

CCC/WK:CMM/MGD
F. #2018R02024

19

681M

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

TO BE FILED UNDER SEAL

- against -

19-M-

MATHEW JAMES,

COMPLAINT AND AFFIDAVIT IN
SUPPORT OF APPLICATION FOR
ARREST AND SEARCH WARRANTS

Defendant.

----- X

(T. 18, U.S.C., §§1028A, 1343 and 1349)

IN THE MATTER OF AN
APPLICATION OF THE UNITED
STATES OF AMERICA FOR A
SEARCH WARRANT FOR (1) THE
PREMISES KNOWN AND
DESCRIBED AS 24 FORSYTHE
DRIVE, EAST NORTHPORT, NEW
YORK 11731 AND ALL LOCKED
AND CLOSED CONTAINERS
THEREIN, AND (2) ANY AND ALL
ELECTRONIC DEVICES LOCATED
AT THE PREMISES OF 24
FORSYTHE DRIVE, EAST
NORTHPORT, NEW YORK 11731

----- X

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR ARREST AND SEARCH WARRANTS**

I, WILLIAM SENA, being duly sworn, depose and state that I am a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

Upon information and belief, in or about and between July 2015 and the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant MATHEW JAMES, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds.

(Title 18, United States Code, Section 1349)

Upon information and belief, in or about and between July 2015 and the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant MATHEW JAMES, together with others, did knowingly and intentionally devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, transmitted and cause to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds.

(Title 18, United States Code, Section 1343)

Upon information and belief, in or about and between July 2015 and the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant MATHEW JAMES, together with others, during and in relation to the crimes charged above, did knowingly and intentionally transfer, possess and use, without

lawful authority, a means of identification of another person, specifically, personally identifiable healthcare information during and in relation to the commission of wire fraud, without lawful authority.

(Title 18, United States Code, Section 1028A)

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for an arrest warrant for the defendant MATHEW JAMES and for search warrants for (a) the premises known and described as 24 Forsythe Drive, East Northport, New York 11731 (the “SUBJECT PREMISES”), and (b) any and all electronic devices located at the SUBJECT PREMISES, including but not limited to computers, tablets, iPads, and cellular telephones (the “SUBJECT DEVICES”). The information to be searched is described in the following paragraphs and in Attachments A and B.

2. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) for approximately three years and am currently assigned to the white-collar crime squad of the Long Island Office of the FBI. In that capacity, I have participated in numerous investigations of criminal activity involving, among other things, health care, wire and mail fraud and identity theft, as well as other types of white-collar criminal schemes. During the course of these investigations, I have conducted or participated in surveillance, undercover transactions, the execution of search warrants, debriefings of informants, and reviews of taped conversations, and financial and phone records. In addition, as a result of my training and experience, I am familiar with techniques and methods of operation used by individuals

involved in criminal activity to facilitate various kinds of fraud and to conceal their activities from detection by law enforcement authorities.

3. I am familiar with the information contained in this Affidavit based on my own personal participation in the investigation described herein, as well as my review of documents, my training and experience, and my discussions with other law enforcement personnel and witnesses. Additionally, any statements in this Affidavit that are attributed to an individual are set forth in sum and substance and in part. This Affidavit is intended to show merely that there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the crimes of wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A (collectively, the "SUBJECT OFFENSES") have been committed, are being committed, and will be committed by the defendant MATHEW JAMES and others, and to conclude that a search of the SUBJECT PREMISES, SUBJECT DEVICES and the information described in Attachment A will yield evidence of these crimes and instrumentalities, contraband and/or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

I. **Background**

5. The defendant MATHEW JAMES owns and operates various corporations, including, but not limited to, Leale Inc., Leale Billing Corp., Remm Consultants, Inc., and Elite Industrial Ltd. (collectively, the “Leale Entities” or the “Billing Companies”). The New York State (“NYS”) Department of State (“DOS”), Division of Corporations, database indicates that Leale Inc. was incorporated in July 2006 and that JAMES is the Chief Executive Officer (“CEO”); that Leale Billing Corp. was incorporated in July 2014 and that Remm Consultants, Inc. was incorporated in August 2018. NYS Department of Labor (“DOL”) records indicate that Leale Inc. and Leale Billing Corp. are medical billing companies; that Elite Industrial Ltd. is a “billing” company providing “scientific/professional and technical services” that commenced operations in January 2018¹; and that JAMES is the owner and President of Leale Billing Corp. and Elite Industrial Ltd. In addition, bank records indicate that Remm Consultants, Inc. is a medical billing company. DOS and DOL records indicate that the SUBJECT PREMISES are listed as the address for each of the Leale Entities, and this investigation has revealed that JAMES primarily operates the Leale Entities out of the SUBJECT PREMISES. A form filed with the DOL on or about December 21, 2017 indicates that Elite Industrial Ltd. had eight employees.

¹ On information and belief, Elite Industrial Ltd. is also a medical billing company.

6. This investigation has revealed that the defendant MATHEW JAMES and others have engaged in a scheme to defraud various insurance companies, including, but not limited to Aetna, Inc., Aetna Life Insurance Co., Cigna Corp., and UnitedHealth Group d/b/a UnitedHealth Care and Optum (each an “Insurance Company” and, collectively, “the Insurance Companies”), using, among other things, fraudulent billing practices.

II. The SUBJECT PREMISES and the SUBJECT DEVICES

7. The SUBJECT PREMISES is a one-story residential home, with a basement, located at 24 Forsythe Drive, East Northport, New York. The house is white with a red brick front. There is a single-car garage attached to the house on the left (when facing the house). There is a front door to the right of the garage, and there are glass pane windows by the front door. There is a mailbox at the street line in front of the house with the number “24” on it. The SUBJECT PREMISES sits on a corner lot at the corner of Forsythe Drive and Adrian Street. A photograph of the Subject Premises is attached as part of Exhibit A.

8. The SUBJECT DEVICES include at least one cellular telephone, bearing telephone number (631) 827-8159 (the “SUBJECT PHONE”). Records from AT&T Wireless indicate that the subscriber for the SUBJECT PHONE is the defendant MATHEW JAMES, and the address associated with the account is the SUBJECT PREMISES.

9. The SUBJECT DEVICES also include computers, tablets, iPads, cellular telephones, and any and all removable data storage media (e.g., compact discs, digital video discs, memory cards, memory sticks, zip discs, magnetic tapes, thumb or flash drives, or other external/dockable peripheral that can be easily removed from a computer system and which also contain removal medial capabilities) located in the SUBJECT PREMISES. As discussed

in more detail below, there is probable cause to believe that the defendant MATHEW JAMES used electronic devices in the SUBJECT PREMISES in furtherance of the fraud scheme.

III. Probable Cause

10. During the course of this investigation, along with other law enforcement agents, I have interviewed, among others, (a) employees of some of the Insurance Companies and (b) patients who received treatment and/or services from certain physicians who in turn used the defendant MATHEW JAMES as a third-party biller to submit claims to the Insurance Companies for payment. Along with other law enforcement agents, I have also reviewed corresponding insurance company, bank and telephone records, and have also listened to recordings of telephone calls.

11. The interviews and a record review have revealed that the defendant MATHEW JAMES is a third-party biller used by doctors nationwide to submit insurance claims. JAMES's customers are primarily plastic or orthopedic surgeons who are out-of-network² for the Insurance Companies. JAMES earns a percentage of the amount paid on the claims.

12. This investigation, including surveillance of the SUBJECT PREMISES conducted as recently as Wednesday, July 24, 2019, has revealed that the defendant MATHEW JAMES operates the Billing Companies from within the SUBJECT PREMISES.³ JAMES

² An out-of-network physician is a physician who does not have a contract with the Insurance Company setting forth the amount of money the physician will be paid for rendering care to an Insurance Company member.

