ID#: 2174

IN THE_____COURT OF THE SECOND JUDICIAL
CIRCUIT IN AND FOR LEON COUNTY, FLORIDA

AFFIDAVIT FOR SEARCH WARRANT

COMES NOW, the Affiant, Noel Pratts, a Special Agent of the Florida Department of Law Enforcement, who personally appeared before a sworn officer, makes this affidavit, which has been submitted to the Court. The Affiant swears under oath that he has probable cause to believe that certain laws are being violated in or about a certain premises and the curtilage thereof and that evidence of the violation of certain laws in the form of computer equipment and data, or printed or written documents and other related items described herein, are being kept in or about certain premises and the curtilage thereof, in **LEON** County, Florida, being known and described as follows:

2540 CENTERVILLE CT., TALLAHASSEE, FL 32308

Directions and Description:

2451 Centerville Road, travel left/north onto Centerville Rd., for approximately 0.1 miles, then turn right onto Centerville Ct. approximately 0.3 Miles. The premises will be on the left/north side of Centerville Ct. approximately 354ft from Centerville Road.

The formal address of the premises to be searched is **2540 CENTERVILLE CT. TALLAHASSEE, FL 32308** and the premises and its curtilage is referred to as "The Premises." The premises is described as a single family Condominium home. The residence has off-white siding with red brick accent around the green door. The number 2540 is clearly displayed on the condominium near the front door of the residence.

The Premises and the curtilage thereof are being used for the purpose of storing computer or electronic devices relating to the unauthorized access of a computer, computer system, computer network, or electronic device. Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized, in violation of section 815.06(2)(a), Florida Statutes, and contains evidence of, or evidence relevant to proving, the referenced felony has been, or is being committed.

INVESTIGATOR BACKGROUND

Your Affiant, Noel Pratts is a Special Agent (SA) with the Florida Department of Law Enforcement (FDLE), assigned to the Tallahassee Regional Operations Center, (TROC) Cyber High/Tech Crimes Squad and has been a law enforcement officer for the past 18 years. Your Affiant has approximately 13 years of experience in criminal investigations. Your affiant is a Certified Cyber Crimes Investigator by The National White-Collar Crime Center Board of Directors and has successfully completed numerous hours of training specific to cybercrimes to include the FBI's Cyber Intrusions, FBI's Exploiting Network Communications, NW3C Basic Network Intrusion Investigations, SANS Introduction to Information Security, Comp TIA Network +, and several others.

Your affiant is a member of the Federal Bureau Investigation (FBI) Cyber Task Force. This Task Force is comprised of federal and state law enforcement agencies engaged in the investigation of computer related crimes involving cyber intrusion. As a Special Agent with FDLE, your affiant is authorized to investigate all criminal matters in the state of Florida, specifically any and all crimes involving computers.

Based on all the above described training and experience, and the investigative facts and activity set forth herein, your affiant has developed probable cause to

believe and does believe that the crimes described herein are or were being committed at or within the Premises or evidence of the said crimes is contained within the herein described account at the Premises. The following facts support your Affiant's probable cause:

CURRENT INVESTIGATION:

On November 10, 2020, Special Agent (SA) Noel Pratts spoke to Derrick Smith from the Bureau of Preparedness and Response with the Florida Department of Health (FDOH) via telephone and he advised that FDOH utilizes a custom-made communications application for Emergency Management designed by ReadyOP.

ReadyOP is a web-based platform developed for incident and emergency planning, immediate access to information, and fast, flexible, and efficient communications. ReadyOp integrates multiple databases and communications platform for fast, efficient access to information, as well as the ability to plan, coordinate, direct and communicate with multiple persons, groups and agencies.

