AO93 Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of Blue IPhone with No Visible Serial Number	Case No. 22-5122MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before March 28, 2022 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: March 14, 2022 at 10:27 a.m.

Deborah M Fine
Judge's signature

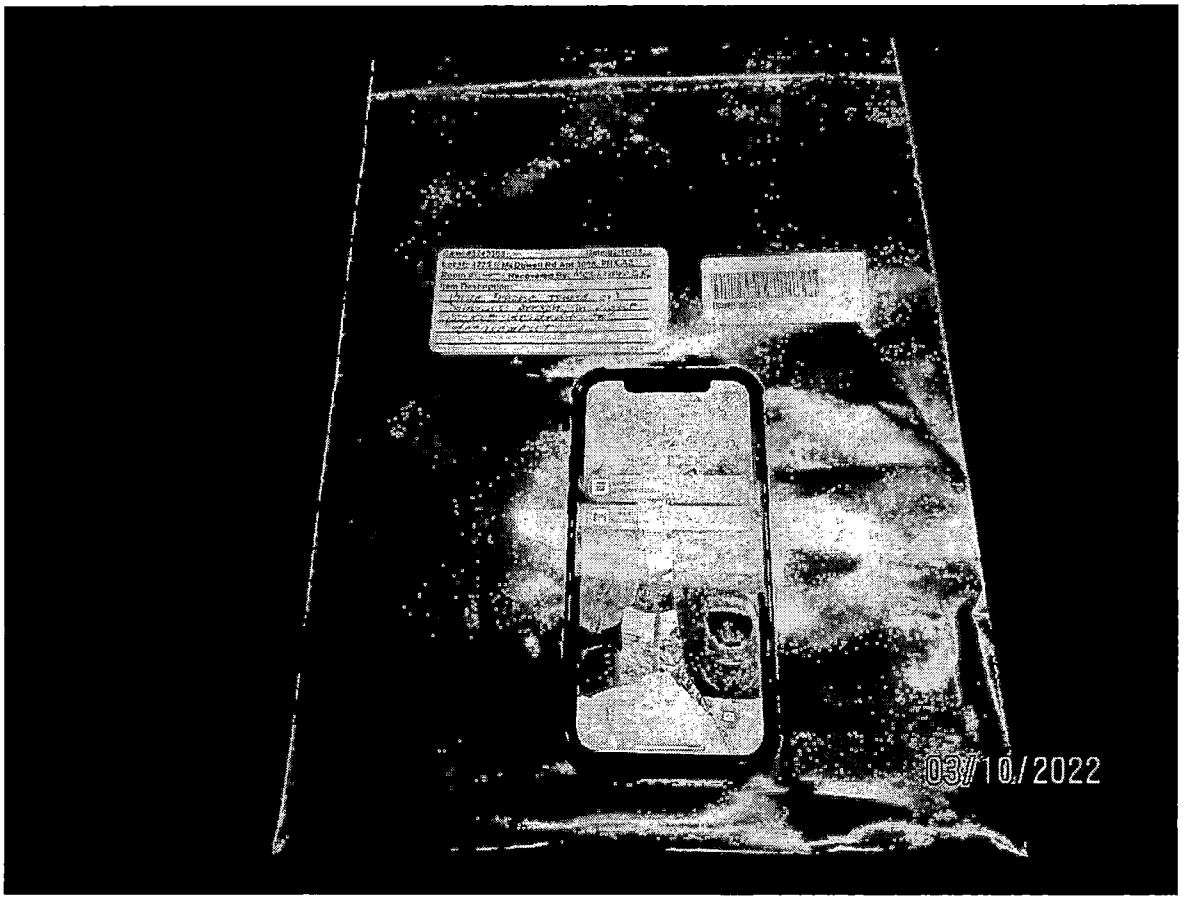
City and state: Phoenix, Arizona

HONORABLE DEBORAH M. FINE, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is a blue IPhone with no visible serial number (hereafter the "Subject Cellular Telephone"). The Subject Cellular Telephone is currently located at the U.S. Postal Inspection Service office in Phoenix, Arizona. This warrant authorizes the forensic examination of the Subject Cellular Telephone for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT B

