent AGUIAR messages indicating, in substance, that he wished to find someone new to make driver's license alterations and discussed options with CC-2.

32. In other chats, CC-2 and AGUIAR sought to troubleshoot issues raised by drivers who had been asked for further identification by the Rideshare/Delivery Companies and/or whose accounts had been suspended or closed. In one set of chats, on or about October 17, 2019, AGUIAR sent CC-2 a photograph showing that a driver had been asked for a Social Security number while attempting to log into the app. CC-2 replied to AGUIAR with a photograph identifying a Social Security number. Other chats concerned account closings, which AGUIAR and CC-2 speculated were attributable to their use of fraudulent documents.

33. In another set of chats in October 2019, AGUIAR asked CC-2 to alter the insurance policy document for Co-Conspirator 3 (“CC-3”) on an account so that it listed a different vehicle. CC-2 responded with an image of an insurance policy document listing the other vehicle.

34. AGUIAR also discussed referral bonuses with CC-2. For example, in a chat between AGUIAR and CC-2 on or about October 15, 2019, CC-2 sent AGUIAR a photo of his phone showing the status of potential referral bonuses. The image below, from which victims’ names have been redacted, shows that CC-2 had seven referred accounts pending, the number of trips each referred driver needed to complete in order to secure the referral bonus, and the amount of the bonus to be earned:



35. AGUIAR also discussed account creation with CC-2 in WhatsApp chats. For example, on or about April 23, 2020, AGUIAR sent CC-2 a photograph of a man (“Subject 1”) in front of a white background. Approximately 21 hours later, AGUIAR sent CC-2 a photo of a hand holding a driver’s license bearing the name and photograph of Victim 2. Approximately 13 minutes later, CC-2 sent AGUIAR a photograph of his computer screen that appears to be opened to Adobe Photoshop and shows the same image of Victim 2’s driver’s license, but now bearing the photo of Subject 1.

36. In my review of the AGUIAR iCloud account, I found other, similar exchanges between AGUIAR and CC-2 involving manipulated identity documents. In other instances, CC-2 sent AGUIAR screen shots of his computer in which he appears to be browsing DarkNet sites to purchase identification cards. For example, on or about November 8, 2019, CC-2 sent AGUIAR the following photo of his computer screen, which appears to depict a DarkNet site selling passports, visas, and other forms of identification:



37. In another instance, on or about August 4, 2020, CC-2 sent AGUIAR a screen shot of what appears to be the photo gallery on his phone, in which a number of driver's license images are visible. I have likewise found thousands of photos of victims' driver's licenses saved in the AGUIAR iCloud Account.

38. During my review of the AGUIAR iCloud Account, I also found images CC-2 sent to AGUIAR of CC-2's computer screen opened to his Hotmail email account. The images depict emails from Delivery Company E and the background check company. The emails reference applications to drive for Delivery Company E and pending background checks on individuals other than CC-2. Other images depict emails with attachments that are pictures of the front and back of driver's licenses and passport-type photos. Other images contain what appear to be Social Security numbers.

39. I have reviewed a bank account in AGUIAR's name at Bank of America. The address associated with the account is [REDACTED] Locust Street, Apt. 207, Lynn, Massachusetts. Between on or about June 27, 2019 and on or about February 26, 2020, approximately \$150,000 was deposited into AGUIAR's Bank of America account. Zelle transfers accounted for approximately \$100,000 of that amount, and payments from Rideshare Company A and Rideshare Company B for completed rides accounted for approximately \$37,000. I have also reviewed an account in AGUIAR's name at Wells Fargo bank that received deposits totaling approximately \$14,000, during the same period, principally comprising Zelle transfers and deposits from Rideshare Company A and Rideshare Company B.

40. I have also reviewed statements of a Zelle account linked to the AGUIAR TELEPHONE and the AGUIAR iCloud Account for the period between approximately July 2019

and July 2020. The account statements reflect the same transfers listed in AGUIAR's bank statements from Bank of America and Wells Fargo.

