AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
OCT - 2 2018
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

United States of America

v.

CHRISTOPHER LAZENBY,

Defendant(s)

Case No.

18MJ02633

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 September 5, 2018, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. § 843(a)(3)	Obtaining a controlled substance by misrepresentation, fraud, forgery, deception, or subterfuge

LODGED

2018 OCT -2 PM 2:

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/

Complainant's signature

Erwin M. Benedicto, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/2/18

STEVE KIM

Judge's signature

City and state: Los Angeles, California

Hon. Steve Kim, U.S. Magistrate Judge

Printed name and title

SEAL OF THE U.S. DISTRICT COURT CENTRAL DIST. OF CALIFORNIA

BB

AFFIDAVIT

I, Erwin M. Benedicto, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") of the U.S. Drug Enforcement Administration ("DEA"), currently assigned to the DEA Diversion Group 1 at the Los Angeles Field Division Office. Until May 25, 2018, I was assigned to the DEA Enforcement Group 1 at the Honolulu District office in Honolulu, HI, and have employed by the DEA since July 15, 2012. Prior to my employment with DEA, I was employed as an attorney in private practice in Los Angeles, California. I have received specialized training from DEA in federal drug law enforcement. I have been involved in numerous drug-related arrests, numerous search warrants, and surveillances. I have debriefed numerous narcotics traffickers following their arrest. I have participated in drug trafficking investigations in which court-authorized wire interception was utilized. During this time, I have become knowledgeable with the enforcement of state and federal laws pertaining to narcotics and dangerous drugs. Based on this experience, I have become well versed in the methodology utilized in narcotics trafficking operations, the specific types of language used by narcotic traffickers, the unique trafficking patterns employed by narcotics organizations and their patterns of drug abuse.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against Christopher LAZENBY ("LAZENBY") for a

violation of 21 U.S.C. § 843(a)(3) (obtaining a controlled substance by misrepresentation, fraud, forgery, deception, or subterfuge). Specifically, on or about September 5, 2018, at a pharmacy located in Los Angeles County, within the Central District of California, LAZENBY filled a fraudulent and counterfeit prescription for controlled substances, which was purportedly issued by a doctor who was in fact an identity theft victim, and which was issued in the name of a false alias (initials B.S.) used by LAZENBY.

3. This affidavit is also made in support of an application for warrants to search the following premises (collectively, the "SUBJECT PREMISES") for evidence of violations of 21 U.S.C. §§ 841(a)(1) and 846 (distribution of a controlled substance, possession of a controlled substance with intent to distribute, and related attempt and conspiracy), 21 U.S.C. § 843(a)(3) (obtaining a controlled substance by misrepresentation, fraud, forgery, deception, or subterfuge), 18 U.S.C. §§ 1341, 1347, and 1349 (mail fraud, health care fraud, and related conspiracy), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1028(a) (unlawful possession, trafficking, production, and use of false identification documents and document-making implements):

a. The premises known as Room 2522, at the Residence Inn by Marriot, located at 3701 Torrance Blvd., Torrance, California ("the SUBJECT HOTEL ROOM").

b. A 2007 silver BMW, model 650i coupe bearing California license plate 6BSN182 ("the SUBJECT VEHICLE").

4. The SUBJECT HOTEL ROOM and the SUBJECT VEHICLE are further described in Attachments A(1) and A(2), which are incorporated as though fully set forth herein. The items to be seized are set forth in Attachment B, which is incorporated as though fully set forth herein.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and do not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. STATEMENT OF PROBABLE CAUSE

6. I am part of a team of agents investigating Christopher LAZENBY for fraudulently submitting online requests to change physicians' DEA registration information to reflect that their (the physicians') places of practice were addresses that were, in fact, mailboxes or a motel room controlled by LAZENBY, as part of what investigators believe is a scheme by LAZENBY and unknown conspirators to fraudulently acquire controlled drugs via counterfeit prescriptions issued under the names of the identity theft victim doctors.[1] Investigators are

[1] A DEA registration number is the number that authorizes physicians, pharmacists, or other practitioners to lawfully prescribe, dispense, or otherwise distribute controlled drugs, or to order controlled drugs.