³ JAMES and his wife reside in the SUBJECT PREMISES as well.

employs multiple individuals in the Billing Companies, who have been observed by law enforcement agents entering and leaving the SUBJECT PREMISES on multiple occasions since October 2018. Additionally, as discussed above, the address reported to the NYS DOS and/or DOL for each of the Leale Entities is the SUBJECT PREMISES, and a form filed with the DOL on December 21, 2017 indicated that Elite Industrial Ltd.'s books and records could be found at that address.

13. As part of the fraudulent scheme, the defendant MATHEW JAMES has:

- a. used fraudulent billing codes both to “upcode” for medical services⁴ and to charge for medical services that were not rendered;
- b. misappropriated private health information;
- c. impersonated patients without the patients’ knowledge; and
- d. attempted to fraudulently induce the Insurance Companies to pay certain physicians more than the insurance companies would ordinarily pay by, inter alia, by indicating that the procedures performed by the physicians were more serious, complicated or emergent than they in fact were.

14. For example, the defendant MATHEW JAMES regularly caused to be submitted claims for complex wound cleansing and closure procedures (such as the removal of debris or dead tissue) when the actual procedure that had been performed was a

⁴ To “upcode” for services means to assign an inaccurate billing code to a medical procedure or treatment in order to increase reimbursement.

comparatively minor wound closure (such as placement of stitches). Insurance Companies generally pay far more for a complex wound repair than they do for a simple wound closure.

15. Typically, insurance companies require medical billers to utilize electronic billing platforms that are accessed over the Internet in order to submit their claims. To utilize these platforms, medical billers must use electronic devices such as computers. At times, insurance companies request additional information regarding claims, including medical records, insurance identification numbers and other private information, which are provided to insurance companies by the medical billers through the online electronic billing platforms and by fax transmission. Billers must also retain claim documentation for significant periods of time after the bills are submitted in order to conduct any reconciliation or appeals that may be necessary. Third-party billers who are paid a percentage of the claims they handle, like the defendant MATHEW JAMES, must additionally retain billing records to ensure that the payments made to them by the doctors are accurate. For all of these reasons, billers generally possess extensive information regarding their billing activities in both paper and electronic form. There is therefore probable cause to believe that the SUBJECT PREMISES and SUBJECT DEVICES will contain records regarding the fraudulent activity described below.

16. The amount insurance companies generally pay a healthcare professional on a claim is normally determined by certain rates and benefits set forth in the relevant health plan. This amount has often been far lower than the high charges submitted by the defendant MATHEW JAMES to the Insurance Companies on behalf of his out-of-network providers for relatively simple procedures.

17. In order to fraudulently induce the Insurance Companies to pay these higher amounts for services rendered, the defendant MATHEW JAMES and others have engaged in a variety of fraudulent activity. In particular, when the Insurance Companies have balked at paying, in full or in part, a patient's fraudulently inflated bills, JAMES has called the Insurance Companies and, using the associated patient's personal identifying information and medical information, pretended to be the patient or a relative of the patient (the "Impersonation Calls"). On these calls, JAMES, impersonating a patient or a patient's family member, asserted that he was being billed by a doctor for the claim, or portion of a claim, associated with the purported procedures that the Insurance Companies had not been willing to pay. On those calls, JAMES then demanded that the Insurance Companies pay the full amount being demanded by the physician so that the unpaid medical bills would not be referred to a debt collection company.

a. JAMES'S Impersonation Calls

18. Many Impersonation Calls were recorded by the Insurance Companies, including a series of calls made in or about 2018 related to Patient A, a child who received a wound cleaning treatment from a doctor for whom the defendant MATHEW JAMES served as a third-party biller.⁵ Prior to these calls, the Insurance Company, a company based in Pennsylvania, had denied the claim for wound cleaning submitted by JAMES. As a part of these calls, an individual who identified himself as Patient A's father repeatedly called the

⁵ These calls were recorded by Insurance Companies as a standard business practice and following notice to all parties on the calls.

Insurance Company to demand the claim be paid. The Insurance Company thereafter paid the claim for wound cleaning. Law enforcement agents later played one of the recorded calls for Patient A's father, who confirmed that the voice on the call was not his.