41. Between approximately July 2019 and July 2020, AGUIAR received approximately \$169,512 in Zelle transfers. AGUIAR received recurring Zelle transfers from over 100 individuals, typically in amounts between \$200 to \$350. Based on my knowledge of this investigation, I believe that many of these transfers were from individuals renting or buying fraudulent driver accounts. For example, the records indicate that CC-1 paid AGUIAR approximately \$250 per week between on or about October 15, 2019 and on or about February 3, 2020.

42. I have reviewed bank records reflecting that, between approximately June 2019 and September 2020, CC-2 received deposits into his Bank of America account totaling approximately \$216,151, primarily comprising approximately \$137,158 in Zelle transfers and approximately \$16,232 in payments from Delivery Company D and from a third-party payment processor for a number of Rideshare/Delivery Companies. The payments from Delivery Company D referenced the names of 13 different individuals.<sup>8</sup> CC-2 received Zelle transfers from more than 95 different names, including approximately \$40,763 from AGUIAR.

**THE PREMISES CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES**

43. I also have probable cause to believe that the Premises contains fruits, evidence, and instrumentalities of violations of the TARGET OFFENSES, as described in Attachment B.

---

<sup>8</sup> Of the approximately \$12,482 in deposits from Delivery Company D in CC-2's account, none appeared to be in CC-2's name, although deposits totaling approximately \$1,694 were not tied to any driver name.

44. On or about May 5, 2021, AGUIAR boarded United Airlines Flight #1246 from Boston Logan Airport to Chicago O'Hare Airport. From there, AGUIAR had a connecting flight, United Airlines Flight #1656, to Cancun, Mexico. I am familiar with a WhatsApp chat on or about November 7, 2019 between AGUIAR and CC-2, in which AGUIAR explained that he intended to leave the United States through Mexico to return to Brazil so as not to have a record of his exit given that he had overstayed his visa.

45. When he was arrested, AGUIAR had in his possession a carry-on bag containing a cell phone and laptop.

46. 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 email, 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.

47. 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 that reveals or suggests who possessed or used the device.



48. Here, AGUIAR communicated with co-conspirators via WhatsApp and used his phone to create driver accounts with the Rideshare/Delivery Companies.

49. 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:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

50. 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 inculcating 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 crimes 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 inculcate 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).

51. 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.

52. 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.

53. 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.

54. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that 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 that storage media such as hard disks, flash drives, CDs, and DVDs can store is 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 onsite.

b. Technical requirements 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.”

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

55. The Premises may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

56. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) AGUIAR. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

57. This warrant authorizes a review of electronically stored information, communications, other records, and information seized, copied or disclosed pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a

complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**UNLOCKING A DEVICE USING BIOMETRIC FEATURES**

58. 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.

59. 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 five 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.

60. The passcode that would unlock device(s) found during the search of the Subject Premises is not currently known to law enforcement. Thus, it may be useful to press the finger(s) of the user(s) of the device(s) to the device's fingerprint sensor or to hold the device up to the face of the owner 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.

61. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it may be necessary for law enforcement to have the ability to require any occupant of the Subject Premises to press their finger(s) against the sensor of the locked device(s) or place the devices in front of their faces in order to attempt to identify the device's user(s) and unlock the device(s).

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

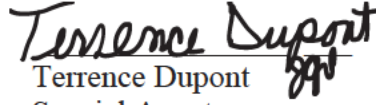


**CONCLUSION**

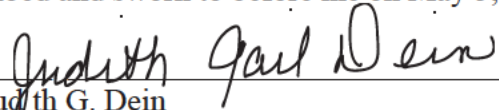
63. Based on my knowledge, training, and experience, and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that AGUIAR conspired to commit wire fraud, in violation of 18 U.S.C. § 1349.

64. Based on my training and experience and the facts set forth above, I believe there is also probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the premises described in Attachment A.

Sworn to under the pains and penalties of perjury,

  
Terrence Dupont  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on May 5, 2021 by telephone

  
\_\_\_\_\_  
Hon. Judith G. Dein  
United States Magistrate Judge