COUNTY OF LARIMER )

) SS IN THE COMBINED COURT

STATE OF COLORADO )

**SEALED**

**AFFIDAVIT FOR SEARCH WARRANT FOR CELLULAR TELEPHONE(S)**

Before the Honorable \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge/Magistrate

Affiant, LEO NAME, a commissioned law enforcement officer, being duly sworn, deposes and says that I have probable cause to believe that there are grounds for the issuance of this search warrant pursuant to C.R.S. § 16-3-301 and C.R.S. § 16-3-301.1; and that I have probable cause to believe that within the devices described and identified as:

**CELL PHONE DESCRIPTION**

**ADD PHOTO OF PHONE IF AVAILABLE**

**ADDRESS WHERE PHONE IS LOCATED**

There is now located the following data stored in the above-referenced cellular telephone(s), SIM card(s) and/or memory card(s), relevant to the criminal activity described in the affidavit, which is incorporated by reference, that can be viewed and or extracted by the Northern Colorado Drug Task Force (NCDTF), the LE AGENCY, and other agents assisting the LE AGENCY:

REVIEW THE LISTED CATEGORIES OF DATA, PLEASE REMOVE ANY CATAGORIES NOT SUPPORTED BY THE FACTS CONTAINED IN YOUR AFFIDAVIT

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
3. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
4. Data contained in notes, reminders, documents, calendars and/or other similar applications pertaining to the Subject Offense(s);
5. Telephone contact lists, phone books and telephone logs who may have been contacted by use of this device or by other means for the purpose of committing Subject Offense(s);
6. Voicemail messages, text messages, MMS messages, Emails whether stored, received, or deleted as they pertain to Subject Offense(s);
7. Photographs or images stored, sent, received or deleted, or documents containing photographs or images pertaining to Subject Offense(s);
8. Videos stored, sent, received or deleted pertaining to Subject Offense(s);
9. Electronic files, data, videos, and communications, including related metadata and location data, stored, sent, received or deleted from social media applications such as Facebook, Snapchat, Instagram, Twitter and/or any other third party programs or applications located on the device pertaining Subject Offense(s);
10. Communications through the (SELECT SIRI OR GOOGLE ASSISTANT) system, including all communications entered into the system as well as communicated from the system to the user pertaining to Subject Offense(s);
11. Global position system (GPS) data and any other geolocation data pertaining to Subject Offense(s);
12. Records of internet activity, including internet protocol (IP) addresses and Port IDs, firewall logs, transactions with internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses pertaining to violations of the law or that show who used, owned, possessed, or controlled the device(s) pertaining to Subject Offense(s);
13. The passwords and usernames for any accounts, cloud-based storage accounts or applications which are accessible through the above-identified digital device(s);
14. Any electronic files or data stored, sent, received, or deleted from social media applications, pertaining to Subject Offense(s) which allow for the posting of information or the communication between parties, including but not limited Facebook, Snapchat, Instagram, and Twitter.

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST.

Items which are evidence of violations of the Colorado Uniform Controlled Substances Act, C.R.S. §18-18-405.

Further, I have probable cause to believe that the requested items constitute property which is designed or intended for use as a means of committing a criminal offense, or which have been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, pursuant to C.R.S. § 16-3-301 and C.R.S. § 16-3-301.1.

Your Affiant is a sworn law enforcement officer with the LE AGENCY and is currently assigned to the Northern Colorado Drug Task Force (NCDTF). Your Affiant has been trained at the state and local levels with regard to my duties and is authorized by law to execute search and arrest warrants in the State of Colorado.

Based on my training and experience, I know that persons involved in the distribution, use and manufacture of a controlled substance utilize multiple cellular telephone devices to aid and facilitate in the distribution of controlled substances and the cellular telephones are likely to contain material evidence pertaining to the distribution of controlled substances.

Your Affiant believes the below-described facts to be true based upon official law enforcement and Northern Colorado Drug Task Force records, conversations with fellow officers, personal observations and interviews.

The facts establishing grounds for issuance of a search warrant and showing probable cause to believe that they exist are as follows:

**PROBABLE CAUSE STATEMENT**

**Conclusion**

Your Affiant believes that the facts described above demonstrate that the above-referenced cellular telephoneshave been utilized to facilitate the illegal trafficking of controlled substances in northern Colorado, and that there is probable cause to believe that these cellular telephones contain evidence of violations of the Colorado Uniform Controlled Substances Act, C.R.S. §18-18-405.

