

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

Premises located at 24 Grove Street, Lebanon, OR
as described in Attachment A

Case No. 6:25-mc-

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Premises located at 24 Grove Street, Lebanon, OR as described in Attachment A hereto,

located in the _____ District of _____ Oregon _____, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. §§ 841(a)(1), 846, 843, 843(c), and 18 U.S.C. § 1956(h)	Distribution of Controlled Substances, Conspiracy to Possess with the Intent to Distribute Controlled Substances, Illegal Use of a Communications Facility, Illegal Controlled Substance Advertisement, and Money Laundering Conspiracy

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- Continued on the attached sheet.
- Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ William Jake VonEssen, via Telephone
Applicant's signature

William Jake VonEssen, Special Agent DEA
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone at 11:51 a.m. _____ *(specify reliable electronic means)*.

Date: October 1, 2025

Amy E Potter
Judge's signature

City and state: Eugene, Oregon

Amy E. Potter, United States Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF WILLIAM JAKE VONESSEN

**Affidavit in Support of an Application
Under Rule 41 for a Search Warrant**

I, William Jake VonEssen, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Drug Enforcement Administration (DEA) and have been since January of 2022. As such, I am an “investigative or law enforcement officer” of the United States within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses enumerated in 18 U.S.C. § 2516. I am empowered to investigate, to make arrests with or without warrants and to execute search warrants under the authority of 21 U.S.C. § 878. I hold a bachelor’s degree in aerospace from Middle Tennessee State University. I have completed the DEA Basic Agent Training Academy, which is a 17-week course in Quantico, VA, that includes (but is not limited to) training in the following areas: surveillance, undercover operations, report writing, confidential source management, drug identification, legal principles, search warrant operations, case initiation and development, interview and interrogation, defensive tactics, physical training, and firearms proficiency. I continue to receive training on a daily basis by conducting criminal drug investigations and drawing from the expertise of agents more experienced than myself. Additionally, as a DEA Special Agent, my experience includes participating in criminal arrests, conducting physical surveillance, trash seizures, searching for evidence during court-authorized search warrants, authoring search warrants, court orders, and subpoenas, conducting interviews, and conducting open-source research as well as research from law enforcement databases. I have participated in several trainings on topics such as financial/money laundering investigation,

Affidavit of William Jake VonEssen **Page 1**

asset forfeiture, online/cyber investigation, technical operations (covert surveillance deployment and monitoring, undercover audio/video ‘bugs’, and basic networking), mobile device forensic extraction and analysis examination, and cryptocurrency exploitation. I am currently assigned to the Columbus Cyber Narcotics Joint Task Force (CNJTF) in Columbus, OH (which consists of investigators with the Drug Enforcement Administration (DEA), Immigration and Customs Enforcement – Homeland Security Investigations (HSI), United States Postal Inspection Service (USPIS), Internal Revenue Service – Criminal Investigations (IRS-CI), Franklin County Sheriff’s Office (FCSO), and Upper Arlington Police Department (UAPD)).

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises at 24 Grove Street, Lebanon, OR 97355, which is described as a two-story residence that is off-white in color with blue trim (hereinafter “the TARGET RESIDENCE”), as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) Distribution of Controlled Substances, 21 U.S.C. § 846 Conspiracy to Possess with the Intent to Distribute Controlled Substances, 21 U.S.C. § 843(b) Illegal Use of a Communications Facility, and 21 U.S.C. § 843(c) Illegal Controlled Substance Advertisement, and Money Laundering Conspiracy 18 U.S.C. § 1956(h) (hereinafter “Target Offenses”). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located at the TARGET RESIDENCE.

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. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from

other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offenses

4. I believe there is probable cause to believe that evidence of the following violations will be found in the places to be searched:

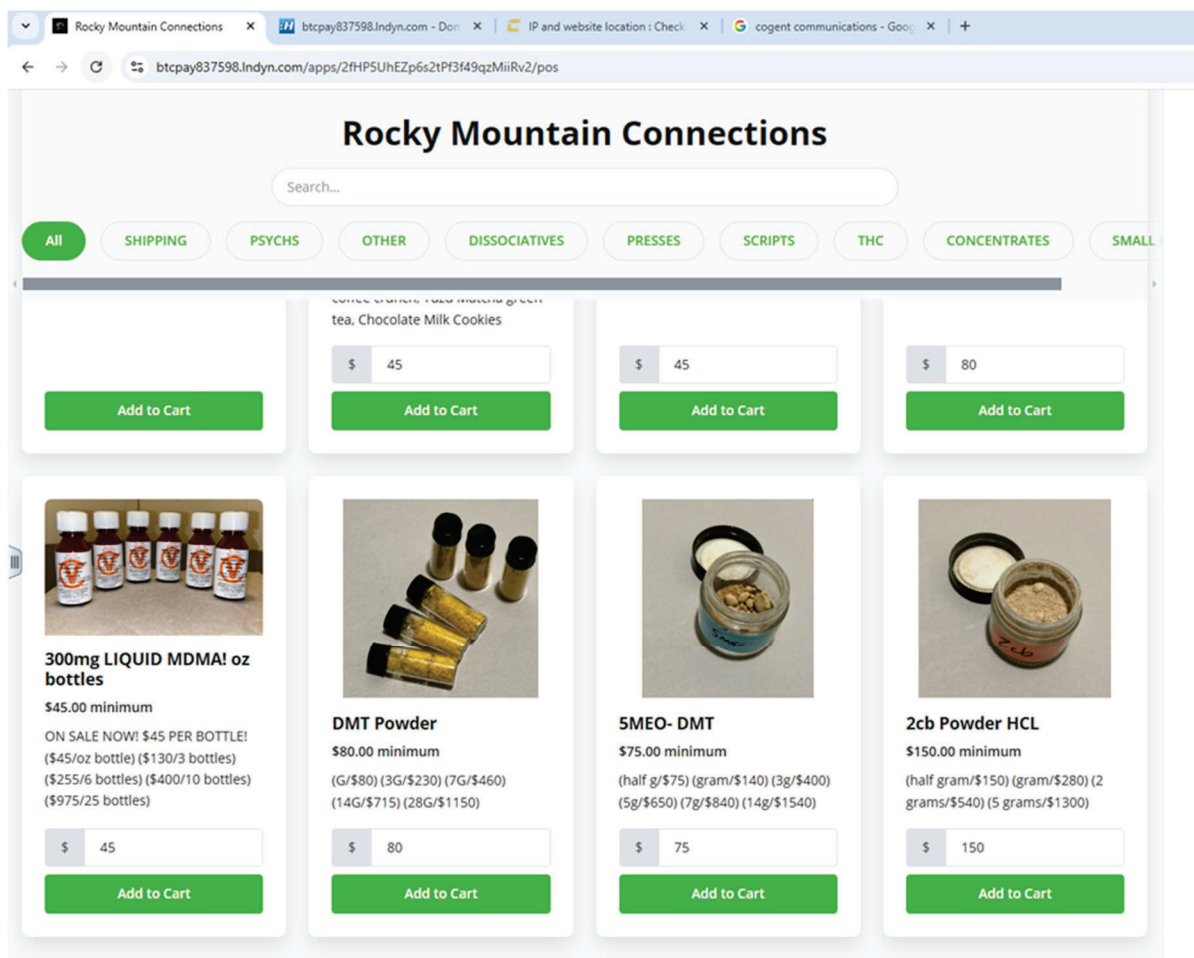
- 21 U.S.C. § 841(a)(1) prohibits the possession with intent to distribute illegal drugs.
- 21 U.S.C. § 846 prohibits conspiring to commit a violation of 21 U.S.C. § 841.
- 21 U.S.C. § 843(b) prohibits the use communications facilities (such as the United States Postal Service (USPS)) to facilitate drug trafficking.
- 21 U.S.C. § 843(c) prohibits advertising the sale of controlled substances online.
- 18 U.S.C. § 1956(h) prohibits laundering of drug proceeds.