presently aware of at least eight doctors or physician's assistants whose DEA registration information was recently changed online to reflect that the respective doctor's place of practice is either mailbox #224 at the UPS Store located at 2202 S. Figueroa St., Los Angeles, California, or mailbox #836 at the UPS Store located at 335 E. Albertoni St., Carson, California. Investigators are also aware of a ninth doctor whose DEA registration information was recently changed online to reflect a practice location address at what investigators have determined is in fact room 323 at the Motel 6 at 5101 West Century Blvd., Inglewood, California. Those identity theft victims are referred to collectively as "the identity theft victim doctors," and, where relevant, individually by initials E.S., J.D., J.S., J.K., K.H., and M.R. During the investigation, we learned that LAZENBY is also personally filling counterfeit prescriptions for controlled drugs, both for himself in the false alias B.S., and for third parties, which were purportedly written by the identity theft victim doctors and bear such doctors' forged signatures.

7. LAZENBY's criminal rap sheet reflects that, in November 2015, LAZENBY sustained felony convictions for possession of a controlled substance for sale, in violation of California Health and Safety Code Section 11378, and Transportation/Sale of a Controlled Substance, in violation of California Health and Safety Code Section 11379(a), for which LAZENBY received a sentence that includes three years' formal probation. Investigators have spoken with LAZENBY's probation

officer, who verified that LAZENBY remains under probation and that the terms of LAZENBY's probation include a standard warrantless search condition. (Accordingly, the instant search warrants may not be required under the Fourth Amendment.)

8. On August 14, 2018, DEA Diversion Investigator ("DI") Evangelina Alvarez spoke with the owner of UPS Store 4672 located at 2202 S Figueroa St., Los Angeles, California. The store owner stated that mailbox #224 at the location was rented to the name of a person with initials J.N. The owner also stated that he (the owner) has refused packages for J.N. because the packages were marked as being in the care of ("C/O") other individuals.

a. I have reviewed records for the rental of mailbox #224 obtained from the UPS Store, including United States Postal Service Form 1583 ("Application for Delivery of Mail Through Agent"), which show:

i. When applying to rent mailbox #224, the individual posing as J.N. provided as identification a Connecticut driver's license number xxxxx9400 and a Department of the Navy identification card both in the name of J.N., and both bearing a photograph of the same male individual. I have compared copies of those identification cards to California Department of Motor Vehicle ("DMV") records for LAZENBY, and observed that he is the person shown in the photographs of "J.N." on the cards.

ii. The telephone number provided on the Form 1583 for mailbox #224 is (424) xxx-2288. I have reviewed

records obtained from AT&T/Cingular Wireless for that phone number, which identify LAZENBY as the phone's subscriber, financially liable party, and billing party.

iii. The Form 1583 also identifies J.N.'s address as 645 W 9th St., Los Angeles, California. As discussed below, investigators have interdicted multiple parcels shipped to a UPS store mailbox at that address, from a mail order pharmacy, containing controlled drugs that, I submit, were fraudulently acquired by LAZENBY using counterfeit prescriptions in the names of the identity theft victim doctors.

iv. I have reviewed an e-mail provided by the owner of UPS Store 4672 that was sent from the renter of mailbox #224. In the email, "J.N." stated that he had two or three packages on the way for relatives that were addressed C/O him and that he did not want the packages refused by the store like the earlier ones just mentioned. The e-mail stated that he ("J.N.") had mailboxes at two other UPS Stores and "neither of them has a problem with me receiving packages addressed to C/O [J.N.], so I didn't know about your rule." The e-mail further explained that one of the packages was for his grandfather's heart medication and the other was kidney medication for his roommate's cat, and that they desperately need both.

b. I have learned that, on July 18, 2018, another person (initials S.S.) was arrested by Los Angeles Police Department ("LAPD") officers, who then conducted a parole or probation search of his residence. During the search, the officers found controlled drugs (illicit and prescription), as

well as prescription pads in the names of third party doctors. The officers also seized a Connecticut driver's license #xxxxx9400 in the name of initials J.N. (I have observed a copy of the seized driver's license and recognize that the photo of J.N. is LAZENBY.) S.S. told the officers that his roommate, LAZENBY, had moved out of the premises five or six days earlier.