19. Law enforcement agents have listened to the above-referenced recorded calls and other recorded calls, which took place between July 2015 and December 2018. The defendant MATHEW JAMES has a distinctive accent and, after listening to these recordings in which JAMES identifies himself as a patient or a relative of a patient (including the calls related to Patient A), and after comparing those recordings to other business-related recorded calls JAMES has made to the Insurance Companies in which he was not impersonating anyone and properly identified himself, law enforcement agents have concluded that it is JAMES's voice on both sets of calls. In total, law enforcement agents have identified over 150 Impersonation Calls made by JAMES in which he pretended to be more than 20 separate individuals.

20. On January 9, 2018, at 2:42 p.m., the defendant MATHEW JAMES made an Impersonation Call, in which he posed as the grandfather of a minor patient, to an Insurance Company call center located outside of the United States.

21. The defendant MATHEW JAMES made many of the above-referenced calls using Voice Over Internet Protocol ("VoIP") numbers subscribed to by JAMES at the SUBJECT PREMISES. Most or all of the Insurance Companies to whom JAMES made calls were located outside of New York State. VoIP calls are made over the Internet as opposed to a telephone landline. An electronic device such as a computer or cellular telephone is required

in order to make a call using VoIP technology. There is therefore probable cause to believe that JAMES used the SUBJECT DEVICES in order to complete these VoIP calls.

22. In reliance on the defendant MATHEW JAMES's fraudulent misrepresentations, the Insurance Companies have routinely paid fraudulently high claims submitted by JAMES. Law enforcement agents estimate that JAMES has obtained more than \$12,000,000 from the Insurance Companies from approximately 2015 to the present as a result of his fraudulent medical billing practices, including but not limited to the Impersonation Calls.

23. Based on the foregoing information, there is probable cause to believe that the SUBJECT PREMISES and the SUBJECT DEVICES will contain evidence, fruits or instrumentalities of violations of the SUBJECT OFFENSES.

**SPECIFICS REGARDING THE SEIZURE
AND SEARCHING OF COMPUTER SYSTEMS**

24. Based on my own experience and consultation with other law enforcement agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer experts in a laboratory or other controlled environment:

a. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, and other digital storage mediums, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law

enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to complete during a search on site; and

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

25. Based on my own experience and my consultation with other law enforcement agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating system, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (“CPU”). Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. I am familiar with and understand the implications of the Privacy Protection Act (“PPA”), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT DEVICES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

26. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, modem, router, and other

system components were used as a means of committing the offense(s) and should be seized on that basis alone. Accordingly, permission is sought herein to seize and search the computers and all related devices consistent with the scope of the requested search, as set forth in Attachments A and B, respectively.

27. It is the FBI's intention to implement a procedure for data seized from digital and computer media. Every attempt will be made to copy the data from any hard drives and digital media seized within thirty days of the seizure (if impractical, we will notify the Court and seek additional time). After the data is copied and verified, a copy will be provided to the defendant MATHEW JAMES. Unlike physical records, however, digital data cannot be provided until it has been copied, without altering the original data. At the execution of the search warrant, agents will provide a telephone number to JAMES to contact members of the investigative team regarding securing a copy of seized digital data.

TECHNICAL TERMS

28. Based on my training and experience, 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. 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.

c. 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.

29. Based on my training, experience, and research, I know that the SUBJECT DEVICES have capabilities that allow them to serve as wireless telephones, digital cameras and GPS navigation devices. 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 SUBJECT DEVICES.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

30. 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.

31. *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 SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES 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).

b. 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.

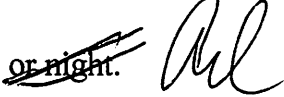
c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. 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.

e. 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.

32. *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 the SUBJECT DEVICES 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 SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

33. *Manner of execution.* Because this warrant seeks permission to examine the SUBJECT DEVICES recovered as a result of the search of the SUBJECT PREMISES, I

submit there is reasonable cause for the Court to authorize execution of the warrant for the SUBJECT DEVICES at any time in the day ~~or night.~~ 

CONCLUSION

34. Based on my training and experience, and the facts set forth in this affidavit, there is probable cause to believe that the defendant MATHEW JAMES have engaged in conspiracy to commit wire fraud, wire fraud and aggravated identity theft.