Statement of Probable Cause

ROCKY MOUNTAIN CONNECTIONS DRUG MARKETPLACE

5. In March of 2025, investigators with the Columbus CNJTF observed a domain named 'rmp.supply' on a known drug trafficker's encrypted messenger app profile. The known drug trafficker had the domain 'pinned' in the 'bio' section of their profile, indicating that they were highlighting and bringing attention to this domain. When CNJTF investigators navigated to 'rmp.supply', they were automatically redirected to a new domain 'btcpay837598.lndyn.com/apps/2fHP5UhEZp6s2tPf3f49qzMiiRv2/pos'. This domain's content

showed a drug marketplace named ROCKY MOUNTAIN CONNECTIONS, which offered several types of drugs for sale, such as methamphetamine, cocaine, illicit pharmaceuticals, DMT, LSD, mushrooms, MDMA, ketamine, cannabis, and various other drugs. Although the domain is setup to facilitate the sale of drugs, the domain mirrors that of a normal online store selling legal goods, in that customers can navigate the webpage, view drugs by category, and browse listings that each include a picture of the drug, its name, and a price to quantity breakdown. For example:



6. RMC uses a service called 'BTCPay' to process transactions, in which customers can choose to pay with Bitcoin, Litecoin, or Monero (all types of cryptocurrency). BTCPay is

an open-source cryptocurrency payment processing system, much like a point-of-sale system or cash register in a ‘brick and mortar’ style store. Once a customer makes a purchase of drugs from RMC, BTCPay’s system automatically provides a cryptocurrency address and the customer is expected to pay the required amount, and if successful, is provided an order and invoice number. BTCPay is not ‘custodial’, in that BTCPay personnel do not control the cryptocurrency or take custody of it. BTCPay is simply a payment processing system that users can set up to take cryptocurrency payments. The user setting up BTCPay to take payments for whatever they use it for is the custodian of the cryptocurrency. BTCPay itself recommends the use of a software wallet called ‘Electrum’ to facilitate cryptocurrency addresses for payment. Directions are provided to users that they should first setup a cryptocurrency wallet in ‘Electrum’, then provide the ‘master public key’ of the wallet to BTCPay before deploying it to the user’s eCommerce domain. This will allow payments to be facilitated by BTCPay and cryptocurrency to be sent to the user’s software wallet. ‘Electrum’ is a non-custodial software wallet and provides each user with a ‘private key’ (represented both by the actual private key, which is often a sixty-four-character string of numbers and letters, and by a ‘seed phrase’ of ‘seed words’).

7. CNJTF investigators have conducted four undercover purchases of drugs from RMC, using Bitcoin (BTC) cryptocurrency to pay for the drugs and shipping. All four purchases were facilitated by BTCPay, and unique Bitcoin addresses were generated for each purchase. All four purchases were shipped from the western Oregon area of the United States, and were all delivered and seized in the Columbus, OH, area (the Southern District of Ohio). The first undercover purchase took place in March of 2025, when CNJTF investigators

purchased/seized 185.53 grams of counterfeit methamphetamine pills and 1.57 grams of LSD. The second purchase took place in April of 2025, when CNJTF investigators purchased/seized 29.09 grams of cocaine and 23.22 grams of alprazolam. The third purchase took place in June of 2025, when CNJTF investigators purchased/seized 420.35 grams of counterfeit methamphetamine pills. The fourth purchase took place in August of 2025, when CNJTF investigators purchased/seized 911.1 grams of counterfeit methamphetamine pills. Based on my training and experience, I know that LSD is a federally controlled schedule I substance, methamphetamine and cocaine are schedule II controlled substances, and alprazolam is a schedule IV controlled substance.

8. All four undercover purchases were shipped by RMC using the United States Postal Service (USPS) and had nearly identical ‘stealth’ techniques and packaging. ‘Stealth’ refers to the manner in which an online drug vendor ships drugs in the mail, specifically the quantity and quality of concealing materials the vendor hides within the package along with the drugs in order to make the package look and feel like a normal USPS package. The return address that was listed on the label affixed to the package that contained the first undercover purchase (containing LSD and methamphetamine) was ‘HARRY’s, 2201 Lloyd Center, Portland, OR’. The return address that was listed on the label affixed to the package that contained the second undercover purchase (containing cocaine and alprazolam) was ‘APPLE-A-DAY, 293 Valley River Center, Eugene, OR’. The return address that was listed on the label affixed to the package that contained the third undercover purchase (containing methamphetamine) was ‘COMMON HEALTH 12000 SE 82nd Avenue, Happy Valley, OR’. The return address that was listed on the label affixed to the package that contained the fourth undercover purchase

(containing methamphetamine) was ‘SCHOOL ZONE, 2201 Lloyd Ctr., Portland, OR’ (the same return address, albeit a different fictitious business name, as the first undercover purchase).

Based on my training and experience, shippers of drugs and drug proceeds will often utilize a fictitious return name and/or address to reduce the possibility of identification and apprehension by law enforcement.

9. On the RMC domain, CNJTF investigators observed a link to a page that included a contact information section for RMC. The page listed the contact email address for RMC as ‘rockymtnpsych@protonmail.com’. In addition to the email address, there were several other references on the domain indicating that ROCKY MOUNTAIN CONNECTIONS used to be named ‘ROCKY MOUNTAIN PSYCHEDELICS’, such as on their ‘policy and Faq page’:

Rocky Mountain Psychedelic information

Policy and Faq

1. Payment Policy

Accepted Payment Methods: Currently accept BTC, LTC and XMR. Doesn't matter where the cyprto comes from, if you are able to send BTC, etc - it will work.

2. Shipping Policy

Processing Time: Orders are processed within 1-2 business days. Don't ask when your pack went out. I don't care to discuss things that can ruin OPSEC - You will be ignored.

Shipping Methods: At this time, USA to USA only, USPS. I do not do Express shipping - don't ask.

Shipping Costs: Shipping cost is \$15, make sure to add it to your cart when checking out.

If package is returned to sender: Due to incorrect address information provided, will not reship. If we mess up your address, we will reship. If pack is seized (zero at this time), we will reship. If USPS does not scan in a package and loses it, after 4 weeks of no product movement, you can pay for half of the original order and we will cover the other half out of pocket.

3. Tracking Policy

Tracking is not provided. If you have not received your order AFTER 14 days, please reach out so that we may locate your package.

