|  |  |  |
| --- | --- | --- |
| IN THE CIRCUIT COURT OF {{COUNTY|upper }} COUNTY, MISSOURI | | |
|  | )  )  )  )  ) | Sikeston DPS: {{ CASE }} |
| STATE OF MISSOURI  COUNTY OF {{COUNTY|upper }} |
|  |  |  |
| **AFFIDAVIT AND APPLICATION FOR A SEARCH WARRANT** | | |

**INTRODUCTION AND AGENT BACKGROUND**

1. I, {{ NAME|title }}, knowing that false statements are punishable by law, hereby affirm and state that the facts contained herein are true to the best of my information and belief. Based on the following information, I hereby request the Court find probable cause and make this Affidavit in support of the issuance of a Search Warrant.
2. I am a {{ RANK|title }} with the {{AGENCY }}, located in the County of {{ COUNTY|title }}, State of Missouri. I am a “Peace Officer” as defined in RSMO § 542.261. I have been employed as a peace officer for more than {{ YEARS }} years. I have training pertaining to the investigation of criminal offenses and as part of my regular duties, I have previously participated in the investigation of various criminal offenses, including the offense which is currently under investigation and is the subject of this Affidavit.
3. I have been assigned to investigate a {{CRIME|title}}, a violation of RSMO § {{RSMO}}. The incident occurred in {{COUNTY|title}} County on or about {{MONTH|title}} {{DAY}}, {{YEAR}}.

**PERSON, PLACE, OR THING TO BE SEARCHED**

See Attachment "A"

**ITEMS TO BE SEARCHED AND SEIZED**

See Attachment "B"

**STATEMENT OF PROBABLE CAUSE**

1. {Type your probable cause statement here. Remember that you have to establish probable cause for what you want to search and also establish that it’s probable that the evidence you wish to search for will be at that location.}
2. Through the course of my investigation, I identified the service provider for the target telephone number following a query of an on-line law enforcement database. Such queries are commonly relied upon by law enforcement to identify a service provider for a particular telephone number. I then contacted the identified service provider and confirmed that they are the provider for the target telephone number. In this case the service provider is identified as

{%- **if** ATT -%}

AT&T Mobility

{%- endif -%}

{%- **if** TMOBILE -%}

T-Mobile

{%- endif -%}

{%- **if** USCELLULAR-%}

U.S. Cellular

{%- endif -%}

{%- **if** VERIZON -%}

Verizon Wireless

{%- endif -%}

.

**APPLICABLE LAW**

1. This search warrant is made pursuant to: 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), 2703(c)(2), 2705(b) and Missouri law.
2. That this Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants, 18 U.S.C. § 2711(3)(B). A District Court of the United States that has jurisdiction over the offenses listed above. 18 U.S.C. § 2711(3)(A)(i).
3. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.
4. Therefore, I am requesting a search warrant allowing the search of service provider(s) listed in Attachment A, public utility and mobile network operators, who provide services nationwide and in the State of Missouri, hereafter referred to as the “service provider”;

{%p **if** PRTT%}

**PEN REGISTER AND TRAP AND TRACE**

1. I know that cellular service providers have the technical capability to install and use both a Pen Register and a Trap and Trace Device. Pen Registers are used to register numbers that are dialed by a telephone and record the length of the call. A Trap and Trace Device is used in conjunction with a Pen Register to capture and record the telephone numbers of incoming calls. Together, these tools provide investigators with a more complete view of the people and businesses that the suspect is communicating with. It is important to note that Pen Register and Trap and Trace Device only record the telephone numbers and cannot capture call content. I also know that it is common for persons who are involved in criminal activity and suspect they may be the focus of a law enforcement investigation to transfer their telephone service to another phone number. This is frequently done in an attempt to thwart the investigation under the believe that the new telephone number will be difficult if not impossible to determine. I know through both training and experience that telecommunications providers track mobile phone through device identifiers such as Electronic Serial Number (ESN), International Mobile Subscriber Identity (IMSI), and International Mobile Equipment Identity (IMEI). Any attempt to transfer service to a different phone number or physical is recorded as the normal course of business and can be provided to law enforcement with a search warrant.

{%p endif %}

{%p **if** PING %}

**PHONE “PING”**

1. I know that cellular service providers have the technical capability to provide real time, or nearly real time, location information of the Target Account described in the search warrant pursuant to an order from this court. This location data, commonly known as a "ping", is extremely useful in law enforcement investigations in determining peoples locations, routes of travel, residences or business or locations that the person stops at. Live ping records are frequently used in surveillance situations where the suspect is difficult to follow either due to the open terrain they are crossing or due to counter surveillance techniques.

{% endif %}

**CELLULAR TELEPHONE TECHNOLOGY AND RECORDS – GENERALLY**

1. I have a general understanding of how cellular telephone networks operate. I am aware that cellular service providers strategically place cell sites (towers). The network is engineered to provide a seamless user experience and allow users to travel virtually anywhere and make or receive uninterrupted calls, send or receive text messages, and initiate a data session using their cellular phone. Usually, cell sites are mounted high on a large pole, building, or other structure that provides line of sight with the population below. Cell sites are also 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 users 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.
2. I am aware when a user 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.
3. Usage event records, commonly referred to as call detail records (CDR’s), stored by their respective cell phone company, typically 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). This data is collected even if caller identification is blocked by the calling party, text message transaction data, the International Mobile Equipment Identity (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.
4. 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.
5. 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 coconspirators, but may also allow investigators other opportunities, including, but not limited to, confirmation or the disproving of alibis, statements, and other observations.
6. 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 the 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 that 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.

**SUBSCRIBER RECORDS**

1. 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.
2. 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.
3. 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.

**PREPAID “BURNER” PHONES**

1. The term “burner phone” is a term commonly used to describe inexpensive cellular telephone that use pre-paid minutes and data and do not require identification or a credit check to activate service. I am aware of the ease of a user being able to purchase and use these phones and how it has challenged law enforcement efforts identify criminals, terrorist threats, and to locate wanted felons. It is 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 cases where pre-paid phones were used by suspects with the intent of concealing their actual identity. This facilitated their continued criminal actions and behavior.
2. Despite the lack of personally identifiable information, pre-paid 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.

**CALL DETAIL RECORDS**

1. 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.
2. 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 (Short Message Service – text messaging) and MMS (Multimedia Message Service – sending text messages with other files such as pictures) 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.
3. I am also seeking evidence of association. I know that establishing the association of coconspirators 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, I know that 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.

**SPECIALIZED LOCATION RECORDS**

1. I am aware cellular service providers maintain specialized location records consisting of engineering data. The data are used by the provider’s engineers to troubleshoot coverage areas and report 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, and data), resource usage, and call failure information. They can also include data for incomplete calls (e.g. denied calls and set-up failures).
2. 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 NELOS (Network Event Location System) – AT&T, RTT (Round Trip Time/Return Trip Time/Real Time Tool) - Verizon, PCMD (Per Call Measurement Data) – Sprint & U.S. Cellular, and TruCall®, TDOA, Time Distance of Arrival, and MDT GPS – T-Mobile USA & Metro by T-Mobile.
3. 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.

**CLOUD STORED DATA**

1. 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.
2. 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.

**ORDER TO PRODUCE ADDITIONAL SUBSCRIBER RECORDS**

1. I request the service provider, and all other telecommunications service providers, be ordered to provide subscriber details for all telephone numbers identified by the target telephone call detail records returned by such in response to this search warrant as either calling or receiving calls associated with the target telephone number, and/or sending or receiving text messages associated with the target telephone number.
2. Subscriber records are records kept during the normal course of business. Subscriber records are necessary to identify with whom the suspect has been communicating. The subscribers identified by these records may be yet unidentified witnesses, victims, or co-conspirators. Quickly identifying these individuals is important to preserve exculpatory and inculpatory evidence. Additionally, this process may be necessary because of number portability (transfer to another service provider) and/or if the original carrier is modified due to roaming and/or other consideration(s)/reason(s.).

**PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENT ACCESS**

1. As allowed per 18 U.S.C. § 2705(b), I request the service provider be ordered to NOT notify any other person of the existence of the warrant and subsequent records access by law enforcement for a period of at least 90 days.
2. This criminal investigation is ongoing, and it is likely that information and evidence obtained in the course of the service of this search warrant will result in further information concerning the identity and involvement of suspects in this case. As such, disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify co-conspirators, and flee from apprehension and prosecution.
3. Alerting the subscriber, customer or owner of the electronic communication information to which the materials relate, to the existence and service of this search warrant may have an adverse result, to include endangering the life or physical safety of an individual, flight from prosecution, destruction of, or tampering with, evidence, intimidation of potential witnesses, or otherwise seriously jeopardize the investigation or unduly delay a trial.
4. I have read this affidavit and the facts contained in here are the truth to the best of my knowledge.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Affiant)

{{ RANK|title }} {{ NAME|title }}

{{ AGENCY }}

DATE: {{ TODAY }}   
TIME:

I have reviewed this Affidavit and Application and hereby apply for a search warrant based upon this Affidavit and place my signature upon this Application.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Prosecuting Attorney)

DATE:

TIME:

Witness my hand and the seal of this Court on {{ TODAY }}.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Judge)

DATE:

TIME:

|  |  |  |
| --- | --- | --- |
| IN THE CIRCUIT COURT OF {{COUNTY|upper }} COUNTY, MISSOURI | | |
|  | )  )  )  )  ) | Sikeston DPS: {{ CASE }} |
| STATE OF MISSOURI  COUNTY OF {{COUNTY|upper }} |
|  |  |  |
| **SEARCH WARRANT** | | |

**THE STATE OF MISSOURI TO ANY PEACE OFFICER IN THE STATE:**

**WHEREAS**, proof having been made before me by {{ RANK|title }} {{ NAME|title }}, the Judge of this Court has found probable cause to believe the allegations of the complaint to be true and that there is probable cause to believe that evidence pertaining to {{CRIME|title}}, a violation of RSMO § {{RSMO}} is presently located at the location(s) described herein.

**YOU ARE COMMANDED TO SEARCH THE FOLLOWING LOCATION(s):**

See Attachment "A"

**FOR THE FOLLOWING PROPERTY OR PERSON(s):**

See Attachment "B"

**NOW, THEREFORE**, you are directed to execute this search warrant, to seize, photograph, or copy the property, article, substance, or person found thereon or therein, and make return of this warrant to this court within ten (10) days after filing.

Witness my hand and the seal of this Court on {{ TODAY }} at \_\_\_\_\_\_\_\_\_ AM / PM.

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

Circuit / Associate Circuit Judge

TIME:

**ATTACHMENT "A"**

**TO MAKE A SEARCH OF:**

**Any telecommunications company providing service to the target account(s), target device(s), or subjects identified by this warrant**, including, but not limited to:

{%p **if** ATT %}

**AT&T Mobility LLC (“AT&T Wireless”)**

Attn: Global Legal Demand Center

11760 U.S. Highway 1

North Palm Beach, Florida 33408

Fax No. (888) 938-4715

Email: gldc@att.com

{%p endif %}

{%p **if** VERIZON %}

**Cellco Partnership**

**DBA Verizon Wireless**

Attn: Verizon Security Assistance Team

180 Washington Valley Road

Bedminster, New Jersey 07921

Fax No. (888) 667-0028

Email: [vsat.cct@verizon.com](mailto:vsat.cct@verizon.com)

{%p endif %}

{%p **if** USCELLULAR %}

**United States Cellular Corporation**

**(“U.S. Cellular”)**

Attn: Subpoena Compliance Center

8410 West Bryn Mawr Avenue, Suite 800

Chicago, Illinois, 60631

Fax No. (866) 669-0894

Email: subpoenacompliance@uscellular.com

{%p endif %}

{%p **if** TMOBILE %}

**T-Mobile US, Inc. (“T-Mobile”)**

4 Sylvan Way

Parsippany, NJ 07054

Fax No. (973) 292-8697

Routine Email: *LERinbound@T-Mobile.com*

Exigent Email*:* [*ler3@t-mobile.com*](mailto:ler3@t-mobile.com)

{%p endif %}

**End of Attachment "A"**

**ATTACHMENT "B"**

FOR THE FOLLOWING RECORDS:

Records from the above listed Service Provider for the Phone Number: **{{ PHONENUMBER }}**

Each of the types of records specified below shall be for the period of {{ STARTDATE }} to {{ ENDDATE }} for evidence related to the crime(s) of: {{CRIME|title}},.

**Subscriber Information:** Subscriber information to include name, address, phone number, contact information, billing address, service address, email address, and phone numbers, payment information such as the payment card or bank account information; information related to a credit application for Services, Social Security number, driver's license number or other government issued identifier, passwords, images, or other personal identifiers, additional accounts, custom settings or preferences, and dates associated with account creation and/or suspension for the listed Target Account(s).

**Call Detail Records:** All records associated with the identified Target Number, also to include all numbers that communicate with these listed numbers relating to all delivered and undelivered inbound and outbound calls to of the above listed numbers, all voice mail, and all data connections for the dates listed above and to include Call to Destination / Dialed Digits search for all numbers listed above.

Originating date and time and ending date and time of cell site/sector, beginning and ending location for each call, Location Area Code (LAC), Cellular Identification (CID), Voice Over LTE (VOLTE) Call Detail Records, VOIP Call Detail Records, Per Call Measurement Data (PCMD), Range To Tower (RTT-EVDO) Data, Network Event Location System (NELOS) switch information, latitude, longitude, orientation, sector, azimuth, beam width, direction and strength of signal from the cellular tower.

The Call Detail Records should include all inbound and outbound calls, direct dispatched number(s), whether published or non-published, blocked or un-blocked, including SMS and MMS text message history with content and cell sites which have been accessed, sent, stored and received, all Voicemail, text and data content stored on the server, direct connect record with cell sites, picture detail and picture content, historical GPS with latitude and longitude coordinates, IP address login information for data sessions and Source and Destination Port Information for those logins, to include cell site/sectors (physical address), orientation, facing, offsets, and period of telephone activation and or registration for the Target Telephone(s). It is requested that the provided records indicate the time zone of the associated dates and times and that records be adjusted to CST and, if practical, a "cheat sheet" or document outlining how to decipher said Call Detail Records.

**Device Information:** Records of the device(s) used by the Target Account to access the service provider’s services. The records shall include the following Device attributes if available; operating system information, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins; Device operation information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements; Unique identifiers, device IDs, and other identifiers from games, apps or accounts you use, or other identifiers unique to service products associated with the same device or account; network and connection information such as the name of the mobile operator or ISP, language, time zone, mobile phone number, and IP address.

**Internet Access Records:** Internet access records for the Target Numbers. These records are to include all assigned IP addresses, date, time, duration and data usage amounts as well as information collected about the IP addresses visited by the Target Account. These IP records shall include the associated PORT number if available.

{%p **if** PING%}

**Ping Records:** Global Positioning System (GPS) Precision Location, E-911 Precision Location, and geographic location information available to the service provider through signal tracking or pinging. The service provider shall initiate a signal to determine the location of the subject's mobile device on their network or with such other reference points as may be reasonable available. This information should be provided upon the request of a law enforcement officer. Once the precision location identifier has been requested to be activated, it should be updated either every 15 minutes or in an agreed upon interval and continue for a period of 30 days, or until asked to cancel the monitoring by a representative of the agency executing this warrant. The request to activate the identifier shall be conducted via telephone, fax or email to the service provider.

{%p endif %}

**Purchase and Business Records:** Records of the purchases identified as the Target Accounts to include receipts, records of items purchased and the associated dates and times of transactions, transaction identifiers, copies of financial instruments such as checks or provided credit card information, stored signatures such as purchase approvals, and unique identifiers of the purchased items such as device serial number, IMEI, IMSI, or UCCID or the phone number associated to purchased service.

**Specialized Location Records:** Records of call, text and data connection location information with the identified Target Numbers. Including, all specialized carrier records that may be referred to as RTT (Real Time Tool), PCMD (Per Call Measurement Data), Network Location Services (NELOS), Mediation Records, e911, 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 above referenced numbers.

**Stored Communication Records:** Stored communications associated with the identified Target Numbers for the above listed Call/Text/Data Detail Records, specifically including all text message content, voicemails, and other stored communications.

**ADDITIONALLY AUTHORIZED COURT ORDERS:  
Authorization to implement special procedure(s):** The Affidavit filed herewith has demonstrated legal justification for the implementation of the following special procedures which shall be employed by the officers who execute this warrant:

**AUTHENTICITY OF RECORD ORDER**

IT IS HEREBY ORDERED that the Service Provider listed in the Attachment(s) shall provide a valid "Authenticity of Records" document consisting of an affidavit and that the document be returned to the Affiant along with a copy of the requested records.

**FIVE DAY RECORD PRODUCTION ORDER**

IT IS HEREBY ORDERED that the organizations described in this search warrant shall produce the requested records within five (5) days of receipt of this search warrant.

**ASSOCIATED NUMBERS ORDER**

IT IS HEREBY ORDERED that, based upon probable cause, the service provider shall provide the following information and services for the account associated with the Target Telephone Number(s). The information and services requested within this Search Warrant not only applies to the original Target Telephone Number(s), but also includes telephone number(s) subsequently assigned to the same handset, SIM card, and/or subscriber. Additionally, the information and services requested in this Search Warrant not only applies to Service Provider, but to other telecommunications carrier that provides service to the Target Telephone Number(s) due to roaming agreements and/or changes in service.

**CARRIER KEY AND CELL SITE LIST ORDER**

IT IS HEREBY ORDERED that the service provider shall provide Officers or their representatives with Carrier Key records related to call detail, text messages, data connections, and cell site information as well as a list of all cell-sites within the geographic area of the Target Account's locations as of the dates indicated in the search warrant to include switch; cell-site number, name, physical address, longitude and latitude, direction and signal strength; all sectors associated with each cell-site, azimuth, beam-width of each related sector; call progress locations (Automated Message Accounting (AMA) Data), dial digit information and extended digit dialing, and a listing of all control channels and their corresponding cell sites for the Target Telephone Numbers, including local and "roam" mode cellular telephone calls, historical data including incoming or outgoing calls, along with the subscriber information for the telephone numbers.

{%p **if** PING%}

**PING ORDER**

IT IS HEREBY ORDERED that the service provider shall initiate a signal to determine the location of the Target Account's mobile device on their network or with such other reference points as may be reasonable available.  The locations determined by this signal shall be provided at such intervals and times as directed by the law enforcement agent serving this order for a period of (30) days from the execution of this order.

{%p endif %}

{%p **if** PRTT %}

**PEN REGISTER AND TRAP TRACE ORDER**

IT IS HEREBY ORDERED that AT&T shall initiate the installation and use of a Pen Register to register numbers dialed or otherwise transmitted from the Target Account(s) described in the search warrant, and to record the date and time of such dialings or transmissions, and to record the length of time the telephone receiver in question is "off the hook" for incoming and outgoing calls, and to include direct connect "dispatch", if applicable; and shall initiate the installation and use of a Trap and Trace Device, including the caller identification feature, on the Target Account(s) described in the search warrant to capture and record the incoming electronic or other pulses which identify the originating numbers of wire or electronic communications, and to record the date, time, and duration of calls created by such incoming impulses and to include direct connect "dispatch" with the understanding that tracing operations including the use of the "caller identification feature" be without geographical limits.

IT IS FURTHER ORDERED that the installation and use of a pen register and trap and trace device, including the "caller identification feature," shall also apply to changed telephone number(s) subsequently assigned to an instrument bearing the same ESN or IMSI as the device currently associated to the Target Account(s) described in the search warrant, or changed ESN or IMSI subsequently assigned to the Target Account(s) described in the search warrant, or an additional changed telephone number(s) and/or ESN whether the changes occur simultaneously or consecutively, listed to the same subscriber and wireless telephone account currently associated to the Target Account(s) described in the search warrant.

IT IS FURTHER ORDERED that the use of both the Pen Register and Trap and Trace shall be for the period of thirty (30) days from the execution of this order unless the Affiant or a representative of the Sikeston Department of Public Safety contacts AT&T requesting their use be ended prior to the expiration of this Order.

{%p endif %}

**PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENT ACCESS**

IT IS FURTHER ORDERED, that the service provider, the service provider, in accordance with 18 U.S.C. § 2705(b) “Delay of Notice” will NOT notify any other person of the existence of this warrant and any access of account records by law enforcement. This order is in effect for no less than 90 days from the date the warrant is issued.

**PRODUCE RECORDS IN AN ELECTRONIC FORMAT**

IT IS ALSO FURTHER ORDERED, that the records provided by the service provider in response to this search warrant shall be provided in an electronic format (Excel, Word, PDF, or TXT) by electronic mail (e-mail) to **{{ NAME|title }}** at **{{ EMAIL }}**.

**End Attachment “B”**