35. Accordingly, I respectfully request that the Court issue warrants for the arrest of the defendant MATHEW JAMES so that they may be brought before the Court and dealt with according to law.

36. In addition, based on my training and experience, and the facts set forth in this affidavit, there is probable cause to believe that in the SUBJECT PREMISES and SUBJECT DEVICES there exists evidence of crimes – specifically, evidence of violations and attempted violations of Title 18, United States Code, Sections 1028A (aggravated identity theft), 1343 (wire fraud) and 1349 (conspiracy to commit wire fraud).

37. Accordingly, I respectfully request that the Court issue a search warrant for SUBJECT PREMISES and the SUBJECT DEVICES, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, which constitute evidence, fruits or instrumentalities of violations of 18 U.S.C. §§ 1028A, 1343 and 1349.

38. Because this application seeks authority to arrest the defendant and to examine the SUBJECT DEVICES recovered as a result of the search of the SUBJECT PREMISES, there is reasonable cause for the Court to authorize execution of the warrants at any time in the day.

REQUEST FOR SEALING AND NON-DISCLOSURE

39. I further request that the Court order that all papers in support of this application, including the affidavit and arrest and search warrants, 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, and not all of the targets of this investigation will be arrested or searched at this time. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, notify confederates or otherwise seriously jeopardize the investigation. Some of the evidence in this investigation involves communications that can be transferred to alternate platforms (including encrypted platforms and platforms beyond the jurisdictional reach of U.S. legal process). If alerted to the existence of the warrant, there is

reason to believe that the subjects under investigation will destroy that evidence and change their patterns of behavior.

Respectfully submitted,



William Sena
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on July 25, 2019



HONORABLE ARLENE R. LINDSAY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

(1) THE PREMISES KNOWN AND DESCRIBED AS 24 FORSYTHE DRIVE, EAST NORTHPORT, NEW YORK 11731 (the "SUBJECT PREMISES"), and

(2) ANY AND ALL ELECTRONIC DEVICES LOCATED AT THE PREMISES OF 24 FORSYTHE DRIVE, EAST NORTHPORT, NEW YORK 11731 (the "SUBJECT DEVICES")

The SUBJECT PREMISES is a one-story residential home, with a basement, located at 24 Forsythe Drive, East Northport, New York. The house is a white color with a red brick front. There is a single-car garage attached to the house on the left (when facing the house) and front door to the right of the garage; there are glass pane windows by the front door. There is a mailbox at the street line in front of the house with the number "24" on it. The house sits on a corner lot at the corner of Forsythe Drive and Adrian Street. A photograph of the SUBJECT PREMISES follows:



The SUBJECT DEVICES include at least one cellular telephone bearing cellular telephone number 631-827-8159 (the "SUBJECT PHONE"). The SUBJECT DEVICES also include any and all computers, tablets, iPads, cellular telephones, and any and all removal data storage media (e.g., compact discs, digital video discs, memory cards, memory sticks, zip discs, magnetic tapes, thumb or flash drives, or other external/docktable peripheral that can be easily removed from a computer system and which also contain removal medial capabilities) located in the SUBJECT PREMISES, as there is probable cause to believe that the defendant MATHEW JAMES used electronic devices in the SUBJECT PREMISES in furtherance of the fraud scheme.

ATTACHMENT B

Items To Be Searched For And Seized

The items to be seized are evidence or instrumentalities of violations of Title 18, United States Code, Sections 1341, 1343, 1347, 1349 (mail, wire and health care fraud and conspiracy to commit said crimes), and 1028A (aggravated identity theft).

With Respect to the SUBJECT PREMISES

The items to be seized are evidence or instrumentalities of violations of Title 18, United States Code, Sections 1341, 1343, 1347, 1349 (mail, wire and health care fraud and conspiracy to commit said crimes), and 1028A (aggravated identity theft).

