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

-This search warrant mask is specifically for the search of Coinbase cryptocurrency exchange for all data associated with an 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: XX-XXXXXXX

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:

CRYPTOCURRENCY EXCHANGE

ADDRESS

Service Via: METHOD OF SERVICE

There is the following records, data, or information for the EXCHANGE account(s) associated with the below-listed cryptocurrency transactions:

|  |  |
| --- | --- |
| **Sending Address** | SENDING WALLET OF TRANSFER INTO EXCHANGE WALLET |
| **Receiving Address** | EXCHANGE ACCOUNT RECEIVING WALLET ADDRESS |
| **TX Hash** | TRANSACTION HASH OF TRANSFER INTO EXCHANGE WALLET |
| **Unit** | CRYPTO TYPE/COIN/TOKEN |
| **Amount** | AMOUNT LISTED IN THE CRYPTO TYPE/COIN/TOKEN TRANSFERED |

|  |  |
| --- | --- |
| **Sending Address** |  |
| **Receiving Address** |  |
| **TX Hash** |  |
| **Unit** |  |
| **Amount** |  |

|  |  |
| --- | --- |
| **Sending Address** |  |
| **Receiving Address** |  |
| **TX Hash** |  |
| **Unit** |  |
| **Amount** |  |

between the dates of DATE (TIME ZONE) through DATE (TIME ZONE) for evidence of the crime of CRIME:

\*\*\*USE ONLY THOSE WHICH APPLY\*\*\*

1. Names, including subscriber names, usernames, and screen names;
2. Date(s) of birth;
3. Addresses, including mailing addresses, residential addresses, business addresses, and e-mail addresses;
4. Local and long-distance telephone connection records;
5. Records of session times and durations, and the temporarily assigned network addresses, such as Internet Protocol (IP) addresses associated with those sessions;
6. Length of service (including start date) and types of service utilized;
7. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (ESN), Mobile Electronic Identity Numbers (MEIN), Mobile Equipment Identifier (MEID), Mobile Identification Numbers (MIN), Subscriber Identity Modules (SIM), Mobile Subscriber Integrated Services Digital Network Number (MSISDN), International Mobile Subscriber Identifiers (IMSI), or International Mobile Equipment Identities (IMEI);
8. Other subscriber numbers or identities, including the registration Internet Protocol (IP) address;
9. Means and source of payment for such service (including any credit card or bank account number) and billing records;
10. Customer's account application;
11. Any identifying information used to establish accounts, to include copies of passports or any other government issued IDs;
12. Signature card;
13. Monthly billing statements;
14. Repayment records disclosing the dates, amounts and method (cash, check, money order or ACH [Automated Clearing House]) of repayment;
15. Full routing and account number for ACH repayments;
16. Correspondence received from or with customer;
17. The number of credit/debit cards issued and the names on the cards;
18. IP addresses used to open account;
19. Phone numbers used to check account balances or to speak with representatives;
20. Proof of residence provided by subject;
21. Any and all Know Your Client (KYC) files and data related to the subject;
22. Detailed transaction information;
23. Detailed account history information;
24. Any IP addresses captured during online access.

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 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.

“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.

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.

**Cryptocurrency Definitions**

“Cryptocurrency,” also referred to as "virtual currency,” or “digital currency,” is a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account, and a store of value. Unlike fiat currency, virtual currency is neither issued nor guaranteed by any jurisdiction and fulfills these functions only by agreement within the community of users of the virtual currency. "Cryptocurrency" is a form of virtual currency that relies on cryptography to create a secure record of transactions. Cryptocurrencies are typically distributed, open-source, peer-to-peer currencies with no central administrating authority that rely on a shared computer networking protocol. “Digital asset” is a term referring to currency or cryptocurrency held in digital form.

Bitcoin[[1]](#footnote-1) and Ether are two forms of decentralized, convertible cryptocurrency that exist through the use of online, decentralized ledger systems. While they mainly exist as Internet-based forms of currency, it is possible to “print out” the necessary information and exchange the cryptocurrency via physical medium. The cryptocurrency is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network.  To acquire cryptocurrency, a typical user will purchase it from another person or business entity. It is also possible to “mine” the cryptocurrency by verifying other users’ transactions. Bitcoin and Ether are just two forms of digital currency, and there are a significant number of other varieties.

When a user acquires cryptocurrency, ownership of the cryptocurrency is transferred to the user’s “public address” on the “blockchain” for that cryptocurrency. The “public address” is somewhat analogous to a bank account number and is comprised of a string of letters and numbers that is often dozens of characters in length (depending on the cryptocurrency). All transactions for Bitcoin, Ether, and many other cryptocurrencies are recorded on what is known as a “blockchain.” This is essentially a distributed public ledger that keeps track of all transactions for a given cryptocurrency, incoming and outgoing, and updates regularly (multiple times per hour). The blockchain records every address that has ever received a unit of that cryptocurrency and maintains records of every transaction for each public address. This is true for Bitcoin on the Bitcoin blockchain, and for Ether on the Ethereum blockchain. The integrity of the historical record on a blockchain is secured using cryptography.

