UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America
v.

CHALONER SAINTILLUS,
aka SHALAM ALI EL BEY

Defendant(s)

Case No. 2:20-mj-0162 JDP

SEALED

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 2019 through October 2020 in the county of Sacramento in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
Title 21 U.S.C. § 841(a)(1)	Distribution of a Controlled Substance;
Title 21 U.S.C. § 846	Conspiracy to Distribute a Controlled Substance

This criminal complaint is based on these facts:

(see attachment)

☒ Continued on the attached sheet.

/s/ Jason Bauwens
Complainant's signature
Jason Bauwens
United States Postal Inspecto
Printed name and title

Sworn to before me and signed telephonically.

Date: October 21, 2020

UNITED STATES MAGISTRATE JUDGE

City and state: Sacramento, California

Jeremy D. Peterson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT OF US POSTAL INSPECTOR JASON BAUWENS

I, Jason Bauwens, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS"). I am currently assigned to the Sacramento, California office. My responsibilities include investigating criminal violations of federal and state law, including illegal narcotics and narcotics proceeds being sent through the U.S. Mail; money laundering; robbery and burglary of postal employees and facilities; destruction of government property; theft/possession of stolen U.S. Mail; mail and bank fraud; and identity theft crimes. I am a "Federal law enforcement officer" within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is, a federal law enforcement agent engaged in enforcing criminal laws and authorized to request a search warrant.

2. I have been employed as a federal law enforcement agent for over 15 years, during which I have graduated from several federal training academies. In 1998, I graduated from the National Park Service Law Enforcement Academy in Sylva, North Carolina, which was a 10-week police academy. In 2003, I graduated from the National Park Ranger Integrated Police Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, which was a 16-week police academy. Most recently, I graduated from the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, which was a 12-week training program. Throughout my career, I have investigated over 1,000 cases involving criminal violations of federal, state, and tribal laws. I have instructed hundreds of hours of training related to the detection, identification, and investigation of narcotics trafficking. I have testified in various federal and state court proceedings. I have participated in multiple Title III wire intercepts regarding narcotics trafficking investigations and have worked with numerous confidential sources.

3. During my training, experience, and interaction with other experienced Postal

Inspectors, Task Force Officers, and other drug-trafficking investigators, I have become familiar with the methods employed by drug traffickers to smuggle, safeguard, store, transport, and distribute drugs; to collect and conceal drug-related proceeds; and to communicate with other participants to accomplish such objectives. I have received specialized training and instruction in narcotics investigation matters including, drug interdiction, drug detection, money laundering techniques and schemes, and drug identification. I have participated in and led numerous investigations targeting individuals and organizations trafficking marijuana, methamphetamine, heroin, cocaine, LSD, steroids, and many other controlled substances, along with narcotics proceeds. I have investigated many drug traffickers and money launderers who utilize the dark web, encrypted message applications, cryptocurrencies and various other concealing platforms in furtherance of their criminal enterprise. During the course of these investigations, I have become familiar with the manner in which drug traffickers conduct their illegal operations. I have written numerous search, seizure and arrest warrants related to drug trafficking investigations, drug proceeds investigations, and drug parcel interdiction.

II. PURPOSE

4. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show that there is sufficient probable cause for the requested arrest warrant and does not set forth all of my knowledge about this matter. Rather, I make this affidavit in support of a criminal complaint naming:

CHALONER SAINTILLUS, (AKA: "SHALAM ALI EL BEY"),

For violations of:

a. Title 21 U.S.C. § 841(a)(1) (Distribution of a Controlled Substance);
b. Title 21 U.S.C. § 846 (Conspiracy to Distribute a Controlled Substance).

III. TECHNICAL BACKGROUND

Based on my training and experience, I am aware of the following concepts:

5. The "dark web," also sometimes called the "darknet," or "dark net" is a colloquial name for a number of extensive, sophisticated, and widely used criminal marketplaces operating on the Internet, which allow participants to buy and sell illegal items, such as drugs, firearms, and other hazardous materials with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply "web"). These online black-market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. A famous dark web marketplace, Silk Road, operated similar to legitimate commercial websites such as Amazon and eBay, but offered illicit goods and services. Law enforcement shut down Silk Road in 2013. Currently operating, popular dark web marketplaces are White House, DarkMarket and Deep Sea.

6. Cellular "smart phones" can connect to the internet, including the dark web, and can be utilized to manage a drug vendor account as well as conduct digital currency transactions.

7. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts." Customers, meanwhile, operate "customer accounts." It is possible for the same person to operate one or more customer accounts and one or more vendor accounts at the same time.

8. "The Onion Router," "Tor network," or simply "Tor," is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in

".onion" and can only be accessed through specific web browser software, including a major dark web browser known as the "Tor Browser," designed to access the Tor network. One of the logos, or "icons," for the Tor Browser is a simple image of the Earth with purple water and bright green landmasses with bright green concentric circles wrapping around the planet to look like an onion.

9. Some software used to access the dark web does not permanently store images of the websites and or other data that are visited on the computer that is running the software.

10. Digital currency (also known as crypto-currency or virtual currency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States and may be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

11. "Bitcoin" (or "BTC[2]") is a type of online digital currency that allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. Bitcoins are a decentralized, peer-to-peer form of electronic currency having no association with banks or governments. Users store their bitcoins in digital "wallets," which are identified by unique electronic "addresses." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access Bitcoins on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number while the private key is like the password to access that account. Even though the public addresses of

[1] For purposes of this affidavit, "digital currency," "crypto-currency," and "virtual currency" address the same concept.

[2] As of October 19, 2020, one Bitcoin is equal to approximately $11,381.00 USD.

those engaging in Bitcoin transactions are recorded on the public ledger, the "Blockchain," the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

12. Although they are legal and have known legitimate uses, Bitcoins are also known to be used by cybercriminals for money-laundering purposes and are believed to be the most oft-used means of payment for illegal goods and services on "dark web" websites operating on the Tor network. By maintaining multiple bitcoin wallets, those who use Bitcoins for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplace.

13. Bitcoin is one example of a digital currency; other digital currencies, such as Ethereum, Monero, Litecoin and Zcash, also exist and are used by darknet actors. The technology underlying these currencies are similar, though Monero and Zcash currencies provide more privacy and anonymity to the users.

14. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones

or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, KeepKey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[3] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer. The Trezor device offers an advanced passphrase option that incorporates a "25th seed word" that must be enabled to access potentially obscured digital currency assets.

15. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law

[3] A QR code is a matrix barcode that is a machine-readable optical label.

enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

16. Darknet marketplaces often only accept payment through digital currencies, such as Bitcoin, and operate an escrow whereby customers provide the digital currency to the marketplace, who in turn provides it to the vendor after a transaction is completed. Accordingly, large amounts of Bitcoin sales or purchases by an individual can be an indicator that the individual is involved in drug trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who have received Bitcoins as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoins to convert them to fiat (government-backed) currency. Such purchases and sales are often facilitated by peer-to-peer bitcoin exchangers who are not registered with the federal or a state government and who advertise their services on websites designed to facilitate such transactions. These unregistered exchangers often charge a higher transaction fee than legitimate, registered digital currency exchangers. This higher fee is essentially a premium that the unregistered exchangers charge in return for not filing reports on the exchanges pursuant to the Bank Secrecy Act, such as CTRs and SARs.

17. When vendors receive orders for narcotics on the darknet, the orders can come from anywhere in the world; vendors are known to use U.S. mail and/or commercial carriers to distribute narcotics.

IV. SUMMARY OF THE INVESTIGATION

18. I am investigator on the Northern California Illicit Digital Economy ("NCIDE") Task Force composed of agents from the Federal Bureau of Investigation ("FBI"), the Drug Enforcement Administration ("DEA"), Homeland Security Investigations ("HSI"), Internal

Revenue Service Criminal Investigation Division ("IRS") and the USPIS. The Sacramento-based NCIDE Task Force investigates violations of U.S. law concerning cryptocurrencies and dark web marketplaces. As a function of this task force, investigators regularly conduct undercover purchases of narcotics from dark web marketplace vendors, to assist in identifying the suspects operating the dark web vendor accounts. Additionally, investigators routinely profile parcels within the US Mail stream, looking for links to dark web narcotics vendors. The investigation described below is one such investigation.

19. During this investigation, Federal Law Enforcement Officers have: (1) personally observed CHALONER SAINTILLUS place a parcel containing fentanyl into the United States Postal Service ("USPS") mail system; (2) have conducted undercover purchases of over 40 grams of fentanyl from online accounts operated by CHALONER SAINTILLUS; and (3) have obtained surveillance images of CHALONER SAINTILLUS mailing additional undercover purchases of heroin, oxycodone and oxymorphone into the USPS mail system. In doing so, CHALONER SAINTILLUS is:

a. Distributing controlled substances.
    i. Under 21 U.S.C. § 841(a)(1), "it shall be unlawful for any person knowingly or intentionally to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance."

b. Conspiring to distribute controlled substances.
    i. Under 21 U.S.C. § 846, "any person who attempts or conspires to commit any offense defined in this subchapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy."

V. FACTS ESTABLISHING PROBABLE CAUSE

A. Case Beginning

20. In April 2020, case agents identified a darknet vendor operating on the Empire marketplace under the moniker "chlnsaint" (hereinafter "VENDOR 1"), who advertised for sale various quantities of fentanyl, carfentanyl, heroin, cocaine, oxycodone, oxymorphone, subutex, adderall, alprazolam and marijuana. VENDOR 1 joined the marketplace in August 2019, and between then and approximately August 2020 when the marketplace was last accessible, had completed over 1,100 sales. As of August 2020, VENDOR 1 had a marketplace feedback rating of approximately 98%. VENDOR 1 advertised they offered both USPS Priority and Express mail shipping options and accepted both Bitcoin (BTC) and Litecoin (LTC) as forms of payment. In addition to being able to contact VENDOR 1 on the marketplace, they also advertised they could be contacted via, Wickr Me, the encrypted messaging application, under the moniker "showstill" (hereinafter "WICKR 1").

21. During the initial investigation of VENDOR 1, case agents conducted a review of various USPS databases, law enforcement databases and open source internet resources, and located numerous commonalities belonging to CHALONER SAINTILLUS (hereinafter "SAINTILLUS"), a thirty-two year old, African American male, residing in Delray Beach, Florida. Law enforcement observed portions of the letters that make up SAINTILLUS' true name, are utilized in the VENDOR 1 moniker. Additionally, the prefix of the gmail account utilized by SAINTILLUS (*chlnsaint*@gmail.com), is an exact match to the darknet moniker.

B. Undercover purchase #1

22. During the week of April 12, 2020, law enforcement conducted its first undercover purchase of five oxymorphone pills, an opiate currently listed as a Schedule II controlled substance, from VENDOR 1 on the Empire marketplace. The purchase was conducted utilizing bitcoin as the method of payment. On April 16, 2020, the parcel related to the

undercover purchase was mailed from a Self Service Kiosk (SSK) located in the post office at 14280 S Military Trail, Delray Beach, FL, 33484. The sender name and address on the parcel was handwritten as "Stephanie Smith 301 SW 7th Ave Delray Beach, FL 33444". The parcel was received at the undercover address provided by law enforcement, which was located in the Eastern District of California, and contained the five oxymorphone pills as purchased. The pills were later lab tested and determined to be oxymorphone.

23. On April 20, 2020, law enforcement conducted a review of the USPS surveillance image(s) taken at the time the undercover parcel was mailed and based on a prior review of numerous booking photos and a Florida Department of Motor Vehicles image, positively identified the person conducting the transaction as SAINTILLUS.

24. On or about April 23, 2020, law enforcement received records provided by T-Mobile USA, regarding a phone number linked to SAINTILLUS, 561-774-4760. Based on the provided information, as of January 04, 2020, the customer name and subscriber name of the cell phone is listed as "SHALAM ALI" with a service address of "222 SW 3RD AVE DELRAY BEACH FL 33444-3652", which is the listed legal address of SAINTILLUS. Law enforcement observed when looking up prior arrest records associated with SAINTILLUS, the name "SHALAM ALI EL BEY" was an alias he utilized. As of October 2020, there has been no change to the customer name or address of the T-Mobile cell phone, 561-774-4760.

25. During the early stages of the investigation, law enforcement conducted multiple detailed reviews of USPS records and databases and located three customer created accounts associated with SAINTILLUS. In USPS Account 1 and 2, the exact VENDOR 1 moniker was utilized in the prefix of the contact email of SAINTILLUS' two accounts. Additionally, on USPS Account 3, case agents observed that the prefix of the email associated with SAINTILLUS' account was "*shalamalielbey*", a known alias associated with SAINTILLUS. See below for the details of the SAINTILLUS USPS customer registration accounts:

///

///

USPS Account 1
Username: Chlnsaint
Name: Chaloner Saintillus
Address: 222 SW 3rd Ave, Delray Beach, FL 33444
Phone: 561-853-4220 and 561-774-4760
Email: chlnsaint@gmail.com

USPS Account 2
Username: Chlnsaint@gmail.com
Name: Chaloner Saintillus - S and S Corporation
Address: 222 SW 3rd Ave, Delray Beach, FL 33444
Phone: 954-605-4135
Email: chlnsaint@gmail.com

USPS Account 3
Username: shalamalielbey@gmail.com
Name: Chaloner Saintillus
Address: 222 SW 3rd Ave, Delray Beach, FL 33444
Phone: 561-774-4760
Email: shalamalielbey@gmail.com

26. In addition to the review of USPS records, case agents also conducted numerous "open internet" searches related to SAINTILLUS. As a result, case agents observed on two separate websites, https://kzchat.info and https://kztorrent.info, forum posts from a user with the name, chaloner saintillus, and the email of chlnsaint@gmail.com. Additionally, during another open internet search, case agents observed a dating profile on the website, ConnectingSingles.com, under the username "Chlnsaint", the same moniker utilized by VENDOR 1 on the Empire marketplace. The dating profile contained a photo of an African American male, with similar features and appearance of that of SAINTILLUS, and claimed to be a 32 year old male located in Delray Beach, Florida. The individual in the dating profile introduced themselves stating, "…I'm shalam what's ur name…".

///

///

///

///

C. Undercover purchases #2 thru #10

27. Between April 21, 2020, and September 1, 2020, law enforcement conducted nine (9) additional undercover purchases of narcotics from VENDOR 1, both from the Empire marketplace moniker, as well as via "direct deal" from the WICKR 1 moniker. The undercover purchases were for various quantities of heroin, fentanyl, oxycodone pills and oxymorphone pills. All of the undercover purchases of narcotics were conducted utilizing bitcoin and all of the parcels were received at undercover addresses located in the Eastern District of California, containing the narcotics as ordered. The parcels were all received in USPS envelopes, all had handwritten labels appearing to be written by the same person and all were shipped from post offices located in the Southern District of Florida. Law enforcement conducted later reviews of USPS surveillance image(s) taken at the time each of the nine additional undercover buy parcels were mailed. As a result, law enforcement observed SAINTILLUS was the person that shipped seven of the nine drug parcels, which were later determined through lab or field tests, to contain heroin, fentanyl or oxycodone. Agents determined no surveillance images existed at the time two of the mailings were conducted. See below for the undercover buy details:

UC Buy #	Drug Purchased	Quantity	Date Received	Surveillance Image	Test Result
2	heroin	1 gram	April 24, 2020	SAINTILLUS	fent and heroin
3	heroin	.4 gram	April 24, 2020	SAINTILLUS	fent and heroin
4	fentanyl	1 gram	April 29, 2020	No Image Avail.	fentanyl
5	fentanyl	7 grams	May 22, 2020	SAINTILLUS	no results
6	fentanyl	7 grams	June 2, 2020	SAINTILLUS	no results
7	oxycodone	5 pills	June 17, 2020	SAINTILLUS	oxycodone
8	fentanyl	14 grams	July 8, 2020	No Image Avail	no results
9	fentanyl	14 grams	July 8, 2020	SAINTILLUS	no results
10	oxymorphone	4 pills	Aug 24, 2020	SAINTILLUS	no results

D. SAINTILLUS Debit Card used to pay for Undercover Buy Parcels

28. Your affiant conducted a check of USPS records to determine the method of payment utilized to pay for the postage on the undercover buy parcels received by law enforcement. As a result, your affiant observed on the undercover buy parcels #1 through #4, a Wells Fargo debit card ending in 9058 was used as the method of payment at the USPS SSK. Law enforcement requested the Wells Fargo bank records associated with the debit card ending 9058. In June 2020, law enforcement received and reviewed the requested Wells Fargo bank records. As a result of the review, your affiant observed the customer registered to the Wells Fargo bank account was SAINTILLUS. During the review of the account records, your affiant also observed besides buying the postage on the first four undercover purchases, SAINTILLUS also made a large number of additional and regular purchases of postage from the USPS Post Office SSK's located at 14208 S. Military Delray Beach, Florida.

E. Surveillance and Seizure of Parcel containing Fentanyl

29. On October 8, 2020, law enforcement initiated surveillance in the vicinity of 245 NW 10th Ave Delray Beach, Florida, the last known location of SAINTILLUS. While conducting surveillance, law enforcement observed SAINTILLUS exit the front door of the residence carrying a USPS Priority Mail envelope. With the envelope in hand, SAINTILLUS entered the passenger seat of a white 2013 BMW four-door with attached State of Florida license plate PELY47. This vehicle was driven by an unknown driver. Florida Department of Highway Safety and Motor Vehicle records indicated SAINTILLUS to be the registered owner of the vehicle.

30. Law enforcement followed SAINTILLUS' vehicle to the United States Post Office located at 14208 S. Military Delray Beach, Florida, where law enforcement witnessed SAINTILLUS exit the vehicle and utilize the SSK for postage and then mail the parcel. After SAINTILLUS departed the post office, law enforcement took custody of the parcel**.** The parcel

bore the exact same sender name and address of previously seized parcels on this investigation, "Stephanie Smith 301 SW 7th Ave Delray Beach, FL 33444". Law enforcement later obtained a federal search warrant in the Southern District of Florida for the parcel, which was mailed by SAINTILLUS. As a result, the parcel was determined to contain approximately 7 grams of a white substance, which field tested positive for fentanyl.

VI. REQUEST FOR SEALING

31. I request that the Court seal the warrant and the affidavit and application in support thereof, except that copies of the warrant in full or redacted form may be maintained by the United States Attorney's Office and may be served on Special Agents and other investigative and law enforcement officers of USPIS, HSI, DEA, FBI and IRS, and federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, as necessary to effectuate the warrant. These documents pertain to and discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation.

32. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the ongoing, covert investigation. Sealing these documents will also better ensure the safety of agents and others.

[CONTINUED ON NEXT PAGE]

VII. CONCLUSION

33. Based on the facts set forth in this Affidavit, I believe there is probable cause that CHALONER SAINTILLUS committed violations of 21 U.S.C. § 841(a)(1) (Distribution of a Controlled Substance), and 21 U.S.C. § 846 (Conspiracy to Distribute a Controlled Substance), thus supporting the legal basis for the Court to issue an arrest warrant based on a criminal complaint.

Respectfully submitted,

/s/ Jason Bauwens
Jason Bauwens
United States Postal Inspector

Approved as to form:

Grant B. Rabenn
Grant Rabenn
Assistant United States Attorney

Sworn and Subscribed to me telephonically on October 21, 2020

Jeremy Peterson
UNITED STATES MAGISTRATE JUDGE