Make sure to sign up for informed delivery through <https://www.usps.com/manage/informed-delivery.htm>

[ftag=MSF0951a18&msockid=2b8a80c2b80f640d32509446b9b4657a](#) (know that informed delivery is not always accurate - do not come yell at me because it isn't updated)

In addition, below shows RMC’s contact information page, which shows connections between RMC and ROCKY MOUNTAIN PSYCHEDELICS:

All my contact information

Proton Email: rockymtnpsych@protonmail.com

Signal: rockymtnconnections.11

Session: (direct contact, no channel)

05112487e4c92d84f5729063312ff8cc6e013daa4cb73cccacc1244797176edd2c

Potato Channel:

(must send me a message for the channel link, this is where I keep everything up to date and post about giveaways)

Potato Contact

@rockymtnpsychv2 - this is my ONLY contact for potato.

Luffa: (Direct contact, no channel)

5YfqutUnzFX

Rocky Mountain Chat Group: - located on SimpleX -Must message for link

MY PGP CODE

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User ID: Rocky Mountain Connections rockymtnpsych@protonmail.com
Comment: Valid from: 7/18/2025 9:07 AM
Comment: Valid until: 7/18/2028 12:00 PM
Comment: Type: 255-bit EdDSA (secret key available)
Comment: Usage: Signing, Encryption, Certifying User IDs
Comment: Fingerprint: 89A04581F45AD061AED00E12EC7850B5AAC411B1