Application is hereby made for issuance of a search warrant, directed to any officer authorized by law to execute warrants in the county wherein said property is located, commanding said officer to search forthwith the above described cellular telephone(s) and to collect any electronic data contained within them, including, but not limited to call logs, contact lists, text and multi-media messages, photographs, videos, emails, documents and data packets.

Below paragraphs should correspond to the listed items to seize above. Delete any paragraphs that are not relevant.

A cellular telephone is a handheld wireless device used for, inter alia, voice and data communication. 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, including 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 including websites, social media sites, bulletin boards, file sharing, and other Internet sites. It also includes GPS technology for determining the location of the device.

Your Affiant is aware that due to the nature and vulnerability of electronic, digital or magnetic data contained within a cellular telephone device, it is best to conduct the search of such a device in a controlled environment so that the data is protected, and unaltered. Therefore, your Affiant expressly requests the authorization to seize any and all media capable of storing electronic, digital or magnetic data contained within a cellular telephone device and any and all related hardware associated with the above-referenced devices.

Your Affiant is also aware that there are numerous ways in which electronic, digital or magnetic data contained within a cellular telephone device may be altered, deleted, erased or encrypted remotely, when a person is not physically in possession of the cellular telephone device. Therefore, your Affiant expressly requests the authorization to take steps to safeguard the data contained within the said cellular telephone devices by removing the power source, such as the battery, or by disabling the device’s ability to connect with a cellular telephone provider or an internet services provider.

Cellular telephones have the ability to store and utilize data from external memory devices. These external digital storage devices, ie. microSD and SD cards provide the device with the ability to capture and store an increased amount of data. By their design, they are removable and portable, allowing the stored information to be transported separately from the cellular telephone and/or utilized by additional cellular telephones and other digital devices.

Based on knowledge, training, and experience, Your Affiant knows that digital storage devices can store information for long periods of time. This information can sometimes be recovered with forensic tools. In addition, examining data stored on digital storage devices can uncover, among other things, evidence that reveals or suggests who possessed or used the computer or digital storage devices.

Based on the technology available to Your Affiant, obtaining the above described data and information will necessarily require an initial extraction of all of the data from the phone. This data, in raw form, is unreadable without the use of specific software. The extraction of the data will involve processing the data through the software, and a report containing only the data listed in the warrant will be produced. As such, only the data listed in this Affidavit and in the Search Warrant will be viewed by Your Affiant and/or his or her designee.

Your Affiant respectfully requests that this Search Warrant be approved so that your Affiant or Designee may search the above described data associated with the cellular phone identified above. A search of the data associated with the cellular phone is necessary because such data may be relevant to the offenses being investigated.

Additionally, your Affiant is aware that searching for and documenting electronic and digital evidence is a highly technical process that requires specific expertise and specialized equipment. Due to the many types of computer hardware and software in use today, it is often necessary to utilize computer software programs in order to analyze the electronic data that may be stored or may have been deleted on a particular cellular telephone device. Similarly, computer experts may need to be consulted during the search of the cellular devices due to the highly technical nature of evidence recovery and its analysis. Therefore, your Affiant requests the authorization to consult with and to receive the assistance of computer and technical experts during the course of the search of these devices.

Based on training, experience, and general knowledge of human behavior in today’s society, Your Affiant knows that most individuals own and possess a cellular telephone, and retain their phones on their person or in their immediate possession. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (“While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.”); *Riley v. California*, 134 S.Ct. 2473, 2484 (2014) (“modern cell phones [] are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”).

Your Affiant also knows from training and experience that criminals frequently communicate with each other and/or other individuals before, during, and after criminal events. Your Affiant also knows from his/her training and experience that this type of communication usually occurs via cellular phones. Analysis of the data contained in a cellphone or other mobile/electronic device could assist Your Affiant with determining the general location of the device before, during, or after the target offense. This information, along with other information that can be obtained through an electronic device such as a cellphone, will assist Your Affiant with furthering the above-described criminal investigation.

For example, evidence relating to the above described offense(s) and/or related events or information is likely to be contained in the categories detailed above. Communications made and preserved through call history, contact information, voice messages, text and MMS messages, emails, and social media applications with communication capability (i.e., Facebook Messenger, Snapchat, and other similar applications) may include evidence of the target offenses. Communications made by the person who possessed and used the phone through any of these methods may also include comments made to others that relate to the target offenses described above, or may include information that can lead to the discovery of other evidence.