On November 10, 2020, at approximately 1420 hours and 1442 hours, an unidentified subject gained access to a multi-user account group "StateESF-8.Planning" and sent a group text stating the following: *"it's time to speak up before another 17,000 people are dead. You know this is wrong. You don't have to be part of this. Be a hero. Speak out before it's too late.- From StateESF8.Planning"*. FDOH estimates that approximately 1,750 messages were delivered before the software vendor was able to stop the message from being transmitted.

FDOH has several groups within ReadyOp's application platform, one of which is StateESF8.Planning. ESF8 is Florida's Emergency Support Function for Public Health and Medical with which they coordinate the state's health and medical resources, capabilities, and capacities. They also provide the means for a public health response, triage, treatment, and transportation. The group StateESF8.Planning is utilized by multiple users, some of which are not employees of FDOH but are employees of other government agencies. Once they are no longer associated with ESF8 they are no longer authorized to access the multi-user group.

All users assigned to StateESF8.Planning group share the same username and password. SA Pratts requested and received a copy of the technical logs containing the Internet Protocol (IP) address for users accessing the ReadyOp web-based platform for the multi-user StateESF8.Planning.

SA Pratts reviewed the logs and identified an IPv6 address 2601:4c1:4000:3a80:286e:3dd1:fcd:5c4a sent the group text on November 10, 2020 at 1420 hours.

An open-source search through WHOIS IP lookup revealed the IPv6 address is under the control and domain of Comcast Cable Communications.

Through the use of investigative resources your Affiant determined that the IPv6 address 2601:4c1:4000:3a80:286e:3dd1:fcd:5c4a resolved to Comcast subscriber Rebekah Jones with a service address of 2540 Centerville Ct., Tallahassee, FL 32308 , Comcast account: 8535101682713212 and email address rebekah.coastal@comcast.net. Jones is a former employee of FDOH who was terminated by FDOH in May of 2020 and is no longer authorized to access the FDOH ReadyOp system.

COMPUTER EVIDENCE

Your Affiant knows from training and experience that digital evidence is not limited to computers. Your Affiant has been involved in numerous cases where persons can access the Internet, store data and communicate with other individuals with the same interests using digital communications devices to include cellular telephones, email devices and personal digital assistants among several others. These devices are frequently found to contain chat communications in the form of short message service (SMS) messages, texts or email as well as enabling Internet access and digital cellular network access.

Your Affiant knows from training and experience that persons using computers for criminal purposes will frequently transfer data to other digital media storage devices. Digital storage media may include but is not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers or other electronic devices to store or retrieve data, which can store the equivalent of thousands of pages of information. Users may store information in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site.

Your Affiant knows from training and experience that searching digital evidence systems for criminal evidence requires experience in the computer and cellular telephone field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system, known as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

Your Affiant knows from training and experiences that computers and other digital communications devices contain volatile memory that contains information only while the device is in a powered on and/or running state. Your Affiant knows

that powering off the device may result in the loss of the volatile information. Your Affiant also knows that adding an external evidence storage device will cause minor changes to the state of the computer but will allow for the best effort in fully capturing the state of the running evidence. Your Affiant knows that this capture of information requires technical expertise to ensure the resulting data can be examined by all subsequent investigators. Your Affiant knows that this captured information may include current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet traffic and other digital communications traffic and passwords, encryption keys or other dynamic details relevant to use of the system.

Your Affiant knows from training and experience that in order to fully retrieve data from a computer or other digital communications system, the analyst needs all magnetic storage media as well as the storage devices. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware access software or 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 documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

Your Affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

Your Affiant knows from training and experience that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

Your Affiant knows from training and experience that digital crime scenes usually include items or digital information that would tend to establish ownership or use of digital devices and Internet access equipment and ownership or use of any Internet service or digital cellular service accounts to participate in the exchange, receipt, possession, collection or distribution of data.

Your Affiant knows from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to further their criminal behavior to include credit card bills, telephone bills, correspondence and other identification documents.