mDMEaHpxJRYJKwYBBAHARw8BAQdABU2BvrdE8tqYEaRqoXSHs9fju+BHVI+/mt+i
gmFMEoi0OVJvY2t5IE1vdW50YWluIENvbm5lY3Rpb25zIDxyb2NreW10bnBzeWN0
QHByb3RvbmlhaWwvY29tPoiZBBMWCgBBFIEEiaBFgFRa0GGu0A4S7HhQtarEEbEF
Amh6cSUCGwMFCQWIFsFCwklBwlClgIGFQoJCAcCBBYCAwECHgcCF4AACgkQ7HhQ
tarEEbHcDAEAyN3EOqQuMMDf2dP1HeDiW+aNBzGwvHr+OUAYX1wdb9MBAOI7gfai
r89NgtcYdkq5/9TH/y9SjymF1BVbBs+0YLMGuDgEaHpxJRIKKwYBBAGXVQEFAQEH
QLiClyA2ov18jHqq2uHx8VZRHXfH64eoK2T7nAaMB/9xAwEIB4h+BBgWCgAmFiEE
iaBFgFRa0GGu0A4S7HhQtarEEbEFAmh6cSUCGwwFCQWIFsACgkQ7HhQtarEEbHq
CgEA5JstJypEQKrnqyt8LUe/YX5JGNE+63zxG4hkMj6U9dkA/OA8lq+j8rm02WZC
N2l6lxeG21V25NRsOKQ5TY6prBIC
=DazM
-----END PGP PUBLIC KEY BLOCK-----

```

10. Notably, the above indicates that the email associated with RMC is rockymtnpsych@protonmail.com, and that those associated with the RMC site also use Session, Signal, Potato, and Luffa, among other applications, to communicate with their customer base. Based on my training and experience, I know that ‘Proton’ is a popular email service for online

drug vendors due to its emphasis on privacy and encryption. I also know that ‘Session’, ‘Signal’, ‘Potato’, Luffa’, and ‘SimpleX’ are all encrypted messenger apps that emphasize privacy and security for users. Based on my training and experience, I am aware that all the mentioned apps are popular with online drug vendors for this reason as well.

IDENTIFYING THE MEMBERS INVOLVED WITH ROCKY MOUNTAIN
CONNECTIONS

11. Per Colorado Secretary of State business records, Jesse WASSON incorporated a business named ‘Rocky Mountain Psychedelics LLC’ on September 20, 2023, which was dissolved on June 21, 2024. Per open-source research, Jesse WASSON is married to Shea WASSON and lives with her at 5846 Flintwood Road, Unit B, Parker, CO. Another historical address for both of the WASSONs is 1991 S. Wolff Street, Denver, CO, which is also where ‘Rocky Mountain Psychedelics LLC’s listed street address, mailing address, and registered agent’s street and mailing address were located. In addition, the investigation has identified an online account named “Rockychoc” on a website called the Drug Buyer’s Guide (DBG). The DBG is an online forum where individuals can post about drugs and drug dealing. The investigation has indicated that Rockychoc is affiliated with RMC. In the Rockychoc “about me” section, it lists a link to the RMC domain and lists the rockymtnpsych@protonmail.com email address. There were posts by Rockychoc from in or around January 2024 on the DBG. The posts make clear that “Rockychoc” were holding themselves out as a new online drug vendor open for business. Up until the present, Rockychoc, which is likely RMC, has made regular advertisements related to drug trafficking on the DBG.

12. Through postal data analysis/research, CNJTF investigators located a USPS online account with a listed email address of 'rockymtnpsych@protonmail.com', a telephone number (303) 474-2626, the name 'Emily Breslin', and an address of 586 Grove Street, Lebanon, OR, that was created in March of 2025. Lebanon, OR is near the return addresses listed on the shipping labels of undercover purchases made by the CNJTF. Per an administrative subpoena served onto Castle Property Management (the company that oversees/rents out the property of 586 Grove Street, Lebanon, OR), the listed tenants (since December of 2023) of 586 Grove Street (as of June 17, 2025) were Amanda HEFFELFINGER (also seen as 'Amanda Sansone' and 'Amanda Borman') and Jennifer BLAKE. HEFFELFINGER's listed telephone number with Castle Property Management was (503) 888-8288 and BLAKE's listed telephone number was (707) 365-5526. Per a Gmail search warrant served onto Google for content associated with HEFFELFINGER's Gmail account, CNJTF investigators know that BLAKE and HEFFELFINGER moved from 586 Grove Street, Lebanon, OR, to 24 Grove Street, Lebanon, OR (the TARGET RESIDENCE), in June of 2025. CNJTF investigators know they purchased the residence per Linn County, OR Geographic Information Systems (GIS).

13. As the case has progressed, CNJTF investigators have observed fewer references to ROCKY MOUNTAIN 'PSYCHEDELICS', and more references to 'CONNECTIONS'. As a result, CNJTF investigators believe that ROCKY MOUNTAIN CONNECTIONS used to be called ROCKY MOUNTAIN PSYCHEDELICS, and that the co-conspirators have slowly been updating their monikers and other information to reflect such. As explained throughout this affidavit, law enforcement has identified several connections between RMC, Jesse WASSON, Shea WASSON, HEFFELFINGER, and BLAKE.

14. Per an administrative subpoena served onto T-Mobile in June of 2025 for toll data and basic subscriber information, the listed subscriber for both HEFFELFINGER's telephone number and BLAKE's telephone number is 'Amandra Sansone' at '345 Taylor Drive, Newberg, OR'. Per open-source research, 'Sansone' is a last name for HEFFELFINGER from a previous relationship, and 345 Taylor Drive is a previous listed address for her. Per open-source information and the federal Google search warrant return for content associated with HEFFELFINGER's Gmail account, HEFFELFINGER appears to be in a relationship with BLAKE and that they moved to the TARGET RESIDENCE in May of 2025.

15. Per administrative subpoenas served onto T-Mobile in August of 2025 for toll data and basic subscriber information, the listed subscriber for both (303) 564-9029 and (720) 233-5968 is Shea WASSON at 5846 Flintwood Road, Unit B. Per a federal grand jury subpoena served onto Payward Interactive, Inc. (better known as 'Kraken'), Jesse WASSON listed their telephone number as the (303) 564-9029 and Shea WASSON listed her telephone number as (720) 233-5968. CNJTF investigators are also aware per open-source research that Jesse WASSON's telephone number used to be (702) 580-0734, but was disconnected around the time that (303) 564-9029 began use. As a result, CNJTF investigators believe that Jesse WASSON is the user of (303) 564-9029 (and used to be the user of (702) 580-0734 when it was in service) and Shea WASSON is the user of (720) 233-5968.

16. Per toll analysis, Jesse WASSON and Shea WASSON, both contact each other frequently—approximately two-hundred sixty (260) times from April to August of 2025. BLAKE and HEFFELFINGER also frequently contact each other—approximately three-hundred thirty-six (336) times from May to August of 2025. Also, relevant here, Jesse WASSON was in

contact with BLAKE approximately one-hundred one (101) times from April of 2025 to August of 2025, likely regarding RMC drug operations and orders.

17. Per an administrative subpoena served onto Southwest Airlines, HEFFELFINGER, BLAKE, and Jesse WASSON were all in Las Vegas, NV from May 4, 2025, to May 6, 2025. Per a Gmail search warrant for information associated with HEFFELFINGER's Gmail account served onto Google, the reason for the travel was for a wedding between BLAKE and HEFFELFINGER. CNJTF investigators located numerous group pictures from the wedding that showed BLAKE, HEFFELFINGER, and Jesse WASSON together. In addition, Shea WASSON was also listed on the 'RSVP' for the wedding as being the 'mixologist' for the wedding. Per a federal iCloud search warrant, investigators know that Shea WASSON did not attend the wedding, despite being invited.

ATTRIBUTING THE ROLES OF EACH MEMBER TO THE ROCKY MOUNTAIN
CONNECTIONS DRUG TRAFFICKING ORGANIZATION

18. In June of 2025, when CNJTF investigators conducted the third undercover purchase of 420.35 grams of counterfeit methamphetamine pills from RMC, CNJTF investigators used Bitcoin to pay for the drugs and shipping. The RMC domain via BTCPay directed the undercover investigator to deposit the Bitcoin to pay for the counterfeit methamphetamine pills into a Bitcoin address ending in 'rlq0'. CNJTF investigators successfully paid the address ending in 'rlq0' the required Bitcoin, and several hours later, the undercover CNJTF investigator received a message from the RMC Potato account (username – ROCKY MOUNTAIN) that indicated that the undercover order was confirmed. Several hours later, the Bitcoin used to pay for the counterfeit methamphetamine pills was moved to another

Bitcoin address ending in '3etg', where it was combined with other funds, totaling \$6,936 worth (at the time of the transactions) of Bitcoin. Several hours after that, that Bitcoin was moved from '3etg' to a Bitcoin address ending in 'J3r2', which is a Bitcoin address associated with a cryptocurrency swapping service called 'ChangeNow', indicating the user moved the Bitcoin with the intent to 'swap' the Bitcoin with another cryptocurrency. ChangeNow is a 'swapping service', which allows users to efficiently 'trade' one cryptocurrency for another. For example, a user could take \$100 worth of Monero, send it to ChangeNow, and 'trade' it for \$100 (minus a fee) worth of another cryptocurrency, such as Bitcoin. Per an administrative subpoena served onto ChangeNow, the Bitcoin used to purchase the counterfeit methamphetamine pills, along with other 'co-mingled' funds in '3etg', was swapped to Monero. Based on my training and experience, this is a popular tactic amongst online drug vendors and cryptocurrency money launderers since it effectively conceals the source and nature of funds by obfuscating the flow of the cryptocurrency, since Monero is a privacy-based cryptocurrency that keeps a substantial amount of transaction data 'off-chain' (unlike Bitcoin or Litecoin), meaning that investigators cannot effectively 'trace' it. Monero is favored by online drug vendors due to this, and Monero has extremely little legal purpose/use. The value of Monero can fluctuate like any cryptocurrency, or a stock, but it is not considered a popular investment option. Per that same administrative subpoena, ChangeNow provided the IP address that was used to execute the swap as 216.147.125.226 and provided the date/time for the swap as approximately 18:54:06 UTC on June 17, 2025. Per a federal grand jury subpoena served onto Starlink (the internet service provider that maintains IP address 216.147.125.226), the customer assigned IP address 216.147.125.226 with source port 50683 on June 17, 2025, at 18:54:12 UTC is listed as Shea

WASSON at 5846 Flintwood Road, Unit B. Furthermore, CNJTF investigators are aware of a Discord account that lists ‘rockymtnpsych@protonmail.com’ as the account’s email address (username – ‘ROCKY MOUNTAIN’). Per a federal 2703(d) court order, on June 13, 2025, at 12:47:09 UTC, the Discord account associated with the ‘rockymtnpsych@protonmail.com’ email address logged in using IP address 216.147.125.226. Per that same federal grand jury subpoena referenced above, 5846 Flintwood Road, Unit B’s assigned IP address at that time was also 216.147.125.226 with source port 52793. It should be noted that Starlink uses a system that allows anywhere from 50 to 100 customers to use the same IPv4 address at the same time. However, the odds that one of those 50 to 100 customers were also using their Starlink internet service to access ChangeNow to initiate a cryptocurrency swap on June 17, 2025, at 18:54:12 UTC and that one of those 50 to 100 customers logged into Discord on June 13, 2025, at 12:47:09 UTC, at the same moment as 5846 Flintwood Road, Unit B’s internet router is extremely unlikely.

19. Throughout July and August of 2025, CNJTF investigators have served Payward Interactive, Inc. (Kraken) with federal grand jury subpoenas for information regarding HEFFELFINGER’s, BLAKE’s, Jesse WASSON’s, and Shea WASSON’s Kraken accounts. Kraken is a cryptocurrency ‘exchange’ (or ‘VASP’, a virtual asset service provider). Kraken offers customers the ability to purchase cryptocurrency, send/receive cryptocurrency to/from other users (whether they have Kraken accounts or not), and/or ‘cash out’ their cryptocurrency in exchange for U.S. currency, along with other options. Upon viewing the responses, CNJTF investigators observed that all four individuals have used Kraken to engage in suspicious activity

that is indicative of money laundering (examples below). In addition, Jesse WASSON listed their contact email address with their old Kraken account as 'rockymtnpsych@protonmail.com'.

20. HEFFELFINGER and BLAKE's Kraken accounts were both activated in early 2025 (January and February of 2025), and both accounts have exclusively used Monero. From January of 2025 to July of 2025, BLAKE received 172.80 Monero over the course of fifteen deposits. After nearly every deposit, BLAKE exchanged the Monero for U.S. currency (totaling approximately \$46,345) within forty-eight hours. The U.S. currency was then wired to a Bank of America account within forty-eight hours of receiving the Monero. From February to July of 2025, HEFFELFINGER received 233.59 Monero over the course of fifteen deposits. After nearly every deposit, HEFFELFINGER exchanged the Monero for U.S. currency (totaling approximately \$66,940) within forty-eight hours. The U.S. currency was then wired to a Bank of America account within forty-eight hours of receiving the Monero. The Monero deposits appear to be indicative of being paid like an employee, since the amounts are somewhat similar (thirteen of the fifteen deposits were between 12 and 18 Monero) and occurred on a schedule (usually every three weeks or so). This activity is not indicative of investing (since the Monero is received from an outside source and is not held for a long period of time) and appears to be indicative of money laundering, as they appear to be using Monero to conceal the source of the funds before cashing it out into their bank accounts.

21. Jesse WASSON's older Kraken account was activated in November of 2023, but she didn't start receiving Monero on the account until May of 2024. Jesse WASSON's second, newer account was activated in July of 2025. Jesse WASSON has received 920.45 Monero, 0.74696990 Bitcoin, and 0.09083633 Bitcoin Cash from May of 2024 to July of 2025. After

nearly every deposit, Jesse WASSON began exchanging the Monero, Bitcoin, and Bitcoin Cash for U.S. currency (totaling approximately \$233,913) within forty-eight hours. Nearly all of U.S. currency was then wired to bank accounts, with less than \$3,000 in U.S. currency remaining between both of Jesse WASSON's accounts (at the time the subpoena was served). This activity is not indicative of investing (since the Monero and other cryptocurrency are received from an outside source and is not held for a long period of time) and appears to be indicative of money laundering, as she appears to be using Monero to conceal the source of the funds (drugs orders made on RMC) before cashing it out into their regular bank accounts.

22. Per a federal grand jury subpoena served onto Wells Fargo for financial records associated with HEFFELFINGER and BLAKE, CNJTF investigators know that HEFFELFINGER and BLAKE are school psychologists, since CNJTF investigators observed an application for an auto loan dated August 30, 2024. The returned financial records from Wells Fargo specifically included HEFFELFINGER and BLAKE's employment and salary information as a part of the loan application. CNJTF investigators observed that HEFFELFINGER reported an income of \$69,996 per year from her employment with the Linn-Benton-Lincoln Education School District. BLAKE reported an income of \$55,992 per year from her employment with the Eugene 4J Student Services Department. Per a grand jury subpoena served onto Canvas Credit Union, Jesse WASSON described their employment as a 'veterinary technician' at 'Mesa Animal Hospital' in 2023 and reported a yearly income of \$54,000. Per federal grand jury subpoenas served onto Kraken, Jesse WASSON listed their occupation as 'self-employed' on their first Kraken account, then listed their occupation as 'hospitality' on their second, newer Kraken account. The amount of cryptocurrency received by the individuals is not conducive to

their reported income to the above-mentioned financial institutions, further indicating that the cryptocurrency they receive is drug proceeds.

23. CNJTF investigators have served Google with a search warrant for information associated with a Gmail account belonging to HEFFELFINGER and have served an Apple search warrant for information associated with the iCloud account belonging to BLAKE. CNJTF investigators located the following in BLAKE'S iCloud—cryptocurrency addresses, cryptocurrency transaction hashes, and saved contact cards for Jesse WASSON and Shea WASSON. CNJTF investigators located the following in HEFFELFINGER'S Gmail account—pictures of bulk amounts of vacuum-sealed bags, evidence of usage on 'cryptopostage.info' for bulk amounts of third-party postage paid with Bitcoin, and pictures of packages received at 586 Grove Street bearing a fictitious name. CNJTF investigators also served Apple with a search warrant for content and information associated with the iCloud account belonging to Jesse WASSON. CNJTF investigators found the following relevant information in Jesse WASSON'S iCloud—pictures of books and pdfs about how to be a drug trafficker (many specifically about how to be an online drug vendor, including titles such as 'Best Resources for Trappers', 'DontLacknSlip, and 'USPSSecrets'), artwork for ROCKY MOUNTAIN PSYCHADELICS, a 'temp.pm' message that appeared to be sent to Jesse WASSON where the message sender addressed them as 'Rocky' and inquired about placing a drug order, artwork of 'ROCKY MOUNTAIN PSYCHEDELICS' that matches 'ROCKY MOUNTAIN CONNECTIONS' branding (a bear alongside mountains), and cryptocurrency seed phrases.

24. The investigation has indicated that Jesse WASSON, Shea WASSON, HEFFELFINGER, and BLAKE are drug traffickers that conspire together and 'constitute' (at

least in-part) the RMC DTO. CNJTF investigators also know that all drug payments made to RMC are made in cryptocurrency, specifically Bitcoin, Litecoin, or Monero. CNJTF investigators know that Jesse WASSON and/or Shea WASSON have taken Bitcoin used to make a purchase of suspected counterfeit methamphetamine pills from RMC and have swapped it to Monero, effectively laundering it since further movement of the money is concealed due to the nature of Monero. CNJTF investigators also know that Shea WASSON is listed on the customer contact information for the internet service at 5846 Flintwood Road, Unit B, that was used to execute that swap. Finally, CNJTF investigators know that Jesse WASSON, Shea WASSON, HEFFELFINGER, and BLAKE are appearing to receive Monero, launder it, and wire it to their respective bank account(s) all in a nearly identical manner.

25. In August of 2025, the RMC official 'feed' on encrypted messenger app 'Potato' announced that RMC would be on 'vacation' from August 1-13 and that the shop would not be shipping orders during that time. This 'feed' is from the official RMC account that is advertised on the RMC domain, and provides updates about shop closures, new stock, availability of products, and news. However, RMC stated that 'pints' and 'breakdown weed' would not be affected by the shop closure and could still be ordered and fulfilled as normal. Based on my training and experience, along with my knowledge of the specific case, 'pints' refer to promethazine and codeine syrup and 'breakdown weed' refers to cannabis available for purchase in 'ounce' quantities. Based on my training and experience, I know that cannabis is a federally controlled schedule I substance, and promethazine, when combined with codeine, is considered a schedule V substance. Both products are available for purchase from the RMC domain. CNJTF investigators previously served T-Mobile with prospective geolocation (ping) warrants on

BLAKE and HEFFELFINGER's cellular devices, starting on July 10, 2025. Throughout a majority of the ping's duration, BLAKE and HEFFELFINGER have been located in the Lebanon, OR area and surrounding towns (Eugene, Corvallis, Albany, etc.), but on August 3, 2025, HEFFELFINGER appeared to fly from Eugene, OR, to Phoenix, AZ, with a brief stop in Las Vegas, NV. Then, on August 6, 2025, BLAKE appeared to leave via a vehicle from Lebanon, OR, to Vacaville, CA, around the same time HEFFELFINGER began to appear to drive from Phoenix, AZ, to Vacaville, CA. After both spending time in Vacaville, CA, the two returned to Lebanon, OR, on August 10, 2025. Per two different T-Mobile search warrants for historical location information and prospective geolocation information, investigators know that Jesse and Shea WASSON remained in the area of 5846 Flintwood Road, Unit B, for a majority of the period between August 1 and August 13. This indicates that both HEFFELFINGER and BLAKE possess a majority of the drugs for sale from RMC, and that Jesse and Shea WASSON possess the 'pints' and 'breakdown weed' for sale at 5846 Flintwood Road, Unit B.

FURTHER ATTRIBUTION OF HEFFELFINGER, BLAKE, AND JESSE WASSON

26. On August 18, 2025, CNJTF investigators conducted an undercover purchase of 911.1 grams of counterfeit methamphetamine pills from the RMC domain. A few hours later, the undercover investigator received a message indicating that the order was confirmed. Several hours after the order was placed, at 2:20 p.m. (all times in this paragraph are in Pacific Daylight Time), investigators with the DEA Eugene Resident Office and USPIS Grants Pass office observed BLAKE appear from the TARGET RESIDENCE with approximately four large tote bags. She subsequently loaded her 2017 gray Hyundai Santa Fe that was parked in the driveway of the TARGET RESIDENCE with the tote bags. A few minutes later, BLAKE and

HEFFELFINGER entered the Santa Fe with their dog and departed the area. At approximately 2:34 p.m., the Santa Fe arrived at the Mr. Nice Guy cannabis dispensary at 700 Park Street, Lebanon, OR. At approximately 2:39 p.m., investigators observed HEFFELFINGER appear from Mr. Nice Guy, enter the Santa Fe's passenger seat, and depart the area. A few minutes later, the Santa Fe arrived at the USPS post office located at 55 Walker Road, Lebanon, OR. Investigators observed BLAKE remove several tote bags from the Santa Fe, then enter the post office. Approximately eight minutes later, investigators observed BLAKE exit the post office with empty bags, enter the Santa Fe, and depart the area. Investigators then followed the Santa Fe to Sweet Home, OR, where the Santa Fe once again arrived at a USPS post office located at 1303 Long Street, Sweet Home, OR at 3:07 p.m. BLAKE repeated what she did at the Lebanon post office, taking tote bags from the Santa Fe into the post office, then coming out of the post office with empty bags minutes later, and departing the area. During this surveillance, the pings operating on the HEFFELFINGER's and BLAKE's cell phones mirrored their locations. Based on my training and experience, I know that this suspicious behavior is indicative especially of online drug vendors. Visiting numerous post offices and dropping off large amounts of packages when not engaged in a legal/normal online business is behavior indicative of dropping off drug orders. USPIS Grants Pass seized two packages that BLAKE appeared to drop off, one from each post office that she was observed visiting.

27. The next day, USPIS Grants Pass applied for, and was granted a search warrant drawn out of the District of Oregon to search the contents of two packages, one that was dropped off by BLAKE at the Lebanon post office, and one that was dropped off by BLAKE at the Sweet Home post office. USPIS Grants Pass executed the search warrant and observed 119.4 grams of

cocaine, 273.7 grams of phenazolam, 422.7 grams of counterfeit methamphetamine pills, 160 gross grams of suspected MDMA, 70 gross grams of suspected diverted pharmaceuticals (Ambien), within the two packages, which were subsequently seized. The return address that was listed on the label affixed to each seized package was 'THE CAT'S MEOW, 12000 SE 82nd Avenue, Happy Valley, OR'. Although the (fake) business name is different, the return address is the exact same address that was listed as the return address on the label affixed to the package that was sent to the undercover agent in June of 2025 that contained 420.35 grams of methamphetamine as a result of CNJTF's third undercover purchase of drugs from RMC. All of the seized drugs are drugs that are available for sale on RMC (with the exception of phenazolam; that said, a pill is advertised on the RMC domain that is identical in color, shape, and stamp to that of the seized phenazolam called 'bromazolam'). Based on my training and experience, phenazolam is not a federally controlled substance; MDMA is a federally controlled schedule I substance; cocaine and methamphetamine are federally controlled schedule II substances; and Ambien (generic name 'zolpidem') is a federally controlled schedule IV substance.

28. As a result of this specific information, along with USPS business records that appear to show a large volume of suspicious packages bearing 'third-party' postage labels, it appears that BLAKE and HEFFELFINGER handle a majority of the drug order 'processing' from their residence of the TARGET RESIDENCE, while Jesse WASSON and Shea WASSON handle other functions regarding RMC, such as customer service, money laundering, and general oversight, along with shipping 'pints' (promethazine and codeine) and 'breakdown weed' (ounce quantities of cannabis) from 5846 Flintwood Road, Unit B.

29. Further evidence of this is that Jesse WASSON appears to be in control of the ROCKY MOUNTAIN Potato encrypted messenger app account, which they likely operate with their electronic devices. For example, the Potato account has picture of an email exchange that showed that the person taking the picture was logged into the 'rockymtnpsych@protonmail.com' email address. Per the Kraken grand jury subpoena and Discord 2703(d) court order, investigators know that Jesse WASSON appears to be in control of the 'rockymtnpsych@protonmail.com' email address. Since the person taking the picture posted it to the official RMC Potato feed from the ROCKY MOUNTAIN Potato account, it is likely that the person in control of the 'rockymtnpsych@protonmail.com' email address also controls the Potato account (Jesse WASSON). Investigators know that ROCKY MOUNTAIN posts updates about drugs coming back in stock on the RMC website on the RMC official Potato feed. These messages appear to consistently coincide with suspicious packages showing up at the TARGET RESIDENCE. This means that Jesse WASSON has knowledge of bulk drug orders arriving at the TARGET RESIDENCE and likely controls the ordering and advertisement of such orders to the Potato feed.

SUMMARY OF PROBABLE CAUSE AND MOST RECENT EVENTS

30. On August 26, 2025, investigators with the San Joaquin Metropolitan Narcotics Task Force (METRO) (which is a law enforcement task force in the Sacramento, CA area) seized a package enroute to the TARGET RESIDENCE. METRO investigators applied for and were granted a federal search warrant to open the package on August 29, 2025. Investigators observed and subsequently seized 260 gross grams of suspected ketamine that was located within the package. The substance field-tested positive for the presence of ketamine. At time of

writing, a product called ‘Ketamine Isomer R -Sand’ is out of stock on the RMC drug marketplace. Based on my training and experience, I know that ketamine is a federally controlled schedule III substance.

31. Investigators have continued to observe BLAKE and HEFFELFINGER at the TARGET RESIDENCE. For example, on September 20, 2025, BLAKE was observed via electronic surveillance appearing from the TARGET RESIDENCE and loading what appeared to be tote bags into the Hyundai parked in the driveway of the TARGET RESIDENCE. Moments later, HEFFELFINGER arrived at the TARGET RESIDENCE in a blue Ford Bronco. After a few minutes, both departed the area of the TARGET RESIDENCE.

32. As a result of the surveillance, electronic surveillance, USPS business record analysis, undercover purchases of drugs, and digital evidence analysis, CNJTF investigators believe there is probable cause to search the TARGET RESIDENCE, mainly based on the following:

- a. The TARGET RESIDENCE is a location that HEFFELFINGER and BLAKE receive bulk amounts of drugs at so that they can be broken down into orders made from the RMC domain;
- b. HEFFELFINGER and BLAKE ‘process’ the orders at the TARGET RESIDENCE, meaning that they take bulk quantities of drugs, break them down into the desired quantity, and package them within the TARGET RESIDENCE;
- c. HEFFELFINGER and BLAKE then take those orders and distribute them at USPS facilities;

- d. HEFFELFINGER and BLAKE communicate with each other and the WASSONs, including about matters regarding RMC operations using electronic devices, and appear to be paid for their work in cryptocurrency. Such cryptocurrency is received by HEFFELFINGER and BLAKE and may be stored within electronic devices and/or physically in the form of ‘cold storage’ or ‘paper’ cryptocurrency wallets;
- e. Assets that that may have been purchased or gained via drug proceeds may be present at the TARGET RESIDENCE;
- f. Jesse and Shea WASSON live at 5846 Flintwood Road, Unit B. Jesse WASSON is engaged in a ‘leadership’ role in the RMC DTO, which involves directing other members of the RMC DTO (mainly HEFFELFINGER and BLAKE) to distribute RMC drug orders;
- g. Jesse WASSON is in control of several RMC encrypted messenger platforms and the ‘rockymtnpsych@protonmail.com’ email address, which are vital to advertising, customer service, and operational functions of RMC. Jesse WASSON is furthermore using electronic devices (such as computers, cellular devices, tablets, and/or other electronic devices) to conduct such business. Such electronic devices are in Jesse WASSON’s possession and/or are located at 5846 Flintwood Road, Unit B, such devices contain evidence of the RMC DTO and drug trafficking in general (cryptocurrency wallet information, RMC branding,

and guides on how to conduct drug trafficking business), and frequently use 5846 Flintwood Road, Unit B's internet service/connection;

- h. Jesse WASSON is likely in possession of a firearm that is located at 5846 Flintwood Road, Unit B, or on Jesse's person, and that other members of the RMC DTO (such as HEFFELFINGER and BLAKE) may follow suit and possess firearms as well;
- i. Assets that may have been purchased or gained via drug proceeds may be present at the TARGET RESIDENCE;
- j. Jesse and Shea WASSON are laundering RMC drug proceeds in the form of cryptocurrency (and/or other assets that were purchased or otherwise gained using such drug proceeds), along with storing cryptocurrency within electronic devices and/or physically in the form of 'cold storage' or 'paper' cryptocurrency wallets at 5846 Flintwood Road, Unit B; and
- k. 5846 Flintwood Road, Unit B, stores certain drugs, such as ounce quantities of cannabis, and promethazine and codeine for the purpose of distribution based on the facts of the investigation described above.

Electronic Records

33. As described above and in Attachment B, this application seeks permission to search for records that might be found on the TARGET RESIDENCE, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the

seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

34. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know: drug traffickers, especially those that operate/vend on social media sites, the clearweb, and/or darkweb use electronic devices to facilitate drug trafficking. Examples include keeping ledgers of drug sales, communicating with drug customers and sources-of-supply about order statuses/issues, and storing media (pictures, videos, audio, etc.) of drugs.

- a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used,

what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- d. Based on actual inspection of other evidence related to this investigation, financial records, electronic evidence search warrants, cryptocurrency tracing, etc., I am aware that digital devices were used to generate, store, and print documents used in the drug trafficking scheme. Thus, there is reason to believe that there is a digital device currently located on the TARGET RESIDENCE.

35. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the TARGET RESIDENCE, because, based on my knowledge, training, and experience, I know:

- a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual

memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital

device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

- c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a digital device to commit a crime such as advertising the sale of controlled substances and communicating with suspected controlled substance customers through communications facilities, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

36. In most cases, a thorough search of the TARGET RESIDENCE for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the TARGET RESIDENCE, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors

and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

- a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on TARGET RESIDENCE could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the TARGET RESIDENCE. However, taking

the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

37. The investigation has shown that BLAKE and HEFFELFINGER are the only two persons residing at the TARGET RESIDENCE, however, it is nonetheless possible that the TARGET RESIDENCE may contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrant applied for would permit the seizure and review of those items as well.

38. In my training and experience, it is likely that the TARGET RESIDENCE will contain at least one Apple brand device, such as an iPhone or iPad, and device running an Android operating system because investigators have applied for and were granted search warrants to search a Google Gmail account belonging to HEFFELFINGER and an Apple iCloud account belonging to BLAKE. Furthermore, per administrative subpoenas served onto T-Mobile for toll records and other basic information associated with telephone numbers known to be used by HEFFELFINGER and BLAKE, investigators believe that HEFFELFINGER possesses at least one Android device, and that BLAKE possesses at least one Apple device.

39. This warrant permits law enforcement agents to obtain from both HEFFELFINGER and BLAKE the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices requiring such biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on

the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.
- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

- f. As discussed in this Affidavit, investigators have reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the TARGET RESIDENCE; (2) hold the Device(s) found at the TARGET RESIDENCE in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the TARGET RESIDENCE in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant. The proposed warrant does not authorize (nor does it prohibit) law enforcement to request that the aforementioned person(s) state or otherwise provide the password or any other means that may be used to unlock or access the Device(s). Moreover, the proposed warrant does not authorize (nor does it prohibit) law enforcement to ask the aforementioned person(s) to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). That is, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic unlocks any Device(s), the

agents will not state or otherwise imply that the warrant requires such person to provide such information; that is, the agents will make clear that any such request is voluntary/the person is free to refuse the request.

Nature of Examination

40. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

41. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

42. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data

falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

43. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

44. If a computer or storage media contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain that computer or storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

45. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

46. The government has made the following prior efforts in other judicial fora to obtain evidence sought under the warrant: grand jury subpoenas, 18 U.S.C. § 2703(d) order, and other warrant requests.

47. Based on my training and experience, I know that individuals involved in drug trafficking on darkweb, clearweb, and/or social media sites often maintain records (including

financial records, receipts, notes, ledgers, mail, tax records, and other papers) related to their crimes, and that these records are often maintained at places where the individuals can have ready access to them, including their residence. In my training and experience, I also know that individuals who have committed crimes using computers, such as HEFFELFINGER and BLAKE, often keep records of their crimes in digital or electronic format, such as on a computer, and that computers are often stored in a residence.

48. It should be noted that because HEFFELFINGER and BLAKE's crimes involved the use of virtual currency and encryption, the items to be seized could be stored almost anywhere within a residence, in both physical and electronic formats. For example, Attachment B seeks virtual currency addresses, virtual currency private keys, virtual currency root keys, PGP keys, and passwords. These pieces of data comprise long and complex character strings, and in my training and experience I know that many virtual currency users write down or otherwise record and store such items because they are too long to commit to memory. As such, these keys, passwords, and addresses may be documented in writing and secreted anywhere within a residence. For all of the foregoing reasons, your affiant respectfully submits that probable cause exists to believe that such records, data, and documents will be found within HEFFELFINGER and BLAKE's residence, including in computers or on other devices that store electronic data.

Background on Bitcoin

49. Bitcoin¹ is a type of virtual currency, circulated over the Internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer

¹ Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

50. Bitcoin are sent to and received from Bitcoin “addresses.” A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to access the funds associated with a Bitcoin address. Only the holder of an address’ private key can authorize transfers of Bitcoin from that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at any given time and may use a unique Bitcoin address for each and every transaction.

51. To acquire Bitcoin, a typical user purchases them from a virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients’ identities.

52. To transfer Bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender’s private key, across the peer-to-peer Bitcoin network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender’s own private key. This information on its own rarely reflects

any identifying information about either the sender or the recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received Bitcoin and maintains records of every transaction for each Bitcoin address.

53. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can trace transactions to, among other recipients, Bitcoin exchangers. Because Bitcoin exchangers generally collect identifying information about their customers, as discussed above, subpoenas or other appropriate legal process submitted to exchangers can, in some instances, reveal the true identity of an individual responsible for a Bitcoin transaction.

54. As stated above, there are thousands of other cryptocurrencies available to the general public. ROCKY MOUNTAIN CONNECTIONS takes payment for drug orders in Bitcoin, Litecoin, and Monero. Broadly speaking, Litecoin is generally similar to Bitcoin in functionality and privacy. It also operates on a decentralized public ledger type infrastructure. Monero however, is considered a 'privacy' cryptocurrency coin. Monero is similar to Bitcoin in functionality, in that in order to send Monero, one needs their own private key to sign the transaction and another's public key (address) to send the Monero to. But transaction

data/information is private, in that Monero transactions are not kept on a public ledger the same way that Bitcoin and Litecoin are.

Conclusion

55. Based on the foregoing, I have probable cause to believe, and I do believe, that members of the RMC DTO, including HEFFELFINGER and BLAKE, have committed the Target Offenses, and that contraband/evidence/fruits/instrumentalities of that/those offense(s), as described above and in Attachment B, are presently located at the TARGET RESIDENCE, which is described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the TARGET RESIDENCE described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

56. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorneys (AUSA) Courter Shimeall and Joseph Huynh. I was informed that it is AUSA Shimeall's and AUSA Huynh's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Request for Sealing

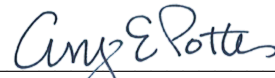
57. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may cause flight from prosecution, cause destruction of or tampering with evidence, or otherwise seriously jeopardize

an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

By phone pursuant to Fed. R. Crim. P. 4.1

William Jake VonEssen
Special Agent, DEA

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at
11:51 a.m. a.m./p.m. on October 1, 2025.



HONORABLE AMY E. POTTER
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is 24 Grove Street, Lebanon, OR 97355, which is described as a two-story residence that is off-white in color with blue trim.



ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the TARGET RESIDENCE located at **24 Grove Street, Lebanon, OR 97355**, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) Distribution of Controlled Substances, 21 U.S.C. § 846 Conspiracy to Possess with the Intent to Distribute Controlled Substances, 21 U.S.C. § 843(b) Illegal Use of a Communications Facility, and 21 U.S.C. § 843(c) Illegal Controlled Substance Advertisement, and Money Laundering Conspiracy 18 U.S.C. § 1956(h). The items to be seized cover the period of **January 1, 2024, through the date of the execution of the search warrant.**

1. The items referenced above to be searched for, seized, and examined are as follows:
 - a. Indicia of occupancy, residency, rental and/or ownership of the TARGET RESIDENCE described above or vehicles located thereon, including, but not limited to, utility and telephone bills, cancelled envelopes, keys, deeds, purchase lease agreements, land contracts, titles, and vehicle registrations.
 - b. Address and/or telephone books, rolodex indices, and any papers reflecting names, addresses, telephone numbers, pager numbers, and fax numbers of co-conspirators, sources of supply, storage facilities, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists.
 - c. Photographs of co-conspirators, assets, and/or drugs, including still photos, negatives, videotapes, films, slides, undeveloped film, memory cards, and the contents therein.
 - d. United States currency, precious metals, jewelry, gold coins, and financial instruments, including, but not limited to, stocks and bonds.
 - e. Books, records, invoices, receipts, records of real estate transactions, auto titles, federal, state, and city income tax returns financial statements, bank statements, cancelled checks, deposit checks, passbooks, money drafts, withdrawal slips, certificates of deposit, letters of credit, loan and mortgage

records, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys, money wrappers, wire transfer applications and/or receipts, fictitious identification, and other items evidencing the obtaining, secreting, transfer, concealment, and/or expenditure of money.

- f. Papers, tickets, notices, credit card receipts, travel schedules, travel receipts, passports and/or visas, and other items relating to travel to obtain and distribute drugs and drug proceeds. Evidence of such travel is often times maintained by drug traffickers in the form of airline receipts, bus tickets, automobile rental records, credit card receipts, travel schedules, diaries, day planners, hotel receipts, logs, travel agency vouchers, notes, cellular telephone tolls, and records of long-distance telephone calls.
- g. Log books, records, payment receipts, notes, customer lists, ledgers, shipping labels and other papers relating to the transportation, ordering, purchasing, processing, storage and distribution of controlled substances, including all records of income and expenses.
- h. Drugs and other controlled substances, along with equipment used to package, ship, manufacture, sell, and/or use controlled substances, such as scales, presses, chemicals, shipping receptacles, etc.
- i. Firearms, firearm accessories, magazines, ammunition, and other dangerous weapons.
- j. Any opened and/or unopened U.S. Mail parcels.
- k. Any and all funds (virtual currency), including cryptocurrency, to include the following:
 - i. any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;
 - ii. any and all representations of cryptocurrency private keys, whether in electronic or physical format;
 - iii. any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include "recovery seeds" or "root keys" which may be used to regenerate a wallet.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer (also referred to as 'device') or electronic

storage (such as flash memory or other media that can store data) and any photographic form.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter “Computer”):

- a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.
- b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
- c. Evidence of the lack of such malicious software.
- d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.
- e. Evidence indicating the Computer user’s state of mind as it relates to the crime under investigation.
- f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.
- h. Evidence of the times the Computer was used.
- i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.
- j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.
- k. Records of or information about Internet Protocol addresses used by the Computer.
- l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- m. Contextual information necessary to understand the evidence described in this attachment.
- n. Routers, modems, and network equipment used to connect computers to the Internet.

4. During the execution of the search of the TARGET RESIDENCE, law enforcement personnel are also specifically authorized to obtain from Amandra HEFFELFINGER and Jennifer BLAKE the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- a. any of the Device(s) found at the TARGET RESIDENCE,
- b. where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit

and warrant attachments A, for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

5. While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

6. The opening, search, and removal, if necessary, of any safe or locked receptacle or compartment, as some or all of the property heretofore may be maintained.

Search Procedure

7. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that

might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

8. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

9. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

10. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

11. If a computer or storage media contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain that computer or storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

12. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

13. The government is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the government. This is to include any and all cryptocurrency from all derivation paths associated with each wallet.

- a. The government is further authorized to copy any wallet files and reconstitute them onto computers controlled by the government. By reconstituting the wallets on its own computers, the government will continue to collect cryptocurrency transferred into the defendant's (Amandra HEFFELFINGER and Jennifer BLAKE) wallets as a result of transactions that were not yet completed at the time that the defendant's devices were seized.