In addition to information or data contained in the phone relating to communications, photos and/or videos stored in the phone may depict individuals involved in or with knowledge of the crimes, may show connections between individuals involved in the target offense(s), and/or may lead investigators to others who can provide further relevant evidence. Based on training and experience, individuals often take and distribute/post photos and videos that include information about their criminal actions and post details and communicate with others about criminal activity and other information relating to criminal activity. Photos and videos depicting involved persons wearing similar clothing to that described by witnesses or observed in recordings can also be found in cellphones.

Geographical location information can be obtained from various areas in the phone, such as connected with phone calls, text or MMS messages, email messages, photos, videos, and social media application. This data is important to establish the location of the phone (and therefore, the person in possession of the phone) before, during, and after the target crimes. Geographical location information may also be helpful to lead investigators to other persons who may have been present at the time the offenses described above occurred, or may lead to the location of other evidence.

Data relating to the internet activity on the phone can provide multiple types of relevant evidence. Web searches can show efforts to identify locations, people, or other information relevant to the planning and/or commission of the offense. Such searches can also show efforts to keep track of the crime and investigation through the internet, which can establish consciousness of guilt and/or knowledge of these crimes. Internet data can show communications with others, through chat rooms, forums, or other websites, and such communications can establish the suspect’s involvement in or knowledge of the crimes, as well as provide information relevant to motive and intent. Internet data can also contain location information, and can demonstrate the use of services, programs, or applications that can themselves contain evidence of the criminal activity and/or the parties’ involvement therein.

In the event that relevant and/or incriminating evidence is located in the phone, it will be critical to establish the individual in possession of the phone at or about the time the communications are made, the photos and/or videos are captured, or social media applications are used. Evidence attributing particular data items located in the device can come in the form of other communications made at or near the time of the incriminating event that can be tied to the suspect(s), call logs and contact information connecting the device and/or particular communication events to the suspect, and other data that can be found on the phone that can establish the identity of the person in possession of the phone at the time the incriminating data was captured by the device. Data relating to possession, dominion and control over the cellphone will assist in associating any communications or data to the person who made such communications or accessed/created/distributed such data.

It is my training and experience that suspects as well as private citizens are utilizing “cloud computing”, which can be accessed from all types of digital devices with access to the Internet, to access and store their digital data. Cloud Computing refers to the use of computing resources hardware and software, or more commonly understood as the cell phone or computer and the applications or software used. The “Cloud” allows data in the form of documents, pictures, videos, music and any other medium to be uploaded to an account on a service provider’s server and accessed by the user utilizing various methods such as computers, tablets, smart phones, etc. It is an offsite storage medium for items typically stored and/or saved on a computer or cell phone.

I have discovered that private citizens and businesses are using electronic service providers who provide the service of storing electronic data from anywhere there is service to the Internet. In doing so, an authorized user can electronically access records and other data on a remote server from any device that can connect to the Internet. This allows the customer to connect to the server and view, transfer, alter, create, copy, and print the data from the remote server as if it was at the same location as the user’s digital device. The user typically owns and controls the data stored at the remote server while the electronic service provider owns the server on which data is stored.

I know that in the past several years cloud services have become an integral part of digital devices and user’s data storage. I know that many digital devices utilize the “cloud” to store backups and/or data to be accessed from multiple devices. I know that many digital devices are using cloud services by default, sometimes without the user’s knowledge. This use of cloud storage has become so closely tied with many devices that the cloud functions as an extension of their digital device. For this reason, persons may have data on the cloud that is not present on the digital device, either because of an attempt to conceal the data, ease of access between multiple devices, or lack of knowledge of the technology. Some of the common cloud storage services are Google Drive, Apple iCloud, Dropbox, Microsoft OneDrive and Office365. Some of the common cloud-based applications are Facebook, Twitter, KIK, Instagram, Snapchat, and WhatsApp. There were 3.5 million applications available as of October 2019 and it would be difficult to list them all or know all that are in use on a digital device until a forensic analysis is conducted.

