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

-This search warrant mask is specifically for the search of Turo for all data associated with identified user ID.

-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 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:

**Turo, Inc.**

**111 Sutter St., Suite 1300**

**San Francisco, CA 94104**

**VIA: ler@turo.com**

The following records, data, or information for Turo, Inc. user identified as User ID: USER ID between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. Subscriber Information-Username, Turo account number, full name, physical address, user name, email address(es), phone number(s), Profile/Avatar Image(s), Apple ID(s), Android ID(s), linked Social Media Account(s): Identifiers, dates of linkage and account activity, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;
2. Device Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Turo App accounts of the target device;
3. Financial Account Information - Linked Bank Accounts: Account Number(s), Routing Number(s), Date(s) of Linkage, Linked Financial Transaction Cards: Full Financial,Transaction Card Number(s) (to include: Major Industry Identifier, Bank Identification Number, Account Number, and Checksum), All records of transaction information, All records of securities, funds, and portfolios associated with the target Turo App account and/or target device from (start date to end date);
4. Transactions – All records of transaction information (Outgoing transactions, Incoming ransactions), Web receipts, date and time of transactions, Source of transactions, Avatar/Profile image of Sender/Receiver;
5. User Activity – All search history and queries to include- pages or other contact viewed, search history, and booking history;
6. Location History (Turo Go) - All location data whether derived from Global Positioning System(GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, wifi locations, and Bluetooth beacons. Such data shall include the date and timestamps of the activity (with identified time zone), the latitude and longitude GPS coordinates, the accuracy display radius (in meters), the source of the activity (e.g. wifi, cell, Bluetooth or GPS, etc…), the specific Device Tag number, the device Platform information, of all location recordings from the period [start date] to [end date];
7. Trip data-from all trips from the period (start date) to (end date) to include amounts charged, start locations and destinations, miles traveled, vehicle information, and other related trip details.
8. In vehicle device data (Turo GO)- Make, model and year of the vehicle, car battery voltage, fuel level, odometer reading, malfunction indicator lamp, door state (lock or unlocked), engine state, vehicle identification number (VIN) and any additional information related to the vehicle or its operator.
9. Communcation Information - All communications between users, whether as a driver or customer, and Turo customer support, whether by phone, text message, email, or internal application.
10. Internet Protocol (IP) address information - all IP address information regarding the IP address used at the time of account creation, and any IP address information stored by Turo.

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 and Crim. P. 41, namely that this property has been stolen or embezzled, or which is designed or intended for use as a means of committing a criminal offense, or which is or had been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, 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.

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.

**Statements Regarding Current Investigation**

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

**Relevant Background Information on Turo**

According to its website, Turo provides an online car sharing platform that connects vehicle owners with travelers and locals seeking to book those vehicles. Turo is accessible online including at turo.com and as an application for mobile devices.

Under its privacy policy, Turo states it collects three categories of personal information (1) personal information given by the user; (2) personal information automatically collected from the user; and (3) personal information from third-party sources. Personal information given by the user includes:

**Account data.** When a user registers for an account with Turo, it requires certain personal information to open the users account, such as the user’s name, email address, and password.

**Profile data**. Turo may also ask the user to provide additional profile information to use certain features of the Services which may include street addresses, phone numbers, driver’s license number, date of issuance and issuing country and/or state, profile photos, employer, city, school, biography, and date of birth. Certain parts of the user’s profile (like your profile photos, employer, city, school, and biography) are part of the user’s public profile page and will be publicly visible to others.

**Vehicle data**. Turo collects information the user provides in relation to a vehicle such as vehicle listing details, vehicle identification number (VIN), availability dates, reviews, and uploaded trip photos.

**Payment data**. Turo collects the user’s digital payment details, bank account or payment card numbers, and transaction information in connection with a potential or actual transaction, which may be processed and stored by one or more third party payment service providers or digital payments companies.

**Identity verification data**. In some instances, Turo may collect identity verification information such as a photograph or scanned copy of a driver’s license, passport, national ID card, or payment card, last four digits of your Social Security number, social insurance number, social media account information, driver’s/motor vehicle record, insurance information, or other forms of identification information. Where we request that you withhold certain information (such as obscuring or redacting aspects of identification information), please do so.

**Communications**. When the user communicates with Turo, including via phone, email, or chat, or use the services to communicate with other users, Turo collects information about the user’s communication and any information the user chooses to provide.

Personal information automatically collected from the user includes:

**Usage data**. Turo collects information about the user’s interactions with the services, such as the pages or other content the user views, searches, bookings made, how long spent on a page or screen, sites from which the user link or browse to in the services, navigation paths between pages or screens, information about activity on a page or screen, access time, duration of access, and other actions on the services.

**Location data**. When the user’s uses certain features of the services, Turo may collect information about your approximate location (e.g., city/town associated with your IP address). When the user opts in to use our location sharing feature, Turo may collect the precise location information of mobile devices.

**Device data**. Turo collects information about computer or mobile devices, such as its operating system type and version number, manufacturer and model, browser type, screen resolution, IP address, unique device identifiers, or general location information such as city, state, or geographic area.

**Trip data**. Turo collects transactional information related to the trips the user takes through the services, including the date and time of your trip, amounts charged, and other related trip details.

**In-vehicle device data**. If a vehicle is enrolled in a Turo Go program or has a Turo Go device installed, Turo may remotely collect certain information about the vehicle. Depending on the make, model, and year of the vehicle, this information may include, GPS location, car battery voltage, fuel level, odometer reading, malfunction indicator lamp (e.g., a check engine light), door state (e.g., locked/unlocked), engine state (e.g., stopped/running), and VIN.

**Cookies and similar technology**. When the user accesses the services, Turo may place small data files on your computer or other device. These data files may be cookies, clear gifs, pixel tags, e-tags, “Flash cookies”, or other local storage provided by your browser or associated applications (collectively “Cookies”).

Personal information from third-party sources incudes:

**Third-party services**. If the user chooses to log in to our services through a third-party site or service (e.g., Apple, Facebook, or Google), the third-party service may send information such as your registration and profile information from that service. The information Turo may receive varies by service and is controlled by the relevant service. By associating an account managed by a third party with a Turo account and authorizing Turo to have access to this information, the user agrees that Turo may collect, store, and use this information.

**Third-party in-vehicle devices**. If the user’s vehicle, or a vehicle booked through the services, includes an in-vehicle device or system operated by a third-party service (including vehicle manufacturers) or installed by the host, that host or service may record information about your use of the car. These devices or systems may monitor the car's condition, performance and operation, track fuel consumption, distance traveled, location, and other information. The host and/or third-party service will be solely responsible for its use of such information but may disclose such information to Turo.

**Background check services**. To the extent permitted by applicable laws, Turo may collect background information about the user from public records, background check providers, or other screening services, including credit reports and information about criminal convictions or from sex offender registries.

**Other sources**. To the extent permitted by applicable law, Turo may receive additional information about you, such as demographic data, fraud detection information, or data from credit bureaus and other third-party data providers.

**Relevant Background Information of Technology**

I know from training and experience that digital evidence is not limited to computers. I have been involved in cases where persons engaged in the type of crime under investigation can access the Internet, display images reflecting their interests or participation in the crime, and communicate with other individuals with the same interests using digital storage devices to include cellular telephones, email devices, and personal digital assistants. These devices are frequently found to contain chat communications in the form of short message service (SMS) messages as well as enabling Internet and digital cellular network access.

I know from training and experience that the complete contents of online accounts may be important to establishing the actual user who has dominion and control of an online account at a given time. Online accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. So, information stored in connection with an online account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation. This helps establish and prove each element of the crime or alternatively, may exclude the innocent from further suspicion. In my training and experience, an online user’s account activity, IP log, location information, search history, stored electronic communications, and other data retained by providers, can indicate who has used or controlled an online account or can provide context for the crime under investigation. This can include evidence of motive and intent to commit a crime (e.g., communications about planning crimes) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. Further, account activity, especially when paired with other evidence of the crime, can show how and when the account was accessed or used and may reflect a user’s motive or state of mind when doing so. For example, as described herein, Providers log 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. Especially when considered in context with other evidence, such information allows investigators to understand the geographic and chronological context of an account’s access, use, and events relating to the crime under investigation. Location data also helps with this. Providers allow users to “tag” their location in posts to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the account user or other suspects.

I know from training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”) or code words (which require entire strings or series of email conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren “:)” to convey a smile or agreement) to discuss matters. Keyword searches would not account for any of these possibilities, so actual review of the contents of an online account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit in order to prevent unnecessary invasion of privacy and overbroad searches. I advise it would be impractical and infeasible for the government to review records produced by a Service Provider and keep only such records as the government finds to be related to the offenses described herein during a single analysis. I have learned through practical experience that various emails often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review, and incorporation of evidence into a consolidated whole. Analysis is content relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually and not in sum. Due to the interrelation and correlation between communication threads and contents of accounts, and any respective attachments, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. Therefore, to obtain the full picture and meaning of the data from the information sought in this application, and to maintain its admissibility at trial, the government needs to maintain access to all of the resultant data. The completeness and potential of probative value of the online accounts and data must be assessed within the full scope of the investigation. As with all evidence, the government will maintain the contents of the account(s) in its custody and control, without alteration.

Based on these facts, Your Affiant believes there exists probable cause to believe that there is material evidence now located in the above described Turo 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 Crim. P. 41.

C.R.S. 16-3-301.1(5)(a) permits a court order for the productions of records to be granted to a Colorado criminal investigator or peace officer whose affidavit supports the issuance of the order. The Colorado criminal investigator or peace officer granted the order need not have authorization to execute a search warrant in the jurisdiction in which the business entity is located. C.R.S. 16-3-301.1(5)(c) permits service of a court order to be made through any electronic or other means established and utilized by the business to receive service of process.

Turo, Inc. 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 Turo, Inc. 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 Turo, Inc. 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 Turo, Inc. 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 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:

**Turo, Inc.**

**111 Sutter St., Suite 1300**

**San Francisco, CA 94104**

**VIA: ler@turo.com**

This Court also finds that there is probable cause to issue this Search Warrant and Court Order for Production of Records pursuant to the provisions of 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41, namely that this property has been stolen or embezzled, or which is designed or intended for use as a means of committing a criminal offense, or which is or had been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, 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.

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 Turo, Inc. user identified as User ID: USER ID between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. Subscriber Information-Username, Turo account number, full name, physical address, user name, email address(es), phone number(s), Profile/Avatar Image(s), Apple ID(s), Android ID(s), linked Social Media Account(s): Identifiers, dates of linkage and account activity, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;
2. Device Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Turo App accounts of the target device;
3. Financial Account Information - Linked Bank Accounts: Account Number(s), Routing Number(s), Date(s) of Linkage, Linked Financial Transaction Cards: Full Financial,Transaction Card Number(s) (to include: Major Industry Identifier, Bank Identification Number, Account Number, and Checksum), All records of transaction information, All records of securities, funds, and portfolios associated with the target Turo App account and/or target device from (start date to end date);
4. Transactions – All records of transaction information (Outgoing transactions, Incoming ransactions), Web receipts, date and time of transactions, Source of transactions, Avatar/Profile image of Sender/Receiver;
5. User Activity – All search history and queries to include- pages or other contact viewed, search history, and booking history;
6. Location History (Turo Go) - All location data whether derived from Global Positioning System(GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, wifi locations, and Bluetooth beacons. Such data shall include the date and timestamps of the activity (with identified time zone), the latitude and longitude GPS coordinates, the accuracy display radius (in meters), the source of the activity (e.g. wifi, cell, Bluetooth or GPS, etc…), the specific Device Tag number, the device Platform information, of all location recordings from the period [start date] to [end date];
7. Trip data-from all trips from the period (start date) to (end date) to include amounts charged, start locations and destinations, miles traveled, vehicle information, and other related trip details.
8. In vehicle device data (Turo GO)- Make, model and year of the vehicle, car battery voltage, fuel level, odometer reading, malfunction indicator lamp, door state (lock or unlocked), engine state, vehicle identification number (VIN) and any additional information related to the vehicle or its operator.
9. Communcation Information - All communications between users, whether as a driver or customer, and Turo customer support, whether by phone, text message, email, or internal application.
10. Internet Protocol (IP) address information - all IP address information regarding the IP address used at the time of account creation, and any IP address information stored by Turo.

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 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 Turo, Inc. 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 Turo, Inc., **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 and Crim. P. 41, 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 Court Order for Production of Records. 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