**AFFIDAVIT FOR SEARCH WARRANT**

**County of [ \_\_\_\_\_\_\_\_\_\_ ]**

**SECTION I**

**INTRODUCTION**

I, [AGENT NAME], being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a warrant to search a cellular device located at

the premises known as [PREMISES ADDRESS], hereinafter “PREMISES,” for certain things particularly described in “[LIST PROPERTY EXHIBIT #B]”.

2. I am a [TITLE] with the [AGENCY], and have been since[DATE]. [[DESCRIBE TRAINING AND EXPERIENCE INCLUDING EXPERTISE WITH CELLULAR DEVICES].

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

**SUMMARY**

*Note: this is a good place to provide a summary of the case which will need to be also placed in the notice of the search provided to the target. The summary should include reasonable specificity as to the nature of the investigation under which the information is sought, it is highly likely the notice will need to be provided contemporaneously with the search.*

**PROBABLE CAUSE**

*Note: Give the facts that establish probable cause to believe that evidence, fruits, or contraband can be found on each cellular device that will be searched and/or seized.*

4. The criminal statutes involved in this investigation are violations of [CODE SECTION, CODE DESCRIPTION].

5. As described above and in “[LIST PROPERTY EXHIBIT #B]”, this application seeks permission to search and seize records that might be found on the described cellular device, in whatever form they are found.

6. Based on the following [INSERT INFORMATION PERTAINING TO THE USE OF THE CELLULAR DEVICE], I am aware that cellular equipment was used to communicate information pertaining to this case. I am further aware that cellular devices are often used to communicate with other parties and to search for and store information.

**I am seeking evidence of ownership, use, and identification**. I know that ownership and control of a digital device can be placed at issue through a simple denial, “that is not my phone.” In my training and experience some of the best ways to establish control are by searching the calendar, contacts, photo gallery, communications, settings, and social networking activity. The calendar often contains appointments specific to an individual such as birthdays and doctor’s appointments. Contacts often contain friends and associates specific to an individual such as mom, dad, dentist, etc… A photo gallery often contains selfie photos that clearly depict the owner/holder of the phone. Communications via text messages, emails, and voicemails often identify the sender/recipient by name, additionally the context of the communications often identify the sender and/or recipient. Settings often contain user names, addresses, and phone numbers, wi-fi network tables, associated wireless devices (such as known wi-fi networks and Bluetooth devices), associated connected devices (such as for backup and syncing), stored passwords, and user dictionaries that can identify the owner/user of the device.

**I am seeking evidence of communication.** In my training and experience associates communicate together via phone calls, text messages emails, and social network posts. These communications often contain direct and indirect statements about crimes. Furthermore, I know that communications rarely explicitly mention an intent to commit a crime. Instead they often allude to such an intent: “gunna go hustle” for instance may be a declaration of an intent to commit a theft crime, but without context it is meaningless. In my training and experience individuals often use digital devices and cellular devices to post messages to others on social networking applications. In my training and experience it is possible for cellular phone users to use a variety of messaging platforms including SMS, MMS, iChat, WhatsApp, call logs, and others. Therefore I seek to search all the communications evidence on the device to understand not only what was said, but what was intended and to whom it was said. I am seeking this information since \_\_\_\_\_\_\_\_\_\_\_.

**I am seeking evidence of location**. In my training and experience cellular devices track historical locations in multiple ways, GPS location, wi-fi transmissions, metadata attached to files, cellular tower connections, and application data. Because the evidence in this case indicates \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ I believe the evidence is relevant to correlate location with criminal activity occurring miles from the user/owners home. I am seeking all location data since \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**I am seeking evidence of association**. I know that establishing the association of co-conspirators is important in proving a concert of action between multiple persons. In my training and experience some of the best ways of linking co-conspirators together is by searching the calendar, contacts, photo gallery, communications, application data, call logs, and social networking connections. In my training and experience a comparison of the calendars of multiple individuals can show an intent to act together and dispel the notion of an accidental meeting. In my training and experience when two or more individuals are in photographs together it demonstrates a mutual relationship. In my training and experience associates communicate together via phone calls, text messages and emails, therefore I am seeking the communications evidence to demonstrate the associations of the individuals in this case. In my training and experience a user’s “connections,” “buddies,” and/or “friends,” on social networking sites is indicative of who their associates are. . Because this evidence is intended to be used to show associations of the user/owner of the device and co-participants I am seeking the above items regardless of the dates the information was created.

**I am seeking specific evidence related to this case**. In addition to the previous information, I believe the GPS location, financial information, cookies, bookmarks, web history, search terms and internet search history on digital devices and cellular devices may contain relevant evidence such as \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_. Therefore, by this warrant I am seeking permission to search all the metadata, file data, setting data, photographic and video data, and communication data on any digital device.

*Note: Subsection (e) is covering devices such as Google Wallet, Apple-Pay, Square Wallet, PayPal that may contain financial transaction information that may show location, type, and nature of a specific purchase. Information may be of value to establish the physical location of the device at a given time.*

[INSERT FACTS THAT DESCRIBE HOW THE CELLULAR DEVICE WAS USED; DATA OR COMMUNICATIONS THAT WAS SENT OR RECEIVED; RECORDS OF DISCUSSIONS ABOUT THE CRIME; IDENTITY OF THE USER; AND OTHER RECORDS THAT INDICATE THE NATURE OF THE OFFENSE AS IT PERTAINS TO ITEMS (a) – (f)].

**DIGITAL FORENSIC EXAMINATION**

*Note: This subsection requires the affiant to have basic computer forensic knowledge. The affiant can also interview another agent that has this knowledge. This subsection is only required where a device will be seized and examined.*

7. Based on my knowledge, training, and experience, I know that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or other storage device, deleted or viewed via the Internet. Digital files downloaded to a storage device can be stored for years and remains on the storage device until it is overwritten by new data.

8. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

9. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

10. Based upon my knowledge, training and experience, I know that searching for information stored in cellular devices often requires that the device be accessed and searched using specialized programs or tools by a qualified expert in a controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Data search processes are designed to recover even “hidden,” erased, compressed, password protected, or encrypted files. Because digital evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment may be necessary to complete an accurate analysis.

In light of these concerns, I hereby request the Court’s permission to conduct an off-site search of the hardware for the evidence described and to employ the use of outside experts who will use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in in “[LIST PROPERTY EXHIBIT #B]”.

As required by Penal Code § 1524.1 (d); those items that are within the scope of this warrant will be copied and retained by investigative agents. Investigating agents will then seal any information from the device that is unrelated to the objective of the warrant (does not fall within the scope of “[LIST PROPERTY EXHIBIT #B]”) and will not further review the information absent an order from the Court.

If no evidence of criminal activity is discovered relating to the seized property and associated peripherals, the device will be returned promptly.

**REQUEST FOR NONDISCLOSURE**

11. [IF APPROPRIATE: It is further requested that pursuant to the preclusion of notice provisions of Penal Code § 1546.2 and 18 U.S.C. § 2703(b), [ISP / COMPANY / ENTITY PRODUCING RECORDS] be ordered not to notify any person (including the subscriber, customer or owner of the electronic communication or device information to which the materials relate) of the existence of this warrant for ninety days.

Note: *A non disclosure request should be made if records will produced by a service provider or other 3rd party.*

12. [IF APPROPRIATE: Your affiant is aware that Penal Code § 1546.2 mandates that the law enforcement agency serving this warrant notify the target of the warrant contemporaneously with the service of the warrant unless an order delaying notification is granted. It is further requested, pursuant to the delayed notice provisions of Penal Code § 1546.2(b), an order delaying any notification to the target / party that may be required by § 1546.2(b) about this warrant, for a period of ninety days.

Such an order is justified because providing prior notice to the target / party in this matter would lead to an adverse result which may result in endanger the life or physical safety of an individual; lead to flight from prosecution; lead to destruction of or tampering with evidence; lead to intimidation of potential witnesses; or otherwise seriously jeopardize an investigation or unduly delay a trial.]

*Note: Penal Code § 1546.2 mandates that the law enforcement agency serving the warrant that includes the production of or access to electronic communication / device information notifies the target of the warrant contemporaneously with the service of the warrant. This mandatory disclosure may be delayed for up to 90 days upon a showing that notification may have an adverse result to the investigation. An “adverse result” means any of the following: (1) danger to the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) serious jeopardy to an investigation or undue delay of a trial. Request for delayed notification is to be made by sworn affidavit(can be part of the warrant) and further requests for extension on delaying notification can be made to the court. If using these paragraphs, include a nondisclosure order with warrant.*

**CONCLUSION**

11. WHEREFORE, I request that a Search Warrant be issued based upon the aforementioned facts, for the search of [LIST PROPERTY EXHIBIT #B], between the hours of 7:00 a.m. and 10:00 p.m. good cause being shown thereof, and the same be brought before this Magistrate or retained subject to the order of the court, or any court in which the offense(s) in respect to which the property of things taken, triable, pursuant to Section 1536 of the California Penal Code.

I swear, under penalty of perjury, that the foregoing Information is true and correct, to the best of my knowledge, information and belief.

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

[AGENT NAME]