Furthermore, due to the ease at which the data on the cloud can be altered, deleted, changed and added to; I believe that if cloud storage is discovered at the time of the execution of the search warrant it is imperative to immediately preserve the data. This may include utilizing the usernames and passwords located through forensic analysis, software tokens stored on the device, or from the suspect directly, to access and preserve the data located on remote servers at the time of the execution of the search warrant. I believe it is necessary to preserve this data quickly as it may change quickly through continued use or because of an attempt to destroy evidence by anyone with access to the Internet, the username and password.

It is also my training and experience that cellular telephones are now being utilized by suspects, as well as private citizens, for the purposes of portable computing. Many smart phones or cellular telephones have the ability to; type and store documents, take and store pictures/videos, access the Internet, deploy applications (which can be programmed to do almost anything), make phone calls, send and receive SMS/MMS messages, connect to social networks, remotely store data on the “cloud”, store large amounts of data on the actual phone, sync with a computer, and show live video streaming.

I also know through my training and experience that communication on digital devices has expanded beyond the use of basic applications which come pre-installed on digital devices. Currently, many people now utilize many different applications to communicate with individuals and/or groups of people. These applications may store user communication records/data on the digital device itself or on the application’s (Company’s) server. For this reason, the digital devices’ access to data through the Internet is an extension of the digital device. An application may reveal messaging information to a user when connected with the username and password to the remote server, but when the phone doesn’t have Internet access, a user may see no data on the device. This data is slightly different than what is described above because the presence of or lack of this data may only be found during the forensic analysis of the digital device. For the reasons stated, it is very important to utilize the device in conjunction with the Internet, usernames and passwords to preserve and analyze this information. I know that many users communicate directly through these applications and\or the communication material may only be accessible by utilizing the Internet, username, and password. If it is discovered that a user has data/communication data stored remotely and access on a digital device is granted when the application is launched, it is important that the analysis also include preserving the data that is accessed remotely.

***Further requests:***

1. Pursuant to Crim. P. 41 and §16-3-304(2), Your Affiant requests that this Court seal the affidavit and search warrant and court order for production of records until the filing of charges based on this law enforcement criminal investigation. The affidavit establishes grounds to believe that disclosure at this time of the affidavit and search warrant and court order for production of records would be contrary to the public interest. Such order for sealing does not apply to representatives of law enforcement agencies, and District Attorney’s Offices.

The executing law enforcement officer(s) seek to also enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imaging, and analysis of any and all of the information described.

Affiant\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_am/pm.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge/Magistrate

COUNTY OF LARIMER )

) SS IN THE COMBINED COURT

STATE OF COLORADO )

**SEALED**

**SEARCH WARRANT FOR CELLULAR TELEPHONE(S)**

Before the Honorable \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge/Magistrate

**TO: ANY PEACE OFFICER AUTHORIZED BY LAW TO EXECUTE SEARCH WARRANTS IN THE STATE OF COLORADO.**

The Court, upon review of a sworn Affidavit filed by LEO NAME, in support of the issuance of this search warrant, hereby commands you to search the following described property, namely:

**CELL PHONE DESCRIPTION**

**ADD PHOTO OF PHONE IF AVAILABLE**

**ADDRESS WHERE PHONE IS LOCATED**

And to Seize:

The following data stored in the above-referenced cellular telephone(s), SIM card(s) and/or memory card(s), relevant to the criminal activity described in the affidavit, which is incorporated by reference, that can be viewed and or extracted by the Northern Colorado Drug Task Force (NCDTF), the LE AGENCY, and other agents assisting the LE AGENCY:

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
3. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
4. Data contained in notes, reminders, documents, calendars and/or other similar applications pertaining to the Subject Offense(s);
5. Telephone contact lists, phone books and telephone logs who may have been contacted by use of this device or by other means for the purpose of committing Subject Offense(s);
6. Voicemail messages, text messages, MMS messages, Emails whether stored, received, or deleted as they pertain to Subject Offense(s);
7. Photographs or images stored, sent, received or deleted, or documents containing photographs or images pertaining to Subject Offense(s);
8. Videos stored, sent, received or deleted pertaining to Subject Offense(s);
9. Electronic files, data, videos, and communications, including related metadata and location data, stored, sent, received or deleted from social media applications such as Facebook, Snapchat, Instagram, Twitter and/or any other third party programs or applications located on the device pertaining Subject Offense(s);
10. Communications through the (SELECT SIRI OR GOOGLE ASSISTANT) system, including all communications entered into the system as well as communicated from the system to the user pertaining to Subject Offense(s);
11. Global position system (GPS) data and any other geolocation data pertaining to Subject Offense(s);
12. Records of internet activity, including internet protocol (IP) addresses and Port IDs, firewall logs, transactions with internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses pertaining to violations of the law or that show who used, owned, possessed, or controlled the device(s) pertaining to Subject Offense(s);
13. The passwords and usernames for any accounts, cloud-based storage accounts or applications which are accessible through the above-identified digital device(s);
14. Any electronic files or data stored, sent, received, or deleted from social media applications, pertaining to Subject Offense(s) which allow for the posting of information or the communication between parties, including but not limited Facebook, Snapchat, Instagram, and Twitter.

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST.

Items which are evidence of violations of the Colorado Uniform Controlled Substances Act, C.R.S. §18-18-405.

The grounds for this Search Warrant are set forth in the accompanying Affidavit for Search Warrant, a true and correct copy of which is attached hereto and is incorporated herein by reference. These grounds establish probable cause to believe that the above-referenced cellular telephone(s)have been utilized to facilitate the illegal trafficking of controlled substances in northern Colorado, and that there is probable cause to believe that these cellular telephones contain evidence of violations of the Colorado Uniform Controlled Substances Act, C.R.S. §18-18-405.

The Court hereby finds probable cause to believe that the requested items constitute property which is designed or intended for use as a means of committing a criminal offense, or which have been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, pursuant to C.R.S. § 16-3-301 and C.R.S. § 16-3-301.1.

Therefore, any member of law enforcement agency or a designee, and/or a computer forensic lab, are commanded to:

* If not already in possession of the device, seize the aforementioned device within 14 days of the date this warrant is signed;
* Access the aforementioned device and view, copy and maintain the above described data contained therein;
* Use and employ such force as may reasonably be necessary in the performance of the duties described herein;
* The ability to use whatever means necessary to override any encryption or secure files encountered during the forensic examination of the phone, which may be destructive to the equipment. This could include having the item transferred to specialized forensic laboratories outside of the jurisdiction and/or the State of Colorado, if necessary.
* The ability to repair the device, replace the screen, replace the chassis, reconnect wires, or replace a battery. I also understand that it may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes including potentially destructive and destructive processes such as gaining root and/or Super user level access, JTAG, ISP-JTAG and chip-off.
* The ability to enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imagining, and analysis of any and all of the information described.
* Deliver to the person from whom the property is taken a copy of this warrant together with a receipt for the property taken, or to leave a copy of the warrant and receipt at the place from which the property was taken;
* Make prompt return of this search warrant, accompanied by a written inventory describing the physical storage media that was seized or copied, to the undersigned judge.

IT IS FURTHER ORDERED:

1. That this Search Warrant and Order and application be **SEALED** until the filing of charges based on this law enforcement criminal investigation, that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Order to be served on any service provider or other person. After charges are filed, disclosure of this Search Warrant and Order and application is governed by Crim. P. 55.1.

Based upon the affidavit of the above-named Affiant, which is incorporated by reference, I am satisfied that there is probable cause to believe there is a legal basis and also legal authority for the issuance of this Search Warrant. You are therefore authorized to execute this Search Warrant according to these terms and as otherwise permitted by law.

Dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_am/pm.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge/Magistrate

COUNTY OF LARIMER )

) SS IN THE COMBINED COURT

STATE OF COLORADO )

**RETURN OF SEARCH WARRANT FOR CELLULAR TELEPHONE(S)**

Pursuant to section C.R.S. § 16-3-301 and C.R.S. § 16-3-301.1, the undersigned law enforcement officer has executed the accompanying Search Warrant by searching and acquiring the data from:

**CELL PHONE DESCRIPTION**

**ADD PHOTO OF PHONE IF AVAILABLE**

**ADDRESS WHERE PHONE IS LOCATED**

within the County of Larimer and State of Colorado. All evidentiary items seized from the cellular telephone has been logged into Fort Collins Police Services evidence under **CASE NUMBER.** Attached to the Return of Search Warrant is the original Search Warrant.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

LEO OFFICER

Dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_am/pm.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Notary Public

Subscribed and sworn to before me this day of \_\_\_\_\_ ­­­\_\_\_\_\_, 20\_\_\_, at \_\_ .

My commission expires: