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

-This search warrant mask is specifically for the search of a Key Programming Device / Vehicle Diagnostic Tool for date relevant to the investigated offense.

-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.

-When PC exists to believe a computer contains evidence or was used to commit a crime, always use include the section authorizing the examination of the devices. Don’t forget to establish what evidence will be found on the computer equipment in the affidavit.

- 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**

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

 JUDGE / MAGISTRATE

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

DESCRIBE DEVICE

ADD PHOTO OF DEVICE IF AVAILIABLE

LOCATION OF DEVICE

The following data stored in the device, relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of ENTER CRIMINAL OFFESNES perpetrated against VICTIM (hereinafter “Subject Offense(s)”):

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

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. All identification and attribution data, in any format or medium, related to the use of the device, including any subscriber or user information (IMEI, MAC addresses, serial numbers) for connected mobile/computer/electronic devices, and/ or other data tending to show the persons in use or control of the device;
3. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
4. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
5. All Wi-Fi, Bluetooth, and USB connection logs;
6. All usage data, including activity logs (with dates, times, and locations of each use), ROM files, software version, vehicle data (i.e., make/model/VIN), key fob data (i.e., serial number, identification number, any other device identification numbers), camera usage, and other data related to the use of the programming/reprogramming/ deprogramming functions of the devices;
7. Any other documents, images, videos, or other data files stored in the device pertaining to the planning and commission of Subject Offense(s).

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

\*\*NOTE: Descriptions of the data, information, functions or services listed above are contained in Attachment A, which is incorporated herein by reference.

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

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

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

BACKGROUND OF AFFIANT

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

Based on this training and experience and conversations with others in law enforcement, I know the following about the following topics regarding this investigation:

Key Programming Device / Vehicle Diagnostic Tool Capabilities

A Key Programming Device/Vehicle Diagnostic Tool is a device that is capable of doing the following functions: universal transponder & key generator, transponder simulation, editing & cloning, ignition coil detection, vehicle diagnostics, vehicle service functions, IMMO function via programmer, transponder reading, frequency detection, key unlocking, immobilizer data processing, IMMO In open OBD mode.

IMMO (Immobilizer) – a car immobilizer system is a piece of security technology that is designed to deter and inhibit vehicle theft. This technology’s goal is to keep a car from being hot-wired and stolen from someone who doesn’t have the key to start the engine.

A Key Programming Device/Vehicle Diagnostic Tool generally speaking will achieve the addition, modification or deletion of electronic keys by communicating with the vehicles on-board computer. A key programing devices will write the newly generated electronic key information into the car’s electronic control unit (ECU) or other related modules to complete the pairing and programming of the new key with the vehicle. Once the device is connected to a vehicle via the OBD2 port, the operator can do a variety of things with the following vehicle systems, including Oil Reset, electronic parking brake (EPB), Battery Management System (BMS), Steering and Suspension (SAS), Diesel Particulate Filter (DPF), Throttle Relearn, Anti-Lock Braking (ABS) Bleed, Key Programming, injector coding, air suspension, transmission relearn, TPMS reset, airbag repair, hybrid control compression test, HVAC Control Module Calibrate, Zero Point Calibration, Injector Balance Test, Fuel Trim Reset, Cylinder Power Balance, Crankshaft Sensors Relearn, Rewriting of the VIN on Power-Train Control Module (PCM), alcohol composition reset, suspension calibration, etc.

Based on training and experience, your Affiant knows that key programming device/vehicle diagnostic tools store a variety of information including Vehicle Identification Numbers, makes, models, data / times of downloads, stored data of vehicles the device has been plugged into, etc.

Nexus between the target offense(s) and the locations within the phone to be searched:

Your Affiant respectfully requests that this Search Warrant be approved so that your Affiant or Designee may search the above-described data associated with the device identified above. A search of the data associated with the key programming device/vehicle diagnostic tool is necessary because such data may be relevant to the offenses being investigated.

Your Affiant also knows from training and experience that criminals use these devices to steal motor vehicles. Once a car thief gains access to a vehicle, the car thief will connect a key programming device/vehicle diagnostic took to the vehicle via the OBD2 Port. Once connected the device can do any of the following functions described above. This information, along with other information that can be obtained through an electronic device such as a key programmer/vehicle diagnostic tool, will assist Your Affiant with furthering the above-described criminal investigation. For example, evidence relating to the above-described offense(s) and/or related events or information is likely to be contained in the categories detailed above.

These devices also allow for notes, photos and other data to be entered by the user when connected to the vehicle that can further the above-described criminal investigation. These devices will store data including vehicle data (year, make, model, VIN, etc.) of the vehicle that the device was plugged into and record any changes made by the user stored in data reports on the device. This data can provide multiple types of relevant evidence to the planning and or/commission of the offense.

In the event that relevant and/or incriminating evidence is located in the device, it will be critical to establish the individual in possession of the device at or about the time the communications are made, the photos and/or videos are captured, and any data logs of the vehicles that the device has been connected to. This information will provide further evidence of the offense and show what vehicle keys had been reprogrammed which will assist in determining how the motor vehicle was stolen.

Computer Processing

Due to the nature and vulnerability of magnetic or digital data, it is necessary to seize media capable of storing magnetic data, and the computer, or what is commonly referred to as the CPU, meaning the computer case which contains the hard drive, motherboard and related hardware. It is necessary to remove these items from the scene and transport them to a controlled environment so a complete search of the items may be accomplished in such a way that the data is protected, and unaltered.

Your affiant is aware that the current technology available for the downloading of data from digital devices such as cell phones, computers, or other mobile devices, does not allow the download of information only for a specific date range. Your affiant is also aware that the current technology available may not allow the downloading of only specific types of data, (e.g. pictures, messages, contacts, application data, etc.) as this data, including dates, may be in raw form, making it humanly unreadable without the use of specific software.  In light of that, the data from the digital device must be downloaded as completely as technologically possible. Once that download is completed, and the downloaded data is processed with specific software, a search of the data for a specific date range or specific type of data content is possible.

Your affiant is also aware that many times, there is only one opportunity to download the information from a digital device. Without obtaining all of the downloadable data from the cell phone, computer, or other mobile device, if additional information is learned later in the investigation, either by law enforcement, the District Attorney’s Office, or defense counsel, the same data that existed at the time of the initial download may no longer be available.  The only way to ensure preservation of all the downloadable data that existed at the time of the original download is to initially obtain all the downloadable data from the cell phone, computer, or other mobile device, and then preserve that data for any future searches.

Your affiant is requesting to obtain all of the downloadable data from the digital device(s). That data will be saved to preserve it in case additional review of the data is warranted and authorized by the courts at a later time. If a future search of the downloaded data from the device is necessary at a later time, additional applications will be made to the courts. At this time, the review of the data extracted from the device(s) will be for the date range and data authorized in the warrant.

***Further requests:***

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

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

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

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

AFFIANT

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

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

JUDGE / MAGISTRATE

 Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

 ) SS

STATE OF COLORADO )

**SEARCH WARRANT**

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

 JUDGE / MAGISTRATE

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

The Court, upon review of a sworn affidavit filed by YOUR NAME HERE, a commissioned law enforcement officer, in support of the issuance of this search warrant, hereby commands you to search the following described property, namely:

DESCRIBE DEVICE

ADD PHOTO OF DEVICE IF AVAILIABLE

ADDRESS WHERE DEVICE IS LOCATED

The following data stored in the device, relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of CRIMINAL OFFENSE(S) perpetrated against NAME OF VICTIM OR LOCATION [IF APPLICABLE] (hereinafter “Subject Offense(s)”):

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

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. All identification and attribution data, in any format or medium, related to the use of the device, including any subscriber or user information (IMEI, MAC addresses, serial numbers) for connected mobile/computer/electronic devices, and/ or other data tending to show the persons in use or control of the device;
3. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
4. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
5. All Wi-Fi, Bluetooth, and USB connection logs;
6. All usage data, including activity logs (with dates, times, and locations of each use), ROM files, software version, vehicle data (i.e., make/model/VIN), key fob data (i.e., serial number, identification number, any other device identification numbers), camera usage, and other data related to the use of the programming/reprogramming/ deprogramming functions of the devices;
7. Any other documents, images, videos, or other data files stored in the device pertaining to the planning and commission of Subject Offense(s).

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

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

Based upon the affidavit of the above-named affiant, which is incorporated by reference, I am satisfied that there is probable cause to believe that the property described is located at the place above described, and probable cause to seize the items described above pursuant to Crim. P. 41, and §16-3-301. YOU ARE THEREFORE AUTHORIZED to search the place described for the property described, and to make a return of this Warrant to the undersigned judge within fourteen days, and to deliver to the person from whom the property is taken, a copy of this Warrant together with a receipt for the property taken, or, to leave a copy of the Warrant and receipt at the place from which the property was taken.

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

* If not already in possession of the device, seize the aforementioned device within 14 days of the date this warrant is signed;
* Access the aforementioned device and view, copy and maintain the above described data contained therein;
* Use and employ such force as may reasonably be necessary in the performance of the duties described herein;
* The ability to enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imagining, and analysis of any and all of the information described.
* Deliver to the person from whom the property is taken a copy of this warrant together with a receipt for the property taken, or to leave a copy of the warrant and receipt at the place from which the property was taken;
* Make prompt return of this search warrant, accompanied by a written inventory describing the physical storage media that was seized or copied, to the undersigned judge.

IT IS FURTHER ORDERED:

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

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

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

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

JUDGE / MAGISTRATE