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

- This search warrant mask is specifically for the search of Ring for all data associated with the identified account.

-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:

**Ring, LLC**

**ATTN: Ring Legal Department, Custodian of Records**

**1523 26th Street**

**Santa Monica, CA 90404**

**Service via email at subpoenas@ring.com**

The following records, data, or information for Ring user identified as:

MAC Address: MAC ADDRESS

Account Holder: NAME

Physical Address: PHYSICAL ADDRESS

Phone Number: PHONE NUMBER

Email Address: EMAIL ADDRESS

between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. **Account information** – username(s), primary email address, secondary email addresses, connected applications and sites, and account activity for the **target date range(s) listed above**, including account sign in locations, browser information, platform information, internet protocol (IP) addresses, all privacy settings, other account settings (including online username(s) and passwords), and/or information used to access **Ring** products and services;
2. **Subscriber information** – all subscriber contact and personal identifying information, including but not limited to, full name, user identification number, birth date, gender, contact email address(es), security question(s) and answers(s), physical address (including city, state, and zip code), telephone numbers, and any other personal identifiers);
3. **All device information** – all mobile, computer, and/or surveillance device(s) used by, associated with, utilized by, and/or connected to the target account(s), including electronic serial number (ESN), integrated circuit card identification (ICCID) number, international mobile subscriber identity (IMSI) number, international mobile equipment identity (IMEI) number, media access control (MAC) address, and/or any other unique identifier, as well as connection logs, login and logout information, and activation dates;
4. **Account device information** – all devices attached to the target account(s), including cameras, doorbells, chimes, path lights, alarms, sensors, motion detectors, panic buttons, alarms, smart devices and beacons, along with product setup information, such as the name and description of the **Ring** product, the location(s) where the product(s) was/were installed, adjustments made during setup, Wi-Fi network information, and product details including the **Ring** product’s model, serial number, and software version;
5. **Service and financial information** – all information regarding types of service(s) utilized by the target account(s), the length of service(s) (including start date and/or activation date), the means and source of any payments associated with the service(s) (including any credit card or bank account numbers(s) or information, including expiration date and security code);
6. **Activity log information** – all activity logs for the target account(s) and data collected in connection with the target account(s), including “nearby incidents,” “history,” camera activity, event history, smart alerts, motions setting, device settings, and shared users for the above-described target date range;
7. **All device content**, including but not limited to any saved video and/or audio recordings, any captured surveillance images, any notification alerts, motion activation alerts, any “linked event” motion alerts, any “favorited” event alerts, any and all history notifications, and any stored dates and times (time stamps) for all device content;
8. **All internal communication data**, including but not limited to all data used in the “Neighbors” communication application, as well as all communications, shared images, shared video, and shared alerts as posted and/or shared by the target account during the above listed dates/times;
9. **All other identifying data, if collected by Ring,** including but not limited to any information on the device(s) used to access the target account(s), including the type of devices, model numbers, International Mobile Equipment Identifier (IMEI) numbers, phone numbers, Global Positioning System (GPS) locations, and/or Internet Protocol (IP) addresses.
10. All records pertaining to communications between Ring and any person regarding the user or the user’s Ring account, including contacts with support services and records of actions taken.

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

**Ring Information**

I know from my training and experience that Ring LLC (hereinafter “Ring”) is a home security and technology company that is popular for its doorbell camera systems. Additionally, Ring maintains a proprietary technology application (“app”) that provides remote access to home surveillance systems, including but not limited to, video surveillance cameras, automatic lighting systems, alarm systems, garage doors, chimes/doorbells, various electronic locking mechanisms, thermostat and water valve controls. The application also utilizes a social media-type platform known as “Neighbors”, which includes, but not limited to, anonymized communications with other Ring customers, such as comments and online communications posts, the sharing of recorded video surveillance video, pictures, and other forms of communications. Customers that utilize Ring are also able to opt into accepting public safety alerts, crime alerts, lost pet alerts, unexpected activity alerts (suspicious persons or circumstances), “neighborly moment” alerts (acts of kindness), and requests for assistance alerts (allows alerts from law enforcement and other safety agencies). Based on my training and experience as well as publicly available data from Ring, I know that Ring surveillance footage is saved and stored for sixty (60) days.

I know from my own experience, from my own research, and from reviewing publicly available information from Ring, they are a home surveillance security system headquartered in Santa Monica, California with operations worldwide. Their platforms can be accessed via their websites and mobile applications.

I know from my own training and experience, from my own research, and from reviewing publicly available information that Ring users download and install the Ring application from the Apple App Store or Google Play Store to their internet-capable smart phone, smart watch, tablets, and computers. The user then installs the Ring application on their smart phone and create an on-line Ring account. The user will then be required to associate a form of payment, either a credit card, debit card, or bank account to their Ring account to pay for subscription services. Ring maintains particular details about each user including name, date of birth, home address, phone number, e-mail account, payment methods and related history, historical alert details, live video surveillance, stored video surveillance, “Neighbors” social media posts, and geo-location history.

I know from my own training and experience, from my own research, and from reviewing publicly available information that Ring stores information regarding their devices that are linked with the user’s account(s). This includes the make, model, and unique serial numbers of all linked devices. I believe with information will assist in identifying the exact make and model of the doorbell camera that captured the burglary.

I know from my training and experience, as well as that of other experienced investigators with whom I have spoken, I know that Ring users have the option to store, upload, and share digital media (video, images and audio) onto Ring’s cloud storage servers. These digital media files may be downloaded from the internet, sent from other users, uploaded from the user’s mobile device, and uploaded from the user’s Ring product. In many cases, a Ring user may configure their product to automatically upload digital media captured on their devices a cloud storage. I believe a review of these digital media files would provide evidence depicting the suspect(s), their associates, and others performing above listed felony(s).

I know from my training and experience, as well as that of other experienced investigators with whom I have spoken, that the most common way for individuals to utilize the Ring application is through the use of an internet-capable smart phone, such as an Apple iPhone or Samsung Galaxy. I know from my training and experience, as well as that of other experienced investigators with whom I have spoken, that most smart phones utilize operating systems designed to provide the user with an integrated and seamless user experience across multiple applications and services. As a result, often these applications will have linkages established between them, even when the individual applications are designed and run by different companies. Likewise, I know that social media applications, such as Facebook and Instagram, are designed to be integrated with other mobile applications for an integrated and seamless user experience. As a result, it is common to be able to locate linked social media account information in the records from other applications and their providers.

I know from my own training and experience, from my own research, and from reviewing publicly available information that Ring maintains their records by the user service records. Ring maintains the original email address and Internet Protocol (IP) address of the profile creator. Ring will also maintain sign-on IP logs, sent and received messages, and other subscriber information.

I know from my training and experience that account records, may support evidence of current, on-going, future, and past criminal activity. I know that such information may be used to verify identities, identify victims, identify witnesses, identify associates and co-conspirators.

I know from my own training and experience, from my own research, and from reviewing publicly available information that Ring collect and store personally identifying information on their users. This information consists of user supplied information that can be used to identify the user and/or account creator of an Ring account. This information may include, but is not limited to usernames, account identification numbers, payment methods, credit card numbers, account information, messages, digital content and download information, digital device information, alert history, and devices including device identifiers, first name, last name, aliases or monikers, electronic mail (e-mail) addresses, telephone numbers, and other user and driver identifiers.

I know that Ring also retains Internet Protocol (“IP”) logs for a given user identity or IP address. These logs may contain information about the actions taken by the user identity or IP address on the Ring application, including information about the type of action, the date and time of the action, and the user identity and IP address associated with the action. For example, if a user views a Ring 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.

I am aware that this information is freely supplied by the user and required in order to create an account or use the services of Ring. I am also aware that in most cases this information is exclusively user supplied and not verified. Therefore, I realize some or all of the information may be fictitious. However, I am also aware that user supplied e-mail addresses and/or telephone numbers may go through a verification process wherein the user must confirm receipt of a message sent to their cell phone in order to access service.

I know from my own training and experience, from my own research, and from reviewing publicly available information that Ring generally collects and stores the following categories of information:

1. Basic subscriber information, such as information collected when a user creates a new Ring account, alters information at a later date, or otherwise interacts with the Ring application including but not limited to usernames, email addresses, passwords, personal identifying numbers (PINs), phone numbers, address, date of birth, gender, privacy settings, application settings, preferences, security questions, and answers to such security questions;
2. Profile information, usernames, nicknames, monikers, profile photographs, feedback, user comments, device information, driver’s license or other state-issued identification information, contact information, saved contacts, favorite contacts, address book(s), and linked social media accounts;
3. Device information, such as phone numbers, International Mobile Equipment Identity (IMEI) numbers linked to the accounts, the make, model, and operating system of any device used to connect to or use the application;
4. Billing information, including the means and sources of payment, such as linked credit cards, debit cards, and/or bank account information, as well as transaction information (including the date and time of transactions);
5. Communications information and data, including communications between users on the “Neighbors” Ring application, such as comments, sharing of videos, and alerts, as well as all information identifying the sender and recipient of any communications as well as the date and time of the communications, connected to the target account(s);
6. Internet Protocol (IP) address information, including IP address information regarding the IP address used at the time of account creation, and any IP address information stored by Ring for the creation of the account;
7. Customer service records, including communications between users and Ring customer support, whether by phone, text message, email, or internal application communications, and sometimes including recording of such communications.

I also know, from my training and experience, that it is common for individuals who utilize Ring to share access to their Ring devices with family members, friends, associates, etc. Because of this, your affiant is also seeking information for any Ring accounts connected to the target Ring accounts, listed above.

Your affiant is seeking evidence of ownership, use, and identification. Your affiant knows that ownership and control of a Ring profile can be placed at issue through a simple denial: “That is not my account.” In your affiant’s training and experience, some of the best ways to establish control are by searching all available service provider records. A photo/video gallery often contains self-taken photographs (commonly known as “selfies”) that clearly depict the owner/holder of the account. Communications via instant messages (“Neighbors”), and posts often identify the sender/recipient by name, additionally the context of the communications often identify the sender and/or recipient.

**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 Ring 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.

Ring, LLC 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 Ring, LLC 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 Ring, LLC 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 Ring, LLC 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:

**Ring, LLC**

**ATTN: Ring Legal Department, Custodian of Records**

**1523 26th Street**

**Santa Monica, CA 90404**

**Service via email at subpoenas@ring.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 Ring user identified as:

MAC Address: MAC ADDRESS

Account Holder: NAME

Physical Address: PHYSICAL ADDRESS

Phone Number: PHONE NUMBER

Email Address: EMAIL ADDRESS

between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. **Account information** – username(s), primary email address, secondary email addresses, connected applications and sites, and account activity for the **target date range(s) listed above**, including account sign in locations, browser information, platform information, internet protocol (IP) addresses, all privacy settings, other account settings (including online username(s) and passwords), and/or information used to access **Ring** products and services;
2. **Subscriber information** – all subscriber contact and personal identifying information, including but not limited to, full name, user identification number, birth date, gender, contact email address(es), security question(s) and answers(s), physical address (including city, state, and zip code), telephone numbers, and any other personal identifiers);
3. **All device information** – all mobile, computer, and/or surveillance device(s) used by, associated with, utilized by, and/or connected to the target account(s), including electronic serial number (ESN), integrated circuit card identification (ICCID) number, international mobile subscriber identity (IMSI) number, international mobile equipment identity (IMEI) number, media access control (MAC) address, and/or any other unique identifier, as well as connection logs, login and logout information, and activation dates;
4. **Account device information** – all devices attached to the target account(s), including cameras, doorbells, chimes, path lights, alarms, sensors, motion detectors, panic buttons, alarms, smart devices and beacons, along with product setup information, such as the name and description of the **Ring** product, the location(s) where the product(s) was/were installed, adjustments made during setup, Wi-Fi network information, and product details including the **Ring** product’s model, serial number, and software version;
5. **Service and financial information** – all information regarding types of service(s) utilized by the target account(s), the length of service(s) (including start date and/or activation date), the means and source of any payments associated with the service(s) (including any credit card or bank account numbers(s) or information, including expiration date and security code);
6. **Activity log information** – all activity logs for the target account(s) and data collected in connection with the target account(s), including “nearby incidents,” “history,” camera activity, event history, smart alerts, motions setting, device settings, and shared users for the above-described target date range;
7. **All device content**, including but not limited to any saved video and/or audio recordings, any captured surveillance images, any notification alerts, motion activation alerts, any “linked event” motion alerts, any “favorited” event alerts, any and all history notifications, and any stored dates and times (time stamps) for all device content;
8. **All internal communication data**, including but not limited to all data used in the “Neighbors” communication application, as well as all communications, shared images, shared video, and shared alerts as posted and/or shared by the target account during the above listed dates/times;
9. **All other identifying data, if collected by Ring,** including but not limited to any information on the device(s) used to access the target account(s), including the type of devices, model numbers, International Mobile Equipment Identifier (IMEI) numbers, phone numbers, Global Positioning System (GPS) locations, and/or Internet Protocol (IP) addresses.
10. All records pertaining to communications between Ring and any person regarding the user or the user’s Ring account, 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 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 Ring, LLC 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 Ring, LLC, **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