Property to be seized

1. Any records and information found within the digital contents of the Subject Cellular Telephone that relate to violations of 18 U.S.C. § 1956(a)(1) (Money Laundering), 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute a Controlled Substance), 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), and 21 U.S.C. § 843(b) (Use of a Communication Facility to Commit a Federal Drug Felony):

   a. all information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of drugs;

   b. all information related to buyers or sources of drugs (including names, addresses, telephone numbers, locations, or any other identifying information);

   c. all records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, PayPal, Cash App or other electronic money transfer services, money order purchase receipts, account statements or any other transfer of money.

   d. all records and information related to United States currency, foreign currency, financial instruments, digital currency including Bitcoin, Etherum, Dash, or other digital coin, public and private keys, wallet addresses, jewelry, precious metals, stocks, bonds, money wrappers, or documents regarding purchase of real or personal property.

   e. all information regarding the receipt, transfer, possession, transportation, or use of drug proceeds;

   f. any information recording schedule or travel;

g. evidence indicating the cellular telephone user's state of mind as it relates to the crime under investigation;

h. contextual information necessary to understand the above evidence.

2. Any records and information found within the digital contents of the Subject Cellular Telephone showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" includes records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the cellular telephone.

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of:	Case No. 22-5122MB
Blue IPhone with No Visible Serial Number	

APPLICATION FOR A SEARCH WARRANT

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:

As further described in Attachment A

located in the District of Arizona, there is now concealed:

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is:

- ☒ 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:

Code/Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with Intent to Distribute Controlled Substances
21 U.S.C. § 846	Conspiracy to Possess with Intent to Distribute Controlled Substances
18 U.S.C. § 1956(a)(1)	Money Laundering
21 U.S.C. § 843(b)	Use of Communication Facility to Commit a Federal Drug Felony

The application is based on these facts:

See attached Affidavit of U.S. Postal Inspector Miranda Garcia

☒ 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.

Reviewed by AUSA Ryan McCarthy

RYAN MCCARTHY Digitally signed by RYAN MCCARTHY Date: 2022.03.11 17:17:06 -07'00'

Miranda Garcia Digitally signed by Miranda Garcia Date: 2022.03.11 17:08:14 -07'00'

Applicant's Signature

MIRANDA GARCIA, POSTAL INSPECTOR

Printed name and title

Sworn to before me and signed in my presence.

Date: March 14, 2022 at 10:27 a.m.