Little to no personally identifiable information about the payer or payee is transmitted in a transaction on the Bitcoin or Ethereum blockchains.  These transactions occur using a public key and a private key. A public key (reflected in the public address) is used to receive units of the cryptocurrency, and a private key is used to allow withdrawals from a public address. This is done by using the private key in a cryptographic “digital signature” that provides for verification and non-repudiation, in that only a person or entity holding the private key corresponding to a given public address (public key) can provide a verifiable digital signature, and anyone in the Bitcoin or Ethereum network can use that digital signature to authenticate the transaction. Only the public address of the receiving party and the sender’s private key are needed to complete the transaction, which by themselves rarely reflect any identifying information.

Digital currencies, including Bitcoin and Ether, have many known legitimate uses. However, much like cash, these cryptocurrencies can be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which they can be used to move funds with high levels of anonymity. However, in some circumstances, payments using these cryptocurrencies may be traced to accounts at a cryptocurrency “exchange” or traditional financial institution using blockchain analysis.

A cryptocurrency “exchange,” also referred to as an “exchanger,” is a business that facilitates the conversion of cryptocurrency to cash or another type of cryptocurrency. An exchange typically accepts payments of fiat currency (currency which derives its value from government regulation or law) or other convertible digital currencies to obtain the desired cryptocurrency. When a user wishes to purchase, for example, bitcoins from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or ACH, or other convertible digital currency to an exchanger, for the corresponding number of bitcoins based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell bitcoins, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed. The user can then conduct transactions with other users of the cryptocurrency, by transferring bitcoins to their Bitcoin addresses, via the Internet.

As described above, ownership of cryptocurrency is established through the record of transfers between public addresses on a blockchain, and private keys are used to control the transfer of assets from those addresses.  A cryptocurrency “wallet” is document or piece of hardware or software that contains a set of cryptocurrency addresses and their corresponding private keys, which can be used to transfer funds from those addresses. The term “wallet” is also used to refer to an address or a collection of addresses that are controlled by the same entity.

“Pig Butchering” is a scam that involves online communication between a suspect and a victim which often, though not always, begins in the form of a purported online romantic relationship and then transitions into an investment scheme. The suspect convinces the victim to send cryptocurrency funds to a purported investment website or company, promising excellent returns on the investment, and in some cases the suspect provides fraudulent documentation or online viewing of said investment returns. The suspect then encourages the victim, referred to as the “pig,” to send increasing amounts of funds, with the goal of “fattening” up the “pig” for an eventual “butchering,” which is the term used to describe the end result of the suspect stealing the large victim’s cumulative funds. In reality, the investment does not exist, the website or documentation provided by the suspect is fraudulent, and the suspect is simply instructing the victim to send cryptocurrency funds to the suspect’s wallet address to facilitate theft. This scam is currently prevalent in the United States, and often involves suspects of international origin who utilize intricate movements of cryptocurrency across the digital landscape, including token swapping and mixing, to obfuscate and eventually monetize the stolen funds into fiat currency. It is possible for the suspects to monetize the stolen funds using accounts with either centralized or decentralized exchanges. These cryptocurrency exchanges often maintain account records in a fashion similar to that of commercial banking institutions.

**Statements Regarding Current Investigation**

BACKGROUND OF AFFIANT

PROBABLE CAUSE NARRATIVE

The below-listed transactions were identified as ultimately leading to a EXCHANGE wallet address(es). These transactions are identifiable by their TX (Transaction) hashes, which are unique identifiers that distinguish all transactions recorded on the blockchain from each other, and are akin to each transaction’s digital fingerprint. EXCHANGE wallet addresses are connected to EXCHANGE accounts assigned to users, and EXCHANGE maintains records of those accounts and their associated users. Therefore, I have probable cause to believe that EXCHANGE maintains under its control the above-listed items 1-24 associated with the listed transactions. Each of these items would assist this investigation in determining the identity of the suspect(s) who ultimately received the victim’s stolen funds in a EXCHANGE account, or in providing details that could further investigation into the suspect(s) identity, origin, and location.

|  |  |
| --- | --- |
| **Sending Address** |  |
| **Receiving Address** |  |
| **TX Hash** |  |
| **Unit** |  |
| **Amount** |  |
| **Date** |  |

|  |  |
| --- | --- |
| **Sending Address** |  |
| **Receiving Address** |  |
| **TX Hash** |  |
| **Unit** |  |
| **Amount** |  |
| **Date** |  |

|  |  |
| --- | --- |
| **Sending Address** |  |
| **Receiving Address** |  |
| **TX Hash** |  |
| **Unit** |  |
| **Amount** |  |
| **Date** |  |

Specifically, the account records identified in this Affidavit and requested Search Warrant are likely to reveal the following items that will aid the investigation as described below:

* Names, addresses, other contact information, length of service, and types of services utilized will aid in identifying the account holder and linking that person to other accounts such as email addresses and phone numbers, where additional evidence may be sought.
* Customer due diligence records (KYC) will aid in verifying the identity of the person in control of the identified account(s), which aid in the identification of the suspect.
* Information related to financial accounts related to the identified customer will aid in verifying the identity of the suspect and identifying additional repositories of evidence.
* Records of session times and durations, and user agent information and temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions will aid in identifying additional locations where evidence may be sought.
* Account notesused by the business to manage or document communication with the customer or other notes used for similar purposes will aid in evaluating the source and use of funds in the target account(s) and separating legitimate activity from money laundering activities.
* Transaction records, including current balances, transaction IDs, addresses utilized in deposit and withdrawal of digital currency, and order history will aid in linking the identified account(s) to this and other thefts, distinguishing such flows from legitimate patterns of activity, and locating ill-gotten funds.

Based on these facts, I believe there exists probable cause to believe that there is material evidence now maintained and in control of EXCHANGE that is crucial to the investigation of this case and the offenses described above, and a search warrant is requested pursuant to 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 production 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.

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

Electronic response via email preferred to: EMAIL ADDRESS

***Further requests:***

1. Pursuant to Crim. P. 41 and §16-3-304(2), I request 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, I also request that this Court order EXCHANGE 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), I request that EXCHANGE 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 \_\_\_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 at \_\_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE

Case No: XX-XXXXXXX

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 Carly Garner 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:

CRYPTOCURRENCY EXCHANGE

ADDRESS

Service Via: METHOD OF SERVICE

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 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 EXCHANGE provide following records, data, or information for the EXCHANGE account(s) associated with the below-listed cryptocurrency transactions:

|  |  |
| --- | --- |
| **Sending Address** | SENDING WALLET OF TRANSFER INTO EXCHANGE WALLET |
| **Receiving Address** | EXCHANGE ACCOUNT RECEIVING WALLET ADDRESS |
| **TX Hash** | TRANSACTION HASH OF TRANSFER INTO EXCHANGE WALLET |
| **Unit** | CRYPTO TYPE/COIN/TOKEN |
| **Amount** | AMOUNT LISTED IN THE CRYPTO TYPE/COIN/TOKEN TRANSFERED |

|  |  |
| --- | --- |
| **Sending Address** |  |
| **Receiving Address** |  |
| **TX Hash** |  |
| **Unit** |  |
| **Amount** |  |

|  |  |
| --- | --- |
| **Sending Address** |  |
| **Receiving Address** |  |
| **TX Hash** |  |
| **Unit** |  |
| **Amount** |  |

between the dates of DATE (TIME ZONE) through DATE (TIME ZONE) for evidence of the crime of CRIME:

\*\*\*USE ONLY THOSE WHICH APPLY\*\*\*

1. Names, including subscriber names, usernames, and screen names;
2. Date(s) of birth;
3. Addresses, including mailing addresses, residential addresses, business addresses, and e-mail addresses;
4. Local and long-distance telephone connection records;
5. Records of session times and durations, and the temporarily assigned network addresses, such as Internet Protocol (IP) addresses associated with those sessions;
6. Length of service (including start date) and types of service utilized;
7. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (ESN), Mobile Electronic Identity Numbers (MEIN), Mobile Equipment Identifier (MEID), Mobile Identification Numbers (MIN), Subscriber Identity Modules (SIM), Mobile Subscriber Integrated Services Digital Network Number (MSISDN), International Mobile Subscriber Identifiers (IMSI), or International Mobile Equipment Identities (IMEI);
8. Other subscriber numbers or identities, including the registration Internet Protocol (IP) address;
9. Means and source of payment for such service (including any credit card or bank account number) and billing records;
10. Customer's account application;
11. Any identifying information used to establish accounts, to include copies of passports or any other government issued IDs;
12. Signature card;
13. Monthly billing statements;
14. Repayment records disclosing the dates, amounts and method (cash, check, money order or ACH [Automated Clearing House]) of repayment;
15. Full routing and account number for ACH repayments;
16. Correspondence received from or with customer;
17. The number of credit/debit cards issued and the names on the cards;
18. IP addresses used to open account;
19. Phone numbers used to check account balances or to speak with representatives;
20. Proof of residence provided by subject;
21. Any and all Know Your Client (KYC) files and data related to the subject;
22. Detailed transaction information;
23. Detailed account history information;
24. Any IP addresses captured during online access.

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

Electronic response via email preferred to: EMAIL ADDRESS

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 EXCHANGE 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 EXCHANGE, **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 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 \_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_ at \_\_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE

1. Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an upper case letter B) to label the protocol, software, and community, and “bitcoin” or “bitcoins” (with a lower case b) to label units of the currency and that practice is adopted here. [↑](#footnote-ref-1)