Your Affiant knows from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

The above information has led your Affiant to believe that probable cause exists to search for the items listed below. There is evidence of a violation of **Florida State Statute 815.06(2)(a)** Offenses Against Users of Computers, computer system, computer networks, and electronic devices, and a person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization: (a) Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized: and this evidence is concealed in the residence at **2540 Centerville Ct., Tallahassee, Florida**

Your Affiant hereby requests the Court's permission to seize the following items, and to conduct an **off-site search** and **analysis**, or to delegate the search and analysis to an off-site computer forensic analyst, of the following items 1 through 15 (hereinafter the "Property"), which are evidence of, or evidence relevant to proving, the felony(s) noted herein;

1. **Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, cellular devices, personal computers to include "laptop" or "notebook" "tablet" or "pocket" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).**

2. **Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.**

3. **Computer storage media and the digital content to include but not limited to floppy disks, hard drives, USB flash drives, SD cards, VHS tapes, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data.**

4 Computer software and application software installation and operation media, and any other computer software related to the unauthorized access of any computer, computer systems, computer network, or electronic device.

5 Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

6 Manuals and other documents (whether digital or written) which describe operation of items or software seized.

7 Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

8 Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of data involving the facilitation of computer crimes offenses.

9 Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to further computer crimes offenses to include credit card bills, telephone bills, correspondence and other identification documents.

10 Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

11 Files and data on the computer that show the suspect's ownership, possession and control at time of the offense.

12 Any and all software that may be utilized to create, receive, distribute, store, or modify the evidence sought and all software that may be used to communicate or store online communications.

13 Encrypted, deleted and unallocated files on electronic media that contain any of the information listed in previous paragraphs.

14 Notations, files or documentation containing passwords or codes necessary to unlock computer files or to access the computer or storage media.

15 Any computer or computer-related device, software program, information pertaining to the use of intrusion software, manuals, log files or other documents related to the unauthorized access of any computer, computer system, computer network, or electronic device.

Your Affiant is aware that the recovery of data by a computer forensic analyst takes significant time, and much in the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from "the Premises". Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

WHEREFORE, affiant makes this affidavit and prays for the issuance of a Search Warrant in due form of law commanding the Executive Director of the Florida Department of Law Enforcement, or any of his duly constituted Special Agents, and the Sheriff of **LEON** County, or any of his duly constituted deputies, including forensic computer analyst experts, to search the above described "Premises" and the curtilage thereof, and any vehicles thereon, or persons located within the "Premises" and the curtilage reasonably believed to be connected with said illegal activity, for the said "Property" heretofore described, and to search said "Property" described above and to seize and safely keep same, either in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, in order that the evidence may be procured to be used in the prosecution of such person or persons who have unlawfully used, possessed, or are using or possessing the same in violation of the laws of the State of Florida.

Special Agent Noel Pratts
Florida Department of Law Enforcement

Sworn to and subscribed before me this 3 day of December, 2020.

X
Certified Officer

X Personally Known
____ Produced identification
Type:

ID#: 2174

IN THE _____ COURT OF THE SECOND JUDICIAL
CIRCUIT IN AND FOR LEON COUNTY, FLORIDA

SEARCH WARRANT

IN THE NAME OF THE STATE OF FLORIDA

The Executive Director of the Florida Department of Law Enforcement, or any of his duly constituted Special Agents, and the Sheriff of **LEON** County, or any of his duly constituted deputies, and the Director of the Homeland Security Investigations, or any of his duly constituted Agents, with any proper and necessary assistance, including forensic computer analyst experts.