Deborah M Fine

Judge's signature

City and state: Phoenix, Arizona

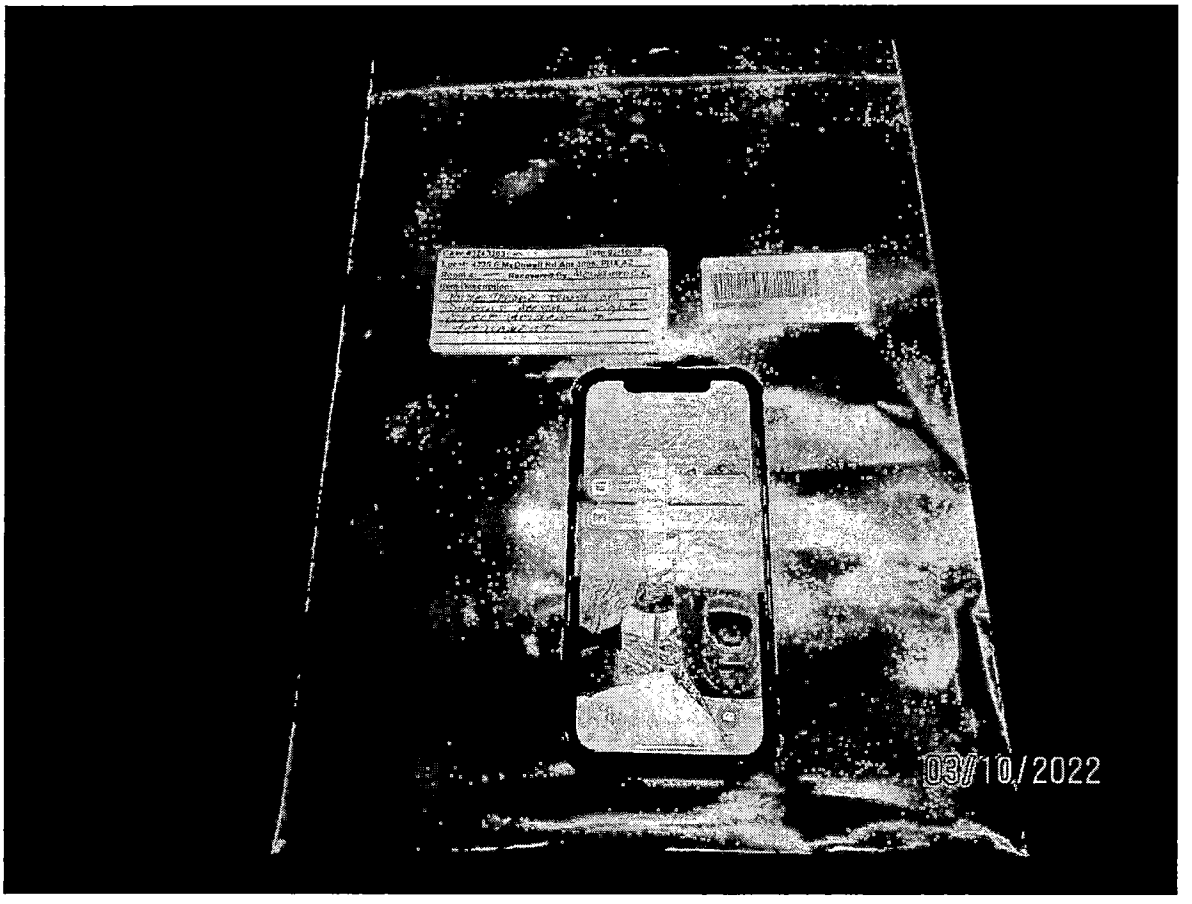
HONORABLE DOBORAH M. FINE, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is a blue IPhone with no visible serial number (hereafter the "Subject Cellular Telephone"). The Subject Cellular Telephone is currently located at the U.S. Postal Inspection Service office in Phoenix, Arizona. This warrant authorizes the forensic examination of the Subject Cellular Telephone for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT B

Property to be seized

1. Any records and information found within the digital contents of the Subject Cellular Telephone that relate to violations of 18 U.S.C. § 1956(a)(1) (Money Laundering), 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute a Controlled Substance), 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), and 21 U.S.C. § 843(b) (Use of a Communication Facility to Commit a Federal Drug Felony):

   a. all information related to the sale, purchase, receipt, shipping, importation, transportation, transfer, possession, or use of drugs;

   b. all information related to buyers or sources of drugs (including names, addresses, telephone numbers, locations, or any other identifying information);

   c. all records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, PayPal, Cash App or other electronic money transfer services, money order purchase receipts, account statements or any other transfer of money.

   d. all records and information related to United States currency, foreign currency, financial instruments, digital currency including Bitcoin, Etherum, Dash, or other digital coin, public and private keys, wallet addresses, jewelry, precious metals, stocks, bonds, money wrappers, or documents regarding purchase of real or personal property.

   e. all information regarding the receipt, transfer, possession, transportation, or use of drug proceeds;

   f. any information recording schedule or travel;

g. evidence indicating the cellular telephone user's state of mind as it relates to the crime under investigation;

h. contextual information necessary to understand the above evidence.

2. Any records and information found within the digital contents of the Subject Cellular Telephone showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" includes records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the cellular telephone.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your Affiant, Miranda Garcia, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant makes this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to examine the cellular telephone further described in Attachment A (hereafter "**Subject Cellular Telephone**"), and in order to extract the electronically stored information set forth in Attachment B, which represent evidence and/or instrumentalities of the criminal violations further described below.

2. I am a United States Postal Inspector and have been so employed since January 2006. I have completed a twelve-week basic training course in Potomac, Maryland, which included training in the investigation of narcotics trafficking via the United States Mail. I am currently assigned to the Phoenix Division Prohibited Mailings Narcotics Team (PMNT) in Arizona, which is responsible for investigating narcotic violations involving the United States Mails. Part of my training as a Postal Inspector included narcotic investigative techniques and the training in the identification and detection of controlled substances being transported in the U.S. Mail.

3. I have assisted on numerous narcotics investigations of individuals for violations of Title 21, United States Code, Sections 841(a)(1) (Possession with Intent to Distribute a Controlled Substance), 843(b) (Use of a Communication Facility to Facilitate the Distribution of a Controlled Substance), and 846 (Conspiracy to Possess with Intent to Distribute a Controlled Substance). The facts and information contained in this affidavit are based on my training and experience, or that of other Postal Inspectors and law enforcement officers involved in this investigation as described below.

4. In preparing this Affidavit, I conferred with other law enforcement officers, who share the opinions and conclusions stated herein. I have personal knowledge of the

following facts or have learned them from other law enforcement officers. I also relied on my training, experience, and background in law enforcement to evaluate this information.

5. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, your Affiant has not set forth all of the relevant facts known to law enforcement officers.

II. BASIS FOR PROBABLE CAUSE

6. Starting in November 2020, law enforcement agents began to investigate a dark web vendor believed to be selling illegal opioid pills through the darknet. Specifically, on November 20, 2020, an undercover agent ("UC") purchased 10 oxycodone pills from the darknet marketplace, "Dark Market," from a vendor identified as "PillPlugPaul." The UC instructed the vendor, PillPlugPaul, to send the pills to a PO Box in Virginia that the UC monitors/controls.

7. On November 30, 2020, law enforcement officers received a package containing 10 pills with the marking "M" on one side and "30" on the other side. The pills subsequently tested positive for fentanyl. Based upon my review of Postal Service databases, this package was sent from the Osborn Post Office on November 23, 2020.

8. At the time, I already aware of a suspicious mailing of packages from the Osborn Post Office on that date. Indeed, I was separately alerted that on November 23, 2020, a single individual had mailed seven (7) packages from the Osborn Post Office, all of which bore the indicia of drug trafficking. I was unaware at the time, but subsequently realized, that the package going to the UC PO Box in Virginia was among these seven packages.

9. I obtained a search warrant (SW20-5291) for one of these seven packages (the rest, including the package destined for the UC PO Box in Virginia, were returned to the mail stream). Upon executing SW20-5291, I discovered that the packaged contained

10 blue pills with "M" stamped on one side and "30" on the other. These pills subsequently tested positive for fentanyl.

10. Approximately three months later, on February 15, 2021, law enforcement officers in Virginia conducted a second UC purchase of oxycodone pills from PillPlugPaul. The UC purchaser again instructed the vendor to send the pills to another PO Box in Virginia that the UC monitors/controls.

11. On February 26, 2020, law enforcement officers in Virginia received a package (the "February Package") containing 10 pills with the marking "M" on one side and "30" on the other side. The pills subsequently tested positive for fentanyl. According to the package's tracking information, I learned the package was mailed from the Laveen Post Office. I obtained the surveillance camera footage from the Laveen Post Office from the date and time of when the February Package was mailed and compared that with the footage from the Osborn Post Office. Upon a review, it appeared two different individuals mailed each of the packages that were sent on behalf of PillPlugPaul to the UC purchaser in Virginia.

12. To identify the individual who mailed the February Package, I continued to review the surveillance camera footage from the exterior of the Laveen Post Office on the date and time of when the package was mailed. In doing so, I observed the individual who mailed the packages got into a black Ford SUV and then drove away from the Laveen Post Office. Though unknown at the time, I subsequently identified this individual as CUMMINGS.

13. Approximately two months later, on April 7, 2021, I was notified of another group of seven parcels that were mailed from the Phoenix Processing & Distribution Center (Phoenix P&DC) and which bore the indicia of drug trafficking. As a result, these packages were pulled from the mail stream for further inspection. I obtained a federal search warrant (SW21-107MB) to search one of these parcels and found it to contain several blue pills

stamped "M" on one side and "30" on the other, weighing approximately 3.2 grams. One of the pills was subsequently analyzed and found to contain fentanyl in a useable quantity.

14. To identify the sender of these packages, I discovered via video surveillance that the sender appeared to be the same individual who mailed the February Package, CUMMINGS. And through video surveillance from the outside of the Phoenix P&DC, I observed CUMMINGS' vehicle enter the parking lot just prior to when the mailing of the seven parcels occurred. The vehicle is described as a black Ford SUV, just like the individual who mailed the February Package.

15. This time, however, I was able to observe the license plate of the black Ford SUV, and observed it bore the license plate number CTV8880 and found CUMMINGS was the registered owner.

16. Upon reviewing CUMMINGS' Arizona Driver's License photograph, I observed he appeared to be the same individual who mailed the February Package and the April package. I also discovered that the return address for the parcel I seized in April, was an address CUMMINGS used to receive mail and was also where investigators have observed the black Ford Edge on multiple occasions.

17. To confirm CUMMINGS's pattern of conduct, a USPIS analyst was able to identify several other related mailings between October 2020 and the current date, which bore similar characteristics to the parcels CUMMINGS mailed in February and April. The analyst utilized various databases which analyze postal intelligence including, but not limited to, phone numbers, addresses, parcel weight, payment type, etc.

18. The analyst identified an additional twenty-one parcels, mailed on four different dates, in which CUMMINGS and/or the black Ford Edge were identified on surveillance video:

a. 12/16/2020, Maryvale Post Office, 9 parcels mailed, black Ford Edge captured on video leaving parking lot shortly after transaction ends;

b. 12/19/2020, Maryvale Post Office, 6 parcels mailed, black Ford Edge captured on video leaving parking lot shortly after transaction ends;

c. 1/22/2021, Maryvale Post Office, 4 parcels mailed, CUMMINGS captured on video mailing parcels and black Ford Edge captured on video leaving parking lot shortly after transaction ends;

d. 2/1/2021, Maryvale Post Office, 2 parcels mailed, CUMMINGS captured on video mailing parcels and black Ford Edge captured on video leaving parking lot shortly after transaction ends;

19. On May 14, 2021, The Honorable Michelle Burns approved a vehicle tracking device warrant for the black Ford Edge. On May 18, 2021, law enforcement installed a tracking device on the black Ford Edge. On June 9, 2021, law enforcement removed the tracking device because the black Ford Edge had been totaled in a vehicle crash just days prior. CUMMINGS was taken into custody on other charges by Phoenix Police Department and remained in custody until on or about August 31, 2021. When CUMMINGS was taken into custody, PillPlugPaul, was not available on the dark web markets.

20. In September 2021, Postal Inspectors were notified of several suspicious parcels were mailed from the Tempe Apache Post Office. After a physical examination of the parcels, I selected three parcels and obtained three separate federal search warrants. All three parcels contained blue M30 pills. A review of video surveillance revealed CUMMINGS appeared to be the mailer of the parcels. Postal clerks advised the mailer told them he was living across the street from the post office. At this time, law enforcement learned PillPlugPaul was back on the dark market.

21. Query of a law enforcement database revealed CUMMINGS had a new vehicle registered to him; a maroon Oldsmobile Alero ("target vehicle"). The address listed on the registration was at an apartment on Apache Blvd in Tempe.

22. In December 2021, law enforcement conducted an online UC buy from PillPlugPaul. Law enforcement attempted to conduct surveillance of this mailing but CUMMINGS was not at his residence on the morning of the mailing. A review of video surveillance from the post office revealed CUMMINGS had conducted the mailing.

23. Shortly after this UC buy, law enforcement learned CUMMINGS was no longer residing at the apartment on Apache Blvd in Tempe and temporarily had no leads on his whereabouts. However, between December 2021 and January 2022, mailings involving the target vehicle continued.

24. On January 3, 2022, the targe vehicle was captured on surveillance cameras entering the Phoenix P&DC. An unidentified male wearing a mask, a dark sweater, and his hair in a top knot, entered the post office and mailed several packages which contain characteristics similar to the packages being mailed by CUMMINGS. The unidentified male was later identified as ELISHA CHRISTOPHER DOBBINS (DOBBINS).

25. On January 14, 2022, CUMMINGS was seen on surveillance exiting the driver side of the target vehicle at the Phoenix P&DC. CUMMINGS was seen on surveillance cameras mailing several packages.

26. On January 18, 2022, the target vehicle was captured on surveillance cameras at the Phoenix P&DC. DOBBINS was observed mailing several packages. DOBBINS exited the post office and entered the passenger side of the target vehicle.

27. I seized one of the parcels mailed on January 18, 2022 and obtained a federal search warrant. The parcel had a return address of Herm Luis, at a residence off 6th Avenue in Phoenix. The parcel was found to contain blue M30 pills.

28. Law enforcement identified a new location where CUMMINGS and DOBBINS currently reside, an apartment within the Residences at FortyTwo 25 Apartments. ("target property").

29. On February 7, 2022, the Honorable Deborah Fine approved a vehicle tracking device warrant for the target vehicle. On February 8, 2022, law enforcement installed a tracking device on the target vehicle. The vehicle tracking device confirmed CUMMINGS's vehicle is consistently at target property overnight, confirming CUMMINGS is likely residing at target property.

30. On February 11, 2022, law enforcement conducted surveillance at the target property on target vehicle. At approximately 10:30 AM, I observed CUMMINGS and DOBBINS walk down the stairs together from the third floor of the Residences at FortyTwo25 Apartments (it was later confirmed this is the staircase nearest to target property). CUMMINGS was carrying a blue and white USPS envelope under his left armpit. CUMMINGS entered the driver's seat, and DOBBINS entered the passenger seat of target vehicle.

31. Law enforcement observed CUMMINGS exit the apartment complex in target vehicle and drive directly to Tempe Main Post Office. Law enforcement never lost sight of target vehicle during this surveillance.

32. Law enforcement immediately went through the backside of the post office to the employee area and watched the transaction take place from a closed-circuit television wherein the video from the retail counter line runs real time. Other law enforcement waited in the parking lot of the post office where DOBBINS was observed exiting the target vehicle with an envelope in hand. At approximately 10:50 am, law enforcement inside the post office watched DOBBINS proceed to mail the parcel. As soon as DOBBINS left the post office, law enforcement immediately seized the parcel. Law enforcement in the parking lot observed DOBBINS get back into the passenger side of the target vehicle empty handed. Law enforcement and the vehicle tracker confirmed CUMMINGS and DOBBINS travelled directly from the target property to the post office to mail suspected narcotics.

33. On this same date, I received a federal search warrant for this parcel. Similar to a previously seized parcel, this parcel also included a return sender as "Herm Louis." On February 14, 2022, law enforcement executed the search warrant and found the parcel to contain approximately 19.5 grams of blue M30 pills which are currently pending analysis at the lab.

34. Using various law enforcement databases, Postal Inspectors were able to identify the mailer of this parcel as DOBBINS. Inspectors obtained a booking photo of DOBBINS and he appears to have shipped packages on January 3rd, 18th, 31st and February 3rd, 7th, 11th, and 24th.

35. On or about February 23, 2022, Mesa Police Department installed a camera in the hallway of the public and common walkway of the apartment complex near target property. The camera has a view of the front door of target property. Law enforcement received verbal consent from the apartment complex manager to install the camera.

36. A review of the hallway camera footage for February 23rd, 2022, captured both DOBBINS and CUMMINGS at the target property. DOBBINS was captured on camera exiting target property. CUMMINGS was observed on camera responding to a delivery at target property. CUMMINGS answered the front door, retrieved an item and went back inside the target property.

37. Postal records reveal CUMMINGS and DOBBINS receive mail at the target property.

38. On March 9, 2022, a law enforcement officer contacted PillPlugPaul on "Wickr," an end-to-end encrypted messaging platform. The officer advised he wanted to make a purchase. PillPlugPaul advised he had product and sent over his price sheet. The agent ultimately did not pay for the order.

39. On March 10, 2022, law enforcement executed a residential search warrant at the target property. Both CUMMINGS and DOBBINS were present inside the residence

at the time. CUMMINGS and DOBBINS exited the target residence without incident and were taken into custody. Law enforcement located **Subject Cellular Telephone** in DOBBINS's possession when he was detained outside of the target residence.

40. In CUMMINGS bedroom, confirmed by indicia in the room, agents located several tiny Ziploc bags with "black clubs" on them as well as several unused postal mailing labels and envelopes. On the bed were two plastic baggies which appeared to have been ripped/cut open and emptied. Between CUMMINGS' bedroom and the adjoining bathroom, there was a trail of blue M30 pills on the floor leading to the toilet. Agents ultimately located five blue M30 pills of suspected fentanyl. It appeared as though CUMMINGS flushed pills down the toilet when law enforcement came to his front door. A laptop and several older cell phones were located in CUMMINGS' bedroom and closet.

41. CUMMINGS was interviewed and invoked his right to an attorney.

42. DOBBINS agreed to waive his Miranda rights. DOBBINS admitted he mails parcels for CUMMINGS. DOBBINS denied being the vendor or source of the pills and denied packaging the parcels. DOBBINS admitted the parcels come to him packaged and he mails them for a monetary amount. DOBBINS estimated he was paid $3,500 a month by CUMMINGS. DOBBINS admitted CUMMINGS sends him money via Cash App. DOBBINS admitted CUMMINGS sends him Bitcoin, which is then converted via Cash App. DOBBINS accesses his Cash App on **Subject Cellular Telephone**. DOBBINS admitted to sending money CUMMINGS sent to him, to his Chase Bank account, withdrawing the money, and giving it back to CUMMINGS.

43. The **Subject Cellular Telephone** is currently in the possession of the United States Postal Inspection Service based on the search warrant executed March 10, 2022. I seek this additional warrant to be certain that an examination of Subject Cellular Telephone will comply with the Fourth Amendment and other applicable laws due to the fact

DOBBINS has the cell phone on his person at the time law enforcement removed him from the residence during the execution of the search warrant.

44. The **Subject Cellular Telephone** is currently in storage at the U.S. Postal Inspection Service office in Phoenix, AZ. In my training and experience, I know that the **Subject Cellular Telephone** has been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the **Subject Cellular Telephone** first came into the possession of the United States Postal Inspection Service.

III. ITEMS TO BE SEIZED

45. Based upon the facts contained in this Affidavit, your Affiant submits there is probable cause to believe that the item listed in Attachment B will be found in the contents of the Subject Cellular Telephone.

46. Based on my training, education, and experience, and discussions with other trained law enforcement personnel, along with information provided by sources of information and confidential sources, your Affiant knows the following:

a. Drug traffickers often keep large amounts of United States currency on hand in order to maintain and finance their ongoing trafficking activities. Traffickers commonly maintain such currency where they have ready access to it, such as in their homes and vehicles. It is also common for traffickers to possess drug proceeds and items purchased with proceeds in their homes and vehicles. Thus, it is common for currency, expensive jewelry, precious metals, or financial instruments to be found in the possession of drug traffickers.

b. Traffickers and persons involved in the manufacturing, distribution, and possession of controlled substances often possess firearms and other weapons, both legal and illegal, in order to protect their person, drugs, or the proceeds of drug transactions. Traffickers commonly maintain such firearms and weapons where they have ready access

to them, such as on their person, in their homes, and in their vehicles. In addition, other firearm-related items, such as gun pieces, ammunition, gun cleaning items or kits, holsters, ammunition belts, original box packaging, targets, expended pieces of lead, photographs of firearms, and paperwork showing the purchase, storage, disposition, or dominion and control over firearms, ammunition, and related items are commonly possessed by drug traffickers along with their firearms.

c. Traffickers often maintain paraphernalia for manufacturing and distributing controlled substances, including packaging materials, scales, and cutting agents. Traffickers commonly maintain such paraphernalia at stash houses, in their homes, or in their vehicles.

d. Traffickers often maintain paper records of their drug trafficking and money laundering activities. Your Affiant knows that such records are commonly maintained for long periods of time and therefore are likely to be found in the Subject Cellular Telephone.

e. Drug traffickers commonly use cellular telephones to communicate with other drug traffickers and customers about drug-related activities through the use of telephone calls, text messages, email, chat rooms, social media, and other internet- and application-based communication forums. Moreover, drug traffickers commonly use other capabilities of cellular telephones to further their drug trafficking and money laundering activities. Therefore, evidence related to drug trafficking activity and money laundering activity is likely to be found on the Subject Cellular Telephone.

47. Based on my training and experience, and consulting with law enforcement partners familiar with dark web and cryptocurrency investigations, when buying and selling illicit substances through the internet, narcotics traffickers frequently use cryptocurrency (such as Bitcoin) due to the relative anonymity it affords. Narcotics traffickers using cryptocurrency commonly use dark web vendors to facilitate this process.

"Cryptocurrency" refers to a digital asset in which encryption techniques are used to generate, regulate, and transfer units of exchange independently of a central banking system. Cryptocurrency transactions are relatively anonymous (like cash transactions) and can be conducted over internet without a face-to-face meeting. Cryptocurrencies can also be used to purchase items from internet vendors, including dark web vendors, who wish to remain anonymous.

