\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INSTRUCTIONS\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-This search warrant mask is specifically for the search of AT&T Mobility for call detail records and associated data

-There is RED text below that needs to be changed based on the needs of your search warrant.

-There is BLUE text below which is provided for information to the reader about what is being requested and why. Make sure you read this information and understand it since you are putting it your search warrant. You may need to adjust some of the wording or content in these areas to the specifics of your case.

- After the warrant is finalized, highlight all of the text by selecting CTRL+A and then change all text to black

-It would be a good idea to delete this section before printing/sending your warrant to get signed.

AT&T - Includes Cricket

|  |
| --- |
| https://s3-us-west-2.amazonaws.com/trax-images/carrier-info-logo/att_logo.png |

11760 US Highway One, 6th Floor

North Palm Beach, FL 33408

Compliance Center - 800-635-6840

Compliance Fax - 888-938-4715

Call Detail Records (without cell site info) - 7 year retention  
Call Detail Records (with cell site info) - July 2008 to present  
Data Records (with cell site info) - 6 months  
Tower Dumps - 60 Days  
SMS Detail Records\* - 1 year  
     \*AT&T does not provide text content  
Historical GPS locations - 1 year  
Real Time Locate - Every 15 minutes by email

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*PLEASE DELETE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Case No:

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS**

BEFORE THE HONORABLE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

JUDGE / MAGISTRATE

Affiant, YOUR NAME HERE, a commissioned law enforcement officer, being duly sworn, deposes and states that I have probable cause to believe that at the place or business entity known or described as:

**AT&T Mobility**

**11760 US Highway One, Suite 600**

**North Palm Beach, FL 33408**

**Via fax: (888) 938-4715**

There is now located within or upon said premises, or in the actual or constructive control of said business, certain records which would be material evidence in a subsequent criminal prosecution in this state or another, namely:

All records associated with mobile number PHONE NUMBER **(Target Telephone Number)** for the dates of DATE OF INTEREST to DATE OF INTEREST, namely:

1. **Specialized Location Records:** All call, voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the **Target Telephone Number**.
2. **Call/Text/Data Detail Records:** All records associated with the **Target Telephone Number** also to include all numbers that communicate with this listed number relating to all delivered and undelivered inbound and outbound calls, text messages, and text message content to any of the above listed numbers, all voice mail, and all data connections**,** and to include Cell-site and sector, date, time, direction, duration, number called or text to and/or received from, and bytes up/down, information related to each call, text or data connection, all text message content, and voicemails, as well as Call to Destination/Dialed Digits search for all numbers listed above. Please preserve all cell-site and sector information related to each call, text or data connections.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the **Target Telephone Number** related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, and whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** All cell-site and sector information related to each number called to and/or received from, and data connections, specific to the **“Time on Tower and/or Sector”**, to include information with the start and end date and time for each time the connection was involved in a **“hand-off”** to another cell-site and/or sector, to include the elapsed time (in seconds) for each **“hand-off”**, that was used during and throughout each voice call (whether completed or not), and which was used during and throughout each data session.
5. **Electronically Stored Records:** All records associated with the **Target Telephone Number** to include all stored communication or files, including voice mail, text messages, including numbers text to and received from and all related content, e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, (IP) Session data, (IP) Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed), date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with the cell identified number.
6. **Carrier Key** related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information.
7. **Cloud Storage**: Content stored in remote storage or ‘cloud accounts’ associated with the target device including, but not limited to, contacts, call logs, SMS and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
8. **Cell Site List(s):** List of all cell-sites as of for all state(s) in which the above records used cell locations. Cell site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, azimuth, and beam-width of each related sector. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records, all appropriate corresponding cell site lists will also be provided.
9. **Subscriber Records:** All information for the identified mobile number including:
   1. All Subscriber information to include name, tax identification number (social security number or employer identification number).
   2. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
   3. Credit information obtained or used by the company to grant account status.
   4. All numbers associated with account.
   5. Billing records.
   6. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
   7. All Authorized users on the associated account.
   8. Activation date and termination date of each device associated with the account and above listed number(s).
   9. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
   10. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed numbers including any and all equipment or sim card changes for the life of the account.
   11. All customer service and account notes.
   12. Any and all number and/or account number changes prior to and after the cell number was activated.
   13. Any other records and other evidence relating to identified mobile number.
   14. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.
10. **IMEI Search:** The Service Provider(s)/wireless carriers shall conduct an IMEI inquiry of the corresponding **Target Telephone Number** IMEI(s) to determine all IMSI/cellular telephone numbers utilized with the aforementioned devices (IMEI) for the same time period described above.
11. **IMSI Search:** The Service Provider(s)/wireless carriers shall conduct a search of the IMSI information corresponding to Target Telephone Number and provide IMEI history information for all devices identified to include all associated IMSI/cellular telephone numbers for those devices for the same time period described above.

For which a search warrant and court order for production of records may be issued upon one or more of the grounds set forth in 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1, §16-3-303.5 and Crim. P. 41, namely that this property is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state, or the seizure of which is expressly required, authorized or permitted by any statute of this state, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant is outstanding.

The facts tending to establish the grounds for issuance of a Search Warrant are as follows:

BACKGROUND OF AFFIANT

STATEMENT OF PROBABLE CAUSE REGARDING CRIME BEING INVESTIGATED – OR IF FOR FUGITIVE PURPOSES, EXISTENCE OF OUTSTANDING WARRANT – AND PC TO BELIEVE THE ACCOUNT LISTED IS AN ACCOUNT THAT COULD LEAD TO MATERIAL EVIDENCE OR A FUGITIVE MIXED WITH THE BELOW PARAGRAPHS

I have a general understanding of how the cellular telephone network operates. I am aware that cell sites (towers) are strategically placed by cellular service providers, to provide a seamless operation so people can travel virtually anywhere and make or receive an uninterrupted call, send or receive text messages, or initiate a data session via their cellular phone. Usually, cell sites will be mounted high on a large pole, building, or other structure which provides line of sight with the population below. Cell sites are typically divided into sectors, which are made up of antennas connected to cellular radio transceivers. Each sector is mounted on the cell site and faces a specific direction to provide maximum cellular coverage for the people in the area. The range of the cell site and sectors depends on many factors to include environmental and geographic factors and whether it is located in a highly populated, urban environment or desolate rural area. Cell site location information (CSLI) does not provide an exact location of a cell phone; the basic call detail record data only provides the physical location of the cell site (latitude and longitude) and a direction (azimuth) the antennas are facing from the cell site.

I am aware when a person either initiates or receives a voice call, text message, or a data session (usage event) from their cellular device, the device broadcasts signals to the cell site that routes its communications. These signals include a cellular device’s unique identifiers as well as details about the usage event. I am also aware cellular service providers collect and store these usage event details (transaction records) associated with cellular phone numbers during the normal course of business. The usage event records, commonly referred to as call detail records, stored by their respective cell phone company, mostly contain the following information with some exceptions based on the specific carrier: Date, time, type of event, duration, phone number initiating the usage event (called, calling), even if caller identification is blocked by the calling party, text message transaction data, the international mobile equipment identifier (IMEI), the international mobile subscriber identifier (IMSI), IP packet data session logs, and cell site location and sector information at the beginning and ending of each usage event.

I believe such information is relevant and material to the ongoing criminal investigation as it may provide investigators with information supporting or refuting the suspect’s alibi, and assist with determining other unidentified co-conspirators, and/or show the general geographic location of the target device before, during, and after the commission of the crime. This is basic information and does not provide an exact location of the person’s cell phone nor does it identify the other parties.

I am aware that obtaining and preserving historical cell phone call detail and specialized location records could also prove to be fruitful, as such records could assist investigators not only with identifying those who may have been in contact with the victim(s) or potential co-conspirators, but may also allow investigators other opportunities, including, but not limited to, confirmation or the disproving of alibis, statements, and other observations.

I know that these records such as those associated with the target phone, are not kept or preserved indefinitely by the cellular service providers and are purged at different intervals. Obtaining and preserving these records at this point in the investigation will ensure the investigators assigned to the case will have them available, and if the case were to go “cold”, future investigators will have access to the records which would otherwise likely not be obtainable. Not only could the preserved records assist in proving one’s guilt, they could also assist in proving one's innocence.

**Specialized Location Records**

I am aware cellular service providers maintain specialized location records consisting of engineering data.  These data sets are used by the providers to troubleshoot coverage areas and report back on potential dead spots, all with the intent to oversee and optimize the cellular network.  Specialized location records typically contain data for every usage event, to include technology details (e.g. voice, text, data), resource usage, and call failure information.  They can also include data for incomplete calls (e.g. denied calls and set-up failures).  These records not only include the basic call detail records, but also an estimation of the target phones location (Latitude and longitude) with a possible accuracy radius, and/or the distance from the cell site at the time of the usage event.  Utilizing specialized location records can provide investigators with a much smaller footprint of a target phones location and could place a target phone within close proximity of a crime scene before, during and after a crime.  Each carrier uses their own nomenclature to describe the technology used to obtain this data including: LOCDBOR (Location Database of Record) – AT&T, RTT (Round Trip Time/Return Trip Time/Real Time Tool) - Verizon & U.S. Cellular, PCMD (Per Call Measurement Data) – Sprint & U.S. Cellular, and TDOA (Time Difference of Arrival) or Timing Advance Information – T-Mobile & Metro by T-Mobile.  I believe this information is relevant and material to the investigation as it provides supplemental geo-location information which, while not precise enough to identify a specific house, is accurate enough to provide block-level accuracy, in some cases.  Investigators can use this information to correlate existing fact patterns and timelines to confirm or refute prior statements and/or evidence regarding the location of the target device.

**Call/Text/Data Detail Records & Electronically Stored Records**

I am seeking evidence of communication between identified subject(s) and previously unidentified individuals and entities. In my training and experience, associates communicate together via phone calls, text messages, and social media applications via data sessions and these communications most commonly occur on or through cellular devices.

In my training and experience individuals often use digital devices and cellular devices to post messages to others on social networking applications. In my training and experience it is possible for cellular phone users to use a variety of messaging platforms including the cellular SMS and MMS technology, as well as third-party applications like Facebook Messenger, WhatsApp, Snapchat, iMessage, and many other applications. Therefore, I seek to search all the communication evidence maintained by the service provider.

I am also seeking evidence of association. I know that establishing the association of co-conspirators is important in proving a concert of action between multiple persons. In my training and experience, one of the most effective methods of linking co-conspirators together is by reviewing the call detail records maintained by the cellular service providers. In my training and experience, associates communicate together via voice calls, text messages and third-party applications by means of a data usage event, therefore I am seeking the call detail record evidence to demonstrate the associations of the individuals in this case. Because this evidence is intended to be used to show associations of the user/owner of the device and co-participants, I am seeking the above items regardless of the dates the information was created.

**Stored Data (Cloud Storage)**

I am aware cellular service providers offer their customers optional free or paid backup digital storage for some of the content stored on their device. These services are offered to secure and restore their digital information in the event their mobile device is lost or stolen. Because these digital storage services are remote and transparent to the consumer, they are often referred to as ‘cloud’ storage. Customers can elect to digitally store the contents of their electronic phone book including details of their contacts, names, phone numbers, email addresses, and other data, calendar events, short message service (SMS) messages, commonly referred to as text messages, multimedia message service (MMS) messages, consisting of pictures, videos, and/or audio files with or without accompanying text, call logs of incoming, outgoing, and missed calls, digital images and videos, music and audio files, and electronic files such as documents and spreadsheets. I believe this information is relevant and material to the matter at hand as the contents of the remote digital storage may contain information presently unavailable to investigators including: associated identifying information from the user’s contacts which would tend to identify possible suspect’s, witnesses, associates, and/or co-conspirators, the content of messages sent between those parties, digital images and videos which may contain evidence of the crime under investigation, and documents related to same.

**Cell Site List(s)**

I am aware cellular service providers maintain a master cell site list of all cell sites within their network. These cell site lists will include the specific switch, cell site number, name, physical address, latitude and longitude of the cell site, all sectors associated with each cell site, azimuth, and beam-width of each related sector. When reviewing call detail and specialized location records from the carriers, the records may only reference a specific switch, cell and sector, or LAC and CID/eNodeB ID, related to each usage event; they usually will not include the location (latitude and longitude) of the actual cell site and azimuth of the sector. It becomes necessary to reference a cell site list in order to plot the exact location of the cell site and to identify the azimuth of the sector used associated with specific usage events.

Also, in the course of the investigation and review of the call detail and specialized location records, it may become necessary to visualize all cell sites within a geographic region of interest, not just the cell sites used by the target phone. It is just as important to show cell sites not used by a target phone, as it is to show cell sites used. By obtaining the master cell site lists from the cellular service providers, investigators are able to plot all of the cell sites in a given region, helping investigators with disproving of alibis, statements, and other observations evidenced by the records.

**Subscriber Records**

I am seeking evidence of ownership, use, and identification of the subscriber, customer or owner of the electronic communication information contained in the records retained by the cellular service provider. I am aware, depending on whether the account is post-paid or pre-paid, a consumer must provide information to the cellular service provider. Post-paid accounts are credit based whereby a customer is provided service and then billed after the provision of services. These types of accounts require sufficient identifying information to enable the cellular service provider to make a determination regarding credit worthiness and recourse in the event the consumer defaults on their contractual agreement. The information required by most cellular service providers include the customer’s personal identifying information, verified using government issued identification or other means, residential address, alternate contact phone numbers, and electronic mail (email) address(es). Additional information can include the type of service plan, additional features subscribed to, such as cloud storage and additional phones on the same account, device type and unique identifiers including IMEI and IMSI, method and source of payment information including financial institution and direct billing checking account numbers, credit or debit card numbers, and/or third-party payment processors, and customer service representative account comments and notes. I believe this information is relevant and material to the matter at hand as it serves multiple purposes including: identifying the subscriber to the target phone number, providing investigators with additional information and leads including subscriber address, additional phone numbers, and/or email addresses, device identifiers used to correlate any seized phones with the account, previously unidentified phones subscribed to on the same account, and financial information. I know that ownership and control of a digital device can be placed at issue through a simple denial, "that is not my phone." In my training and experience some of the best ways to establish ownership and control are by reviewing account information and subscriber records from cellular service providers.

**Burner Phones**

I am aware of the ease of being able to purchase a pre-paid cellular phone, and how it has impacted law enforcement's effort when attempting to identify criminals and locate wanted felons. It becomes very difficult, sometimes impossible, to determine the identity of a subscriber when the pre-paid providers do not require the identity of the person when obtaining/purchasing a pre-paid cellular phone. From prior training and experience, I know of many cases where pre-paid phones were used by suspects to further facilitate their criminal behavior, with the intent of concealing their true identity. Despite the lack of personally identifiable information, prepaid accounts can still provide investigators with information to identify the user. By examining the call detail and specialized location records of a pre-paid target phone, investigators can examine call and text incoming and outgoing usage events to help identify co-conspirators, associates, friends and family, who could help identify the party utilizing the pre-paid phone. Additionally, pre-paid services typically require some mechanism of payment including pre-paid cards, cash payments at retail establishments, or via an online portal. The financial information may assist investigators with identifying the locations where the pre-paid cards were purchased, the location of the retail establishments used for cash payments, and/or associated online account information and Internet Protocol (IP) addresses.

Based on these facts, Your Affiant believes there exists probable cause to believe that there is material evidence now located in the above described **AT&T Mobility** account that is crucial to the investigation of this case and the offenses described above, and a search warrant is requested pursuant to 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1, and §16-3-303.5.

**AT&T Mobility** is a provider of electronic communication services subject to the Stored Communication Act (SCA), 18 U.S.C. §2703, et seq. The SCA permits a state court with jurisdiction over an offense to issue an extraterritorial warrant for production of electronic communication content and electronic communication records. 18 U.S.C. §2703(g) authorizes service of the warrant via methods other than in-person service by a law enforcement officer. It is the intent of this affiant, consistent with the SCA and the procedures established by **AT&T Mobility** for compliance with the SCA, to serve this warrant via fax and/or email or law enforcement portal.

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

***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.
2. So as not to disrupt this ongoing investigation, Your Affiant also requests that this Court order **AT&T Mobility** NOT to take adverse action against the subject account, such as disabling or terminating the account, because of this warrant.
3. Pursuant to 18 U.S.C. §2705(b) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), Your Affiant requests that **AT&T Mobility** be ordered NOT to disclose the existence of this search warrant and court order to the subscriber for a period of one year from receipt of the requested documents, unless otherwise ordered by a court of competent jurisdiction. Based on the information set forth in this affidavit, notification of the warrant may have an adverse result, as defined in 18 USC §2705(b)(1)-(5), i.e., disclosure may endanger the life or physical safety of an individual; allow flight from prosecution; allow destruction of or tampering with evidence; allow intimidation of potential witnesses; and/or would otherwise seriously jeopardize an investigation or unduly delay a trial.

I believe the above facts to be true from official LAW ENFORCEMENT AGENGY records, conversations with fellow officers, personal observations and interviews. I am a YOUR TITLE with the LAW ENFORCEMENT AGENGY. I have been trained at the State, and local levels with regard to my duties. I am authorized by law to execute search warrants in the County of Larimer and State of Colorado.

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

AFFIANT

This affidavit was sworn to and subscribed by telephone this DATE day of MONTH 20\*\* at \_\_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS**

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

Judge / Magistrate

The Court, upon review of an affidavit filed by YOUR NAME HERE which is incorporated by reference, in support of the issuance of this order, hereby orders the production of the following records, for which there is probable cause to believe are in the actual or constructive possession or control of the business entity known or described as:

**AT&T Mobility**

**11760 US Highway One, Suite 600**

**North Palm Beach, FL 33408**

**Via fax: (888) 938-4715**

This Court also finds that there is probable cause to issue this Search Warrant pursuant to the provisions of 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1, §16-3-303.5, and Crim. P. 41, namely that this property is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state or federal court, or the seizure of which is expressly required, authorized or permitted by any statute of this state or the United States, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant is outstanding.

IT IS ORDERED that the internet service/social media provider provide the following records, data, information and technical assistance:

All records associated with mobile number PHONE NUMBER **(Target Telephone Number)** for the dates of DATE OF INTEREST to DATE OF INTEREST, namely:

1. **Specialized Location Records:** All call, voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the **Target Telephone Number**.
2. **Call/Text/Data Detail Records:** All records associated with the **Target Telephone Number** also to include all numbers that communicate with this listed number relating to all delivered and undelivered inbound and outbound calls, text messages, and text message content to any of the above listed numbers, all voice mail, and all data connections**,** and to include Cell-site and sector, date, time, direction, duration, number called or text to and/or received from, and bytes up/down, information related to each call, text or data connection, all text message content, and voicemails, as well as Call to Destination/Dialed Digits search for all numbers listed above. Please preserve all cell-site and sector information related to each call, text or data connections.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the **Target Telephone Number** related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, and whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** All cell-site and sector information related to each number called to and/or received from, and data connections, specific to the **“Time on Tower and/or Sector”**, to include information with the start and end date and time for each time the connection was involved in a **“hand-off”** to another cell-site and/or sector, to include the elapsed time (in seconds) for each **“hand-off”**, that was used during and throughout each voice call (whether completed or not), and which was used during and throughout each data session.
5. **Electronically Stored Records:** All records associated with the **Target Telephone Number** to include all stored communication or files, including voice mail, text messages, including numbers text to and received from and all related content, e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, (IP) Session data, (IP) Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed), date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with the cell identified number.
6. **Carrier Key** related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information.
7. **Cloud Storage**: Content stored in remote storage or ‘cloud accounts’ associated with the target device including, but not limited to, contacts, call logs, SMS and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
8. **Cell Site List(s):** List of all cell-sites as of for all state(s) in which the above records used cell locations. Cell site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, azimuth, and beam-width of each related sector. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records, all appropriate corresponding cell site lists will also be provided.
9. **Subscriber Records:** All information for the identified mobile number including:
   1. All Subscriber information to include name, tax identification number (social security number or employer identification number).
   2. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
   3. Credit information obtained or used by the company to grant account status.
   4. All numbers associated with account.
   5. Billing records.
   6. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
   7. All Authorized users on the associated account.
   8. Activation date and termination date of each device associated with the account and above listed number(s).
   9. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
   10. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed numbers including any and all equipment or sim card changes for the life of the account.
   11. All customer service and account notes.
   12. Any and all number and/or account number changes prior to and after the cell number was activated.
   13. Any other records and other evidence relating to identified mobile number.
   14. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.
10. **IMEI Search:** The Service Provider(s)/wireless carriers shall conduct an IMEI inquiry of the corresponding **Target Telephone Number** IMEI(s) to determine all IMSI/cellular telephone numbers utilized with the aforementioned devices (IMEI) for the same time period described above.
11. **IMSI Search:** The Service Provider(s)/wireless carriers shall conduct a search of the IMSI information corresponding to Target Telephone Number and provide IMEI history information for all devices identified to include all associated IMSI/cellular telephone numbers for those devices for the same time period described above.

This warrant and court order for the production of records shall be served upon the business entity to whom it is directed within fourteen days after being signed by the court.

The business entity is ORDERED to produce the above described records to the affiant or his/her designee within thirty-five (35) days of service.

The records should be provided to:

YOUR NAME

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

The business entity shall also provide a notarized attestation of accuracy that the records produced represent complete and accurate copies of all records identified in this order that are in the actual or constructive control of the business entity. If the business entity does not produce all records identified in this order, it shall identify the records not produced. Failure to comply with this order shall support a finding of contempt of court.

Upon receiving the records from the business entity, the peace officer named herein shall file a return and inventory with the court indicating the records that have been received and the date and time upon which the records were received. The peace officer named herein may also file the original of the attestation of accuracy with the court.

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.
2. That AT&T Mobility NOT take adverse action against the subject accounts, such as disabling or terminating the accounts, because of this warrant.
3. Pursuant to 18 U.S.C. §2705(b) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), that AT&T Mobility, **NOT disclose the existence of this search warrant and court order to the subscriber for a period of one year**, unless otherwise ordered by a court of competent jurisdiction, as notification of the warrant may have an adverse result, as defined in 18 USC §2705(b)(1)-(5), i.e., disclosure may endanger the life or physical safety of an individual; allow flight from prosecution; allow destruction of or tampering with evidence; allow intimidation of potential witnesses; and/or would otherwise seriously jeopardize an investigation or unduly delay a trial.

THE INFORMATION SO ORDERED is related to the active and ongoing criminal investigation by YOUR AGENCY and in accordance with 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1, §19-2-504, and §16-3-303.5 the records and information requested are or have been used as a means of committing a criminal offense or would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court; the seizure of which is expressly required, authorized, or permitted by statute; or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

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 this **\_\_\_\_\_day of \_\_\_\_\_\_\_\_\_ 20\_\_**, at \_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE