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

-This search warrant mask is specifically for the search of Facebook for all data associated with the identified account name, pen registry and location 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.

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

Case No:

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**AFFIDAVIT FOR SEARCH WARRANT AND EX PARTE COURT ORDER AUTHORIZING USE/INSTALLATION OF A PEN REGISTER AND TRAP AND TRACE DEVICE, GEOGRAPHICAL LOCATION INFORMATION, AND AUTHORIZING RELEASE OF SUBSCRIBER INFORMATION**

## 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:

**Facebook, Inc.** (internet service/social media provider)

**Facebook Security LE Response Team**

**1601 Willow Road**

**Menlo Park, CA 94025**

**Served via https://facebook.com/records**

The following records, data, or information for Facebook User identified as ACCOUNT NAME **(hereinafter known as the “subject account”)** between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE(S):

* All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
* Additional Facebook accounts that were registered to the email address and/or phone number(s) utilized to establish the accounts;
* All Accounts associated by device or cookie: to include User ID, subscriber name, cellphone number and email address.
* All devices(s) used and otherwise associated with the subscriber’s accounts – ESN, ICCID, IMSI, IMEI numbers and activation dates;
* All activity logs for the accounts and all other documents showing the user’s posts and other Facebook activities;
* All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them and any associated metadata [camera make, model, capture date and time, capture latitude and longitude, etc.] and original sized image associated with those images and videos;
* All profile information; news feed information; status updates; links to videos, photographs, articles, and other items; notes; wall postings; friend lists, including past and present friends along with the associated friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook identification number(s) and Facebook identification number(s) of all group or network members; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;
* All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending “Friend” requests;
* All “check ins” and any other location information, including location history data;
* All Future and Past “events” the user responded to;
* All IP logs and associated port IDs, including all records of the IP addresses that logged into the accounts;
* All records of the account’s usage of the “Like” and “Follow” features, including all Facebook posts and all non- Facebook webpages and content that the user has “liked” and/or “followed”;
* All records of the account’s usage of the “Share” feature, including all Facebook posts and all non- Facebook webpages and content that the user has “shared”;
* All information about the Facebook pages that the accounts is or was a “fan” of;
* All records of Facebook searches performed by the accounts;
* All information about the user’s access and use of Facebook Marketplace;
* The types of service(s) utilized by the user, the length of service(s) (including start date), and the means and source of any payments associated with the service(s) (including any credit card or bank account number);
* All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the accounts;
* All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook accounts, including contacts with support services and records of actions taken.

For which a search warrant and court order may be issued upon one or more of the grounds set forth in 18 U.S.C. §2703 (Stored Communications), 18 U.S.C. §§3122 and 3123 (Pen Register and Trap and Trace), C.R.S. §16-3-301 (Search Warrant), §16-3-301.1 (Production of Records), §16-3-303.5 (Location Tracking), and Crim. P. 41 (Search Warrant), 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.

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

**Electronic Definitions**

“Internet” means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are physically located in the same state.

“Computers”, “digital media storage”, or “digital storage devices” may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

Internet Service Providers “ISP’s” or Electronic Service Providers “ESP’s” are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “email address,” an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password.

“Internet Protocol Address” or “IP address”: Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of numbers separated by periods; an example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP’s customers or subscribers. Most ISPs employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next customer. On the other hand, some ISPs, including most cable providers, employ static IP addressing, that is a customer or subscriber’s computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer. A modem is an electronic device that allows one computer to communicate with another.

Social Media: In general, social media may be defined as websites and applications that enable users to create and share content or to participate in social networking.

IMEI: IMEI (International Mobile Equipment Identity) is a unique identification number that identifies mobile devices.

IMSI: An international mobile subscriber identity (IMSI) is a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber.

Cookie: A cookie is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application. One purpose of a cookie is to save log in and password information for an account. It also serves the purpose of saving user preferences for a site, such as a search engine saving a search or a news website saving a certain font you prefer.

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 FACEBOOK ACCOUNT LISTED IS AN ACCOUNT THAT COULD LEAD TO MATERIAL EVIDENCE OR A FUGITIVE MIXED WITH THE BELOW PARAGRAPHS

Your Affiant is aware from prior experience that nearly all user-initiated Facebook activity, including the posting of images, status updates, the sending of messages, etc., is associated with an Internet Protocol (IP) address. This IP address would assist your affiant in finding the geographic location from which any messages made by the subject were posted, to include if these messages are sent with a mobile device. Your Affiant is also aware mobile devices connected to a Facebook account can sometimes store location data associated with the device’s Facebook activity. Your Affiant believes obtaining the records requested in this affidavit will help identify from which mobile or wireless networks the subject, or anyone with access to his Facebook profile, is in fact accessing that profile. This information would help identify his current location, establish a pattern of movement while on the run, identify anyone he may be staying with or associating with, aid in his apprehension, and further the investigation named in this affidavit.

Your Affiant knows from information from other officers and experience that Facebook honors Pen Register/Trap and Trace Orders for a Facebook profile. Information the company could forward Your Affiant could include IP address logs, “message headers,” login activity, and location information associated with any device used to log into Facebook.com. Facebook can provide such information to Your Affiant via Your Affiant’s given email address on an as-needed basis, depending on the facts of a given case.

Your Affiant believes that message headers (NOT message content), all Internet Protocol (IP) address logs, last known locations, location histories, and the installation of a pen register and trap and trace device on the subject accounts will assist in locating the subject. The information requested in this affidavit is necessary and relevant to the investigation and will assist in locating the subject.

In the experience of Your Affiant, the message headers (NOT message content), all Internet Protocol (IP) address logs, last known locations, location histories, and the installation of a pen register and trap and trace device has yielded information in past investigations that is relevant and material to criminal/fugitive investigations. Such information included leads relating to the general location of the subject account holder, and the names of family members, associates and other individuals who can assist in the apprehension of the subject, or identities of anyone who may aid in the flight and/or harboring of the subject. Your Affiant further states that, based upon his training and experience, one method to identify associates is to obtain account information for messages made to and from the subject accounts and then conduct an investigation related to those names and addresses. Based upon the subscriber information, Your Affiant would then direct other investigators to monitor the addresses and determine if the subject is present or if the associates may lead investigators to the subject.

Your Affiant further advises the Court that the general geographic location of the subject derived from message headers (NOT message content), all Internet Protocol (IP) address logs, last known locations, and location histories can be used to corroborate the observations of surveillance agents. More specifically, surveillance agents can compare observations of the general area in which the subject accounts are accessed to determine if the subject is in the area.

**Description of Facebook**

Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com and/or a proprietary software application installed on a device. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user’s full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make some information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and/or administrator, as well as a PDF of the current status of the group profile page.

Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the state to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s “Neoprint,” IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

**Your Affiant further advises this Court that the installation and use of a pen register and trap and trace device on the subject account will in no way allow the active, real-time monitoring of any content or conversation(s).**

1. IT IS REQUESTED that a pen register be installed by the internet service/social media provider on the subject accounts, to register subject accounts, to record message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories, for a period of sixty (60) days from the date the warrant is served upon Facebook, or until such time as the investigation is completed, whichever comes first.
2. IT IS REQUESTED that the internet service/social media provider, pursuant to probable cause, shall provide, on an ongoing (**NOT real-time**) basis, the following information relating to the subject accounts: message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories, beginning from the date the warrant is served upon Facebook, and continuing for the sixty (60) day time period, or until the investigation is completed, whichever comes first.
3. IT IS REQUESTED that the internet service/social media provider shall authorize and provide YOUR NAME HEREongoing (**NOT real-time**) access to the following information relating to the subject accounts: message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories related to the pen register/trap and trace device, some of which is only available to such authorized users, **sent to** YOUR NAME HERE **daily (once every 15 minutes) via the email address** YOUR EMAIL ADDRESS**, beginning from the date the warrant is served on Facebook, Inc. and continuing for the sixty (60) day time period, or until the investigation is completed, whichever comes first.**
4. IT IS REQUESTED, pursuant to 18 U.S.C. § 2703, that the internet service/social media provider shall furnish to law enforcement information including message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories, unobtrusively and with minimum interference with the services that are accorded the persons whose transmissions are the subject of the pen register and trap and trace device.
5. Based on the experience of Your Affiant, the disclosure of the requested Warrant and Court Order may result in furthering the flight of the subject or the destruction of, or tampering with, evidence or may otherwise seriously jeopardize the investigation and the subject’s safety. Therefore, IT IS REQUESTED that this Search Warrant and Order and Affidavit be **SEALED** until otherwise ordered by the court, and that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Warrant/Order to be served on any service provider or other person.
6. IT IS REQUESTED, so as not to disrupt this ongoing investigation, Your Affiant also requests that this Court order Facebook NOT to take adverse action against the subject accounts, such as disabling or terminating the accounts, because of this warrant.
7. IT IS REQUESTED, pursuant to 18 U.S.C. §3123(d) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), that Facebook be ordered **NOT to 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. 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 in my presence 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 EX PARTE COURT ORDER AUTHORIZING USE/INSTALLATION OF A PEN REGISTER AND TRAP AND TRACE DEVICE, GEOGRAPHICAL LOCATION INFORMATION, AND AUTHORIZING RELEASE OF SUBSCRIBER INFORMATION**

## 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:

**Facebook, Inc.** (internet service/social media provider)

**Facebook Security LE Response Team**

**1601 Willow Road**

**Menlo Park, CA 94025**

**Served via https://facebook.com/records**

This Court also finds that there is probable cause to issue this Search Warrant and also for an Ex Parte Order authorizing use/installation of a pen register and trap and trace device, and authorizing release of subscriber and/or location information pursuant to the provisions of 18 U.S.C. §2703 (Stored Communications), 18 U.S.C. §§3122 and 3123 (Pen Register and Trap and Trace), C.R.S. §16-3-301 (Search Warrant), §16-3-301.1 (Production of Records), §16-3-303.5 (Location Tracking), and Crim. P. 41 (Search Warrant), 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:

The following records, data, or information for Facebook User identified as ACCOUNT NAME **(hereinafter known as the “subject account”)** between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE(S):

* All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
* Additional Facebook accounts that were registered to the email address and/or phone number(s) utilized to establish the accounts;
* All Accounts associated by device or cookie: to include User ID, subscriber name, cellphone number and email address.
* All devices(s) used and otherwise associated with the subscriber’s accounts – ESN, ICCID, IMSI, IMEI numbers and activation dates;
* All activity logs for the accounts and all other documents showing the user’s posts and other Facebook activities;
* All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them and any associated metadata [camera make, model, capture date and time, capture latitude and longitude, etc.] and original sized image associated with those images and videos;
* All profile information; news feed information; status updates; links to videos, photographs, articles, and other items; notes; wall postings; friend lists, including past and present friends along with the associated friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook identification number(s) and Facebook identification number(s) of all group or network members; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;
* All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending “Friend” requests;
* All “check ins” and any other location information, including location history data;
* All Future and Past “events” the user responded to;
* All IP logs and associated port IDs, including all records of the IP addresses that logged into the accounts;
* All records of the account’s usage of the “Like” and “Follow” features, including all Facebook posts and all non- Facebook webpages and content that the user has “liked” and/or “followed”;
* All records of the account’s usage of the “Share” feature, including all Facebook posts and all non- Facebook webpages and content that the user has “shared”;
* All information about the Facebook pages that the accounts is or was a “fan” of;
* All records of Facebook searches performed by the accounts;
* All information about the user’s access and use of Facebook Marketplace;
* The types of service(s) utilized by the user, the length of service(s) (including start date), and the means and source of any payments associated with the service(s) (including any credit card or bank account number);
* All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the accounts;
* All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook accounts, including contacts with support services and records of actions taken.

Pursuant to §16-3-301.1, C.R.S., a criminal investigator or peace officer is hereby authorized to serve this order during normal business hours of the above-named business entity, and to receive the records during normal business hours of the business entity. Service shall issue in the same manner as a summons in a civil action or by personal service on a manager or supervisor of the business entity or through any electronic or other means established and utilized by the business to receive service of process. This order must be served within 14 days after the date it is issued.

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, BADGE NUMBER

LAW ENFORCEMENT AGENGY

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 a pen register be installed on the subject accounts by the internet service/social media provider, to register subject accounts, to record message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories, for a period of sixty (60) days from the date the warrant is served upon Facebook (hereinafter known as the “sixty (60) day time period”), or until such time as the investigation is completed, whichever comes first.
2. The internet service/social media provider, pursuant to probable cause, shall provide, on an ongoing (**NOT real-time**) basis, message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories relating to the subject accounts, beginning from the date the warrant is served on Facebook, and continuing for the sixty (60) day time period, or until the investigation is completed, whichever comes first.
3. The internet service/social media provider shall authorize and provide YOUR NAME HERE ongoing (**NOT real-time**) access to the following information relating to the subject accounts: message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories related to the pen register/trap and trace device, some of which is only available to such authorized users, **sent to** YOUR NAME HERE **daily (once every 15 minutes) via the email address** YOUR EMAIL ADDRESS**, beginning from the date the warrant is served on Facebook, and continuing for the sixty (60) day time period, or until the investigation is completed, whichever comes first.**
4. The internet service/social media provider shall furnish law enforcement information including message headers (**NOT message content**), all Internet Protocol (IP) address logs, last known locations, and location histories, unobtrusively and with minimum interference with the services that are accorded the persons whose transmissions are the subject of the pen register and trap and trace device.
5. This Search Warrant and Order and application be **SEALED** until otherwise ordered by the court, 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.
6. Facebook NOT take adverse action against the subject accounts, such as disabling or terminating the accounts, because of this warrant.
7. Pursuant to 18 U.S.C. §3123(d) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), that Facebook, **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 in items 1-5 above is related to the active and ongoing criminal investigation by YOUR AGENCY and in accordance with 18 U.S.C. §2703, 18 U.S.C. §§3122 and 3123, and C.R.S. §16-3-301, 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 and Ex Parte Order. You are therefore authorized to execute this Search Warrant and Ex Parte Order according to these terms and as otherwise permitted by law.

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

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

JUDGE / MAGISTRATE