48. Rather than a traditional banking account which is used in the central banking system, cryptocurrencies use a "cryptocurrency wallet." A cryptocurrency wallet is a device, physical medium, program, or service which stores the public and private keys for cryptocurrency transactions. Public and private keys are required to transfer cryptocurrencies between wallets through a technology known as the blockchain. The cryptocurrency wallet's public key can be used to track ownership of the cryptocurrency, but the ownership of a cryptocurrency wallet is often more difficult to determine by law enforcement than the owner of a traditional baking account used in the central banking system.

49. In addition to items which may constitute evidence and/or instrumentalities of the crimes set forth in this Affidavit, your Affiant also requests permission to seize any articles tending to establish the identity of persons who have dominion and control over the Subject Cellular Telephone.

IV. DIGITAL EVIDENCE STORED WITHIN A CELLULAR TELEPHONE

50. As described in Attachment B, this application seeks permission to search for records and information that might be found in the contents of the Subject Cellular Telephone. Thus, the warrant applied for would authorize the copying of electronically stored information under Rule 41(e)(2)(B).

51. *Probable cause.* Your Affiant submits that there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on the Subject Cellular Telephone for at least the following reasons:

a. Your Affiant knows that when an individual uses a cellular telephone, the cellular telephone may serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The cellular telephone is an instrumentality of the crime because it is used as a means of committing the criminal offense. The cellular telephone is also likely to be a storage medium for evidence of crime. From my training and experience, your Affiant believes that a cellular telephone used to commit a crime of this type may contain: data that is evidence of how the cellular telephone 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.

b. Based on my knowledge, training, and experience, your Affiant knows that cellular telephones contain electronically stored data, including, but not limited to, records related to communications made to or from the cellular telephone, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic "address books;" photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system ("GPS") information.

c. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a cellular telephone, deleted, or viewed via the Internet. Electronic files downloaded to a cellular telephone 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. This is so because when a person "deletes" a file on a cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the cellular telephone until it is overwritten by new data.

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

52. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the cellular telephone was used, the purpose of the use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be found in the contents of the Subject Cellular Telephone because:

a. Data in a cellular telephone can provide evidence of a file that was once in the contents of the cellular telephone 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).

b. As explained herein, information stored within a cellular telephone may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware

detection programs) can indicate who has used or controlled the cellular telephone. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the cellular telephone was remotely accessed, thus inculpating or exculpating the owner. Further, activity on a cellular telephone can indicate how and when the cellular telephone was accessed or used. For example, as described herein, cellular telephones can contain information that log: session times and durations, activity associated with user accounts, electronic storage media that connected with the cellular telephone, and the IP addresses through which the cellular telephone accessed networks and the internet. Such information allows investigators to understand the chronological context of cellular telephone access, use, and events relating to the crime under investigation. Additionally, some information stored within a cellular telephone may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The geographic and timeline information described herein may either inculpate or exculpate the user of the cellular telephone. Last, information stored within a cellular telephone may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how the cellular telephone was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a cellular telephone 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, cellular telephone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one cellular telephone is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a cellular telephone 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 storage medium. 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.

53. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit imaging or otherwise copying the contents of the Subject Cellular Telephone, including the use of computer-assisted scans.

54. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

55. Your Affiant submits there is probable cause to believe that the items listed in Attachment B, which constitute evidence and/or instrumentalities of violations of 18 U.S.C. § 1956(a)(1) (Money Laundering), 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute a Controlled Substance), 21 U.S.C. § 841 (Possession with Intent to Distribute a Controlled Substance), and 21 U.S.C. § 843(b) (Use of a Communication Facility to Commit a Federal Drug Felony), are likely to be found in the contents of the **Subject Cellular Telephone** further described in Attachment A.

Miranda Garcia Digitally signed by Miranda Garcia Date: 2022.03.11 17:09:22 -07'00'

MIRANDA GARCIA, POSTAL INSPECTOR
UNITED STATES POSTAL INSPECTION SERVICE

Subscribed and sworn to before me this 14th day of March, 2022. at 10:27 a.m.

Deborah M Fine

HONORABLE DEBORAH M. FINE
United States Magistrate Judge