Specifically, all documents or other materials relating to the defendant MATHEW JAMES's ("JAMES") operation of any and all businesses related to medical billing and/or his conduct as a third-party medical biller, including but not limited to JAMES's ownership and operation of various corporations, including, but not limited to, Leale, Inc., Leale Billing Corp., Remm Consultants, Inc., and Elite Industrial Ltd. (collectively, the "LEALE ENTITIES"), for the period of time of July 2015 to the present.

Such documents and materials include:

1. all documents relating to assets, liabilities, income, expenses, sales and accounts receivable of the defendant MATHEW JAMES or any of the Leale Entities, including, but not limited to, (a) invoices, payroll records, expenses and liabilities, cash receipts and disbursements, general journals, general ledgers, sales ledgers, purchase journals, accounts receivable ledgers, accounts payable ledgers, bills of lading, contracts, agreements, change orders, charge backs, bank statements, cancelled checks, deposit tickets, debit memos, credit memos, wire transfers, check books, passbooks, contracts, work papers, ~~cash~~, correspondence, memoranda, notebooks, client lists and drafts, all records and other documents showing the LEALE ENTITIES' company letterhead or reference to any LEALE ENTITY or JAMES; (b) all records relating to income and expenditures, such as income and payroll tax returns, vendor invoices, and (c) all records of communications and correspondence, such as: mailings, fax machines including records of recorded transmissions, telephone records (including cellular or computerized telephones and answering machines with numbers stored in and relayed to such devices); (d) any and all documents relating to the existence and rental of safe deposit boxes, keys to safe deposit boxes and access to safes or cabinets, locked or unlocked, containing items described above.


2. All documents relating to any mail box belonging to the defendant MATHEW JAMES or any of the LEALE ENTITIES located at a commercial mail receiving agency, including, but not limited to, customer applications and correspondence;

3. All documents relating to communications or contacts between the defendant MATHEW JAMES and/or any of the LEALE ENTITIES' employees or agents, or any and all victims and/or insurance company victims, including not limited to, letters, phone messages, email, text messages, "chat" or instant messages, including any attachments to such emails or messages, sent by or received by the user(s) of any computer included in and/or maintained on the SUBJECT DEVICES, whether saved or deleted, and whether contained directly in an email, text message, chat, or instant message account or in a customized "folder;"

4. All documents relating to the defendant MATHEW JAMES's calendar, contact, or personal planner data or files, created or maintained by the user(s) of any computer included in and/or maintained on the SUBJECT PREMISES.

With Respect to the SUBJECT DEVICES⁶

1. All records on the SUBJECT DEVICES described in Attachment A that relate to violations of Title 18, United States Code, Sections 1341, 1343, 1347, 1349 (mail, wire and health care fraud and conspiracy to commit said crimes), and 1028A (aggravated identity theft) and involve the defendant MATHEW JAMES, including the information identified above in Attachment B with respect to the SUBJECT PREMISES, as well as the following information for the time period July 1, 2015 to the present:

- 
- a. names and telephone numbers, as well as the contents of all call logs, contact lists, text messages (including those sent, received, deleted and drafted), instant messages, ~~photographs, videos, Facebook posts~~, Internet activity (including browser history, web page logs, and search terms entered by the user), geo-location data, application data, and other electronic media;
 - b. lists of customers and related identifying information;
 - c. information related to and amounts of checks deposited and money withdrawn, related to the LEALE ENTITIES' purported business, as well as dates, places, and amounts of said transactions;

⁶ Any SUBJECT DEVICE seized will be reviewed on premises to determine ownership by both physical review and questioning of any occupants to the extent possible. Moreover, the room or area in which any SUBJECT DEVICE is located will be taken into consideration before seizure (i.e. devices located in a child's room will not be seized unless there is some indicia that the device is not utilized by the child).

- d. any information related to sources of checks (including names, addresses, phone numbers, or any other identifying information);
- e. any information recording the defendant MATHEW JAMES's schedule or travel;
- f. all bank records, checks, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the times the SUBJECT DEVICES were used;

5. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICES; and

6. Contextual information necessary to understand the evidence described in this Attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.