WHEREAS, complaint on oath and in writing supported by affidavit of credible witness, to-wit: Special Agent NOEL PRATTS of the Florida Department of Law Enforcement, has been made to me, the undersigned Circuit/County Court Judge in and for **LEON** County Florida, and WHEREAS said facts made known to me and considered by me have caused me to certify and find that there is probable cause to believe that certain felony laws have been violated, to wit: unauthorized access of any computer, computer system, computer network, or electronic device. Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized, in violation of section F.S. 815.06(2)(a), in or by means of, certain computer equipment, or that evidence of, or evidence relevant to proving a violation or certain laws is contained within and together with said computer equipment and data described hereinafter, which is/are located in or about a certain Premises and Curtilage in Leon County, Florida being known and described as follows:

2540 CENTERVILLE CT., TALLAHASSEE, FL 32308

1

DIRECTIONS AND DESCRIPTION

From Publix, 2111 Centerville Road, travel left/north onto Centerville Rd., for approximately 0.1 miles, then turn right onto Centerville Ct. approximately 0.3 Miles. The premises will be on the left/north side of Centerville Ct. approximately 354ft from Centerville Road.

The formal address of the premises to be searched is **2540 CENTERVILLE CT. TALLAHASSEE, FL 32308** and the premises and its curtilage is referred to as "The Premises." The premises is described as a single family Condominium home. The residence has off-white siding with red brick accent around the green door. The number 2540 is clearly displayed on the condominium near the front door of the residence.

NOW THEREFORE, you are hereby ordered and authorized to seize the following items, hereinafter referred to as "The Property", and to conduct an off-site search and analysis for the below-described items, as applicable. You may utilize the assistance of computer forensic examiners either from your agency or other agencies to locate any of the items stored on computers or electronic storage media.

1. **Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, cellular devices, personal computers to include "laptop" or "notebook" or "pocket" or "tablet" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).**

2. **Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.**

3. **Computer storage media and the digital content to include but not limited to floppy disks, hard drives, USB flash drives, SD cards, VHS tapes, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data.**

4. Computer software and application software installation and operation media, and any other computer software related to the unauthorized access of any computer, computer systems, computer network, or electronic device.

5. Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

6. Manuals and other documents (whether digital or written) which describe operation of items or software seized.

7. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

8. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of data involving the facilitation of computer crimes offenses.

9. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to further computer crimes offenses to include credit card bills, telephone bills, correspondence and other identification documents.

10. Items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

11. Files and data on the computer that show the suspect's ownership, possession and control at time of the offense.

12. Any and all software that may be utilized to create, receive, distribute, store, or modify the evidence sought and all software that may be used to communicate or store online communications.

13. **Encrypted, deleted and unallocated files on electronic media that contain any of the information listed in previous paragraphs.**

14. **Notations, files or documentation containing passwords or codes necessary to unlock computer files or to access the computer or storage media.**

15. **Any computer or computer-related device, software program, information pertaining to the use of intrusion software, manuals, log files or other documents related to the unauthorized access of any computer, computer system, computer network, or electronic device.**

In addition to the seizure of the above-mentioned "Property", the Court gives permission to seize the computer hardware (and associated peripherals) and software and to conduct an off-site analysis of the hardware and software for the evidence described, or enlist the aid of a qualified Forensic Analyst, if, upon arriving at the scene, the law enforcement officers executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

NOW THEREFORE, with such lawful assistance as may be necessary, to include forensic computer analyst experts from your agency or other agencies, you are hereby commanded, in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, to enter and search the aforesaid "Premises" and curtilage thereof, and any vehicles thereon, or any persons located on the "Premises" or within the curtilage reasonably believed to be connected with said illegal activity, for the "Property" described in this warrant and if the same or any part thereof be found, you are hereby authorized to seize and secure same, giving proper receipt therefore and delivering a completed copy of this warrant to the person in control of the "Premises", or in the absence of any such person, leaving a completed copy where the items are found, and making a return of your doings under this warrant within ten (10) days of the date hereof, and you are further directed to bring said property so found before the Court having jurisdiction of this offense to be used in the prosecution of persons violating this offense and thereafter to be disposed of according to law.

Sworn to and subscribed before me this ____day of 12/3/2020, 20___.

12/3/2020 5:57:57 PM

CIRCUIT /COUNTY JUDGE