9. On August 16, 2018, I spoke with the owner of UPS Store 5824 located at 335 E Albertoni St. #200, Carson, California. He told me that on July 25, 2018, mailbox #836 at the location was rented in the name of a person with initials J.N. When applying to rent mailbox #836, "J.N." provided as identification the same Connecticut driver's license and Navy identification card that was used to rent mailbox #224 at UPS Store 4672, as discussed above.

a. I reviewed the records for the rental of mailbox #836, including the United States Postal Service Form 1583 ("Application for Delivery of Mail Through Agent"). That form has a signature purporting to be by J.N. The address listed for J.N. on the form 1583 is 645 W 9th St., Los Angeles, California, and the form identifies J.N.'s telephone numbers as (424)xxx-2287 and (424)xxx-2288. (As noted above, this was also "J.N."'s address on the Form 1583 on renting mailbox #224, and the 2288 phone number is subscribed to LAZENBY and was also provided on renting mailbox #224.) Also listed on the form as an "undersigned" is a person with initials B.S.; a discussed below, this is the same name in the SUBJECT HOTEL ROOM is rented.

b. Here again, I have compared the copies of the identification cards used to rent mailbox #836 to California DMV records for LAZENBY, and I recognized that the LAZENBY is the person shown in the photographs for the cards.

10. On August 15, 2018, I spoke with an employee at the Motel 6 located at 5101 West Century Blvd., Inglewood, California, who told me an individual identifying himself as J.N. checked into the motel using what she believed was a counterfeit Connecticut driver's license. The employee, who told me that she is familiar with Connecticut driver's licenses, informed J.N. that his driver's license appeared to be counterfeit. I reviewed records provided by the employee showing that "J.N." checked into the motel on July 16, 2018 and stayed two nights. The employee provided copies of what I recognize to be the same identification documents described above, i.e., the Connecticut driver's license and the Navy identification card each in the name of "J.N." and bearing LAZENBY's image. The employee further told me that J.N. also answered to the name B.S.

11. On August 21, 2018, I and DEA contractor Patrick Leonard went to UPS Store 4977 located at 645 W. 9th St., Los Angeles, California, to determine whether LAZENBY maintained a mailbox at that location. Staff at the UPS Store confirmed that LAZENBY maintained mailbox #243 at that location. Moreover, I reviewed the documents related to that mailbox (e.g., "Application for Delivery of Mail Through Agent" and "Mail Service Agreement"), which show "Christopher Lazenby" (LAZENBY)

as the customer and mail recipient for mailbox #243. I viewed a copy of the California identification card associated with the mailbox, which I recognized also depicts LAZENBY.

a. Staff at the UPS Store informed me that the facility had three parcels for delivery to mailbox #243. These parcels were: (i) one UPS Next Day Air Saver Envelope bearing tracking number 1Z 2EF 878 13 2555 9089, "[J.C.], 866-216-5449, 645 W. 9th St. # 110-243, C/O Chris Lazenby, Los Angeles, CA 90015-1640"; (ii) one USPS Signature Tracking Envelope bearing tracking number 9302 1201 8490 0306 7570 63, addressed to "[L.H.D.], 645 W. 9th St. # 110-243, C/O C Lazenby, Los Angeles, CA 90015-1640"; and (iii) one FedEx Standard Overnight Envelope bearing tracking number 4488 5506 6589, addressed to "[J.C.], 645 W. 9th St. # 110-243, C/O Chris Lazenby, Los Angeles, CA 90015-1640".

b. Staff at the UPS Store showed me the three parcels. There was an approximately two inch rip in the side of the FedEx parcel, through which I was able to observe that the FedEx parcel contains three pharmacy pill bottles; labeling on one bottle showed that it contained hydrocodone (a Schedule II narcotic commonly known by the brand names Vicodin and Norco), labeling on a second bottle showed that it contained Adderall (a Schedule II amphetamine), and I was not able to read the label on the third bottle.

c. I was able to observe the name of the prescribing doctor shown on the pharmacy labels for the two bottles noted above. It is the name of one of the doctors whose DEA

registration information regarding practice location was recently changed as described above.

d. The address for the shipper for each of the three parcels was "4750 E. 450 South, Whitestone IN 46075". On August 21, 2018, DI Alvarez conducted an internet search of that address and observed that it is associated with a retail pharmacy, Express Scripts Pharmacy, Inc., which is registered with DEA # FE4301468.

e. Based on my observations and the other facts herein, I took custody of the three parcels in anticipation of seeking a search warrant.

12. On August 22, 2018, the Hon. Michael R. Wilner, United States Magistrate Judge, issued a search warrant for the above parcels (Case No. 18-MJ-02192). DI Desiree P. Wang and I then searched the three parcels.

a. The FedEx parcel contained: (i) one bottle of hydrocodone/acetaminophen Tab 10/325 (brand names Vicodin or Norco), 28 tablets; (ii) one bottle Vyvanse Caps 70 mg (generic name lisdexamfetamine dimesylate), 180 tablets; and (iii) one bottle amphetamine mix 30 mg (brand name Adderall), 180 tablets. These are all Schedule II controlled substances.

b. The UPS parcel contained: (i) one bottle alprazolam 1 mg (brand name Xanax), 270 tablets. Alprazolam is a Schedule IV controlled substance.

c. The USPS parcel contained: (i) one bottle hydromorphone HCL 8 mg (brand name Dilaudid), 42 Tablets; and

(ii) one bottle amphetamine mix 20 mg (Adderall), 180 tablets. These are all Schedule II controlled substances.

d. Each of the parcels also contained an invoice from Express Scripts Pharmacy, Inc. Two of the invoices identifies the prescriber as J.K., while the other identifies the prescriber as K.H. As noted above, both J.K. and K.H. are among the doctors whose identities are believed to have been stolen by LAZENBY. DI Alvarez later spoke with J.K., during which he verified that he never saw the patients named on the seized drugs, nor did they issue prescriptions for the seized drugs. (Investigators have not yet interviewed K.H.) The labeling on the seized bottles and the pharmacy invoices showed that each of the drugs were purportedly prescribed to one of the "patients" named on the envelopes, that is, L.H.D. or J.C.

13. On August 28, 2018, I and DI Alvarez returned to UPS Store 4977 at 645 W. 9th Street to determine whether any other parcels had arrived for LAZENBY. Staff at the UPS Store informed me that the facility had one parcel for delivery to mailbox #243.

a. Staff at the UPS Store showed me the parcel; it was a cardboard box, bearing a UPS Next Day Air Saver label with tracking number 1Z 2EF 878 13 2585 5740. The parcel was also addressed to "[L.H.D.]...C/O C LAZENBY". The USPS parcel that I interdicted on August 21, as discussed above, was also addressed to "[L.H.D.]" C/O LAZENBY, which contained amphetamine tablets and hydromorphone tables, both Schedule II controlled substances, prescribed by one of the doctors whose DEA

registration information is believed to have been fraudulently changed.

b. The address for the shipper for parcel was "4750 E. 450 South, Whitestone IN 46075", which is the address for Express Scripts Pharmacy, Inc. Each of the three parcels seized on August 21 was also addressed from the same location, as discussed above.

c. Based on my observations and the other facts herein, I took custody of the parcel in anticipation of seeking a search warrant.

14. On August 29, 2018, the Hon. Steve Kim, United States Magistrate Judge, issued a search warrant for the above parcel (Case No. 18-MJ-02287). DI Alvarez and I then searched the parcel.

a. The parcel contained one bottle of promethazine with codeine syrup (generic name Phenergan syrup with codeine), approximately 16 fluid ounces. Promethazine is a Schedule V controlled substance.

b. The parcel also contained an invoice from Express Scripts Pharmacy, Inc. The invoice identifies the prescriber as K.H., who as discussed above is believed to be one of the identity theft victim doctors, and who purportedly prescribed some of the drugs within the parcels I seized on August 21, 2018. Moreover, as described above, L.H.D. was one of the patients to whom drugs on August 21 were purportedly prescribed.

15. On September 5, 2018, I and DI Alvarez returned to the UPS Store (Store #4977) at 645 W. 9th Street to determine whether any other parcels had arrived for LAZENBY.

a. Staff at the UPS Store informed me that the facility had three parcels for delivery to mailbox #243. These parcels were: (i) one cardboard box, approximately 7.5" by 6" by 4.5", bearing a UPS Surepost label, with tracking number: 1Z 408 933 YW 2575 4504, addressed to "[L.H.D.], 645 W. 9th St. #110-243, C/O C Lazenby, Los Angeles, CA 90015-1640"; (ii) one standard size letter envelope, approximately 4" by 8.5", containing possible correspondence, mailed from "Norcal Mutual, 1700 Bent Creek Boulevard, Mechanicsburg, PA 17050", addressed to "[K.H.], M.D., 618 N. 3rd St., Apt. 6, San Jose, CA 95112-5128"; and (iii) one standard size letter envelope, approximately 4" by 8.5", containing possible correspondence, mailed from "2200 E. Devon Ave, Ste. 200, Des Plains, IL 60018-4501", addressed to "[K.H.], 618 N. 3rd St., Apt. 6, San Jose, CA 95112-5128."

b. The UPS Surepost parcel was addressed to "[L.H.D.]...C/O C LAZENBY". The USPS parcel that I interdicted on August 21 and the UPS parcel that I interdicted on August 28, as discussed above, were also addressed to "[L.H.D.]" C/O LAZENBY.

c. The address for the shipper for UPS Surepost parcel was "4750 E. 450 South, Whitestone IN 46075", which as noted is the address for Express Scripts Pharmacy, Inc. Each of the three parcels seized on August 21, and the address of the

parcel seized on August 28, was also addressed from the same location, as discussed above.

d. On September 5, 2018, I performed an internet search for "Norcal Mutual, 1700 Bent Creek Boulevard, Mechanicsburg, PA 17050", which is the address of the mailer of one of the parcels. Norcal Mutual is a provider of medical professional liability insurance. The letter from Norcal Mutual also has a yellow sticker which states "Notify Sender of New Address, [K.H.], MD, 110-243, 645 W. 9th St., Ste 110, Los Angeles, CA 90015-1662". This address, as described above, is for LAZENBY's private mailbox.

e. On September 5, 2018, I also performed an internet search for "2200 E. Devon Ave., Ste. 200, Des Plains, IL 60018-4501". It is the address listed for Asset Recovery Solutions, LLC, which provides debt relief and asset recovery services. Like the Norcal Mutual envelope described in the preceding paragraph, the Devon Ave. letter has a yellow sticker which states "[K.H.], MD, 110-243, 645 W. 9th St., Ste. 110, Los Angeles, CA 90015-1662".

f. Based on my observations and the other facts herein, I took custody of the parcels in anticipation of seeking a search warrant.

16. On September 6, 2018, the Hon. Paul L. Abrams, United States Magistrate Judge, issued a search warrant for the above parcels (Case No. 18-MJ-02387). DI Alvarez and I then searched the parcel.

a. The UPS Surepost parcel contained one bottle of promethazine with codeine syrup (generic name Phenergan syrup with codeine), approximately 16 fluid ounces. Promethazine is a Schedule V controlled substance.

b. The UPS Surepost parcel also contained an invoice from Express Scripts Pharmacy, Inc. The invoice identifies the prescriber as K.H., one of the identity theft victim doctors who purportedly prescribed drugs seized on August 21 and 28, 2018, as described above. Moreover, as before, the seized drugs were purportedly prescribed to L.H.D., who was also one of the purported patients for the drugs seized on those dates.

c. The letter from Norcal Mutual contained a billing statement addressed to K.H.

d. The letter from 2200 E. Devon Ave. contained a billing statement from Asset Recovery Solutions, LLC, addressed to K.H.[2]

17. On September 21, 2018, I and DI Alvarez spoke to the Pharmacist-in-Charge ("PIC") of the Saint Antony Pharmacy, located at 310 E. Grand Ave., Unit 105, El Segundo, California. The PIC showed me a total of eight prescriptions in the names of patients with the initials B.S., K.S., L.S., S.R. and J.H., which as described below were filled by or under the supervision of LAZENBY using the false alias B.S.

---

[2] Regarding mail matter in fact intended to be delivered to K.H., investigators intend to notify K.H. and provide a copy of the seized mail matter to K.H., while preserving the seized mail matter for evidence.

a. I know from the investigation that LAZENBY uses the false alias B.S. For example, as discussed below herein, the SUBJECT HOTEL ROOM is rented by LAZENBY in the name B.S., and the name B.S. was also listed in LAZENBY's application to rent mailbox #836 at the UPS Store located at 335 E. Ablertoni St. Moreover, the employee I interviewed at Motel 6 remembered that the person who was using the name with the initials J.N. (LAZENBY) also answered to B.S.

b. I showed the PIC a picture of LAZENBY. The PIC positively identified LAZENBY as B.S. The PIC described the circumstances regarding how the eight prescriptions were filled as follows.

c. According to the PIC, on or about August 28, 2018, B.S. (i.e., LAZENBY) came to the pharmacy with a patient with initials S.R. to fill two prescriptions.

i. One of the prescriptions was for S.R., and was purportedly issued by M.R. at the "City of Angeles Primary Care Clinic." (As noted above, M.R. is one of the identity theft victim doctors, that is, one of the doctors whose DEA registration information regarding practice location was recently changed to an address controlled by LAZENBY; investigators have not yet interviewed M.R.) The phone number associated with S.R. for the prescription is (424) xxx-2288. I have reviewed records obtained from AT&T/Cingular Wireless for that phone number, which identify LAZENBY as the phone's subscriber, financially liable party, and billing party. Through this prescription, S.R. obtained 30 pills of 30-mg

dextroamphetamine, 30 pills of 70-mg Vyvanse, and 60 tablets of 30-mg amphetamine salts (brand name Adderall). These are all Schedule II controlled substances.

ii. The second prescription was for a person with initials L.S., who the PIC understood to be B.S.'s (LAZENBY's) son. This prescription was purportedly issued by J.K from the "Helping Hands Community Health Center." As discussed above, J.K. is also one of the identity theft victim doctors, and J.K. was one of the purported prescribers for drugs seized from the above interdicted parcels. When DI Alvarez interviewed J.K., he also verified that he did not authorize or issue this prescription, nor was L.S. one of his patients. The phone number associated with L.S. for the prescription is (310) xxx-0787. I have reviewed records obtained from AT&T/Cingular Wireless for that phone number, which identify LAZENBY as the phone's subscriber, financially liable party, and billing party. Through this prescription B.S. obtained 90 tablets of 30-mg amphetamine salts (brand name Adderall), which as noted is a Schedule II controlled substance.

d. According to the PIC, on or about September 4, 2018, B.S. (LAZENBY) again came to the pharmacy to fill three new prescriptions in the name of a purported patient with initials J.H. The PIC understood B.S. (LAZENBY) to be J.H.'s "caregiver;" from my training and experience, I know that drug traffickers will often acquire black market drug stock by filling fraudulent prescriptions in the names third parties, for whom the traffickers claim to be "caregivers." One of the

prescriptions listed B.S. as J.H.'s "emergency contact" and noted that B.S. is in possession of J.H.'s insurance card. The prescriptions were purportedly issued by, respectively, J.D., J.K., or E.S., at the "Helping Hands Community Healthcare Center." (J.D., J.K., and E.S. are among the identity theft victim doctors referenced above; E.S. is a physician's assistant.) Moreover, the phone number associated with each prescription is (424) xxx-2288, which as noted above is subscribed to LAZENBY. Through these prescriptions B.S. obtained 180 pills of 15-mg Oxycodone HCL, 30 pills of 10-mg Fluoxetine HCL, 60 pills of 37.5-mg Phentermine, 90 pills of 10-mg Diazepam, 60 pills of 30-mg Amphetamine Salts, and 60 pills of 30-mg Adderall XR. Oxycodone, amphetamine salts, and Adderall are Schedule II controlled substances; diazepam and phentermine are Schedule IV controlled substances; and fluoxetine is a non-controlled prescription drug.

e. According to the PIC, on or about September 5, 2018, B.S. (LAZENBY) came to the pharmacy to fill three additional prescriptions. One prescription was issued to B.S., the second to K.S. (whom the PIC understood to be B.S.'s wife), and the third prescription to J.H. The prescriptions were purportedly written by J.D. or E.S. at the "Helping Hands Community Healthcare Center."

i. The phone number associated with the prescription for B.S. is (310) xxx-0787, which as described above is subscribed to LAZENBY. Through this prescription B.S. obtained 90 pills of 10-mg Diazepam, 30 pills of 10-mg Zolpidem

Tartrate (brand name Ambien), and 90 pills of 30-mg amphetamine salts (brand name Adderall). Diazepam and Ambien are Schedule IV controlled substances, and Adderall is a Schedule II controlled substance.

ii. The phone number associated with the prescription for K.S. is (424) xxx-2288, which as described above is subscribed to LAZENBY. Through this prescription B.S. obtained 90 pills of 30-mg amphetamine salts (brand name Adderall), a Schedule II controlled substance.

f. The phone number associated with the prescription for J.H. is (424) xxx-2288, which as described above is subscribed to LAZENBY. Through the prescriptions for J.H., B.S. obtained 180 pills of 15-mg Oxycodone HCL, which as noted is a Schedule II controlled substance.

g. The PIC and the PIC's staff showed me pharmacy surveillance footage of B.S. picking up some of the prescriptions described above. I recognized that the person shown has the same height, build, and features as LAZENBY.

18. On October 1, 2018, DI Alvarez spoke to an employee of Express Scripts Pharmacy, Inc. That employee identified addresses to which LAZENBY had recently received parcels, one of which was a Residence Inn by Marriot located in Torrance, California.

19. On October 1, 2018, I and DI Alvarez spoke to the manager and a member of the staff at the Residence Inn by Marriot, located at 3701 Torrance Blvd., Torrance, California. I asked whether an individual by the name of B.S. was currently

renting a room at the location. The manager showed me an electronic record that showed B.S. was currently staying in Room 2522 (i.e., "the SUBJECT HOTEL ROOM"). I showed the manager a picture of LAZENBY. The manager positively identified LAZENBY as the person using the name B.S. who is staying in Room 2522 (the SUBJECT HOTEL ROOM). I showed the same picture of LAZENBY to the staff member who positively identified LAZENBY, stating that the person in the photograph looks like B.S. The manager informed us that B.S. has recently been receiving shipments of parcels to the hotel, and that B.S. has been dropping of parcels with the hotel front desk for outbound shipment. The manager retrieved logs of parcels that B.S. has received, noted that they show a large number of inbound parcels; the manager also stated that the parcels that B.S. had received included parcels contained printers and laptops. (Based on the facts herein, I believe that this is equipment used by LAZENBY to manufacture counterfeit identification cards and/or prescriptions.)

20. I and DI Alvarez then went to the parking lot in front of Room 2522 (the SUBJECT HOTEL ROOM). Approximately 10 minutes later, we observed LAZENBY walk out of the SUBJECT HOTEL ROOM, down a stairway into the hotel parking lot, and then get into the front driver seat of the SUBJECT VEHICLE (a silver color BMW model 650i coupe, bearing California license plate 6BSN182), and drive away alone. We ran the SUBJECT VEHICLE's California DMV records, which showed that it is registered to a third party (initials C.D.) and had been recently sold in approximately May 2018. Given the facts herein that LAZENBY has used multiple

false aliases to reserve hotel rooms and post office mailboxes, I believe that he likewise used a false alias to acquire the SUBJECT VEHICLE. In any event, given the facts herein, including evidence that LAZENBY is traveling to pharmacies to fill fraudulent prescriptions, I submit that probable cause exists to search the vehicle being used by LAZENBY for evidence of the offenses under investigation, even if it is not registered to him.

21. From my training and experience, I know that prescription drug traffickers often steal the identities of doctors to, for example, create counterfeit prescription pads in their names, which the traffickers then use to fill the prescriptions in the names of third parties (e.g., in patient names that are in fact false identities, identity theft victims, or conspirators receiving cash kickbacks in exchange for filling the prescriptions or allowing their names to be used). Accordingly, based on the facts herein and on my training and experience, I believe that LAZENBY is employing fraud and identity theft to acquire controlled drugs for further black market sale. Moreover, from the records that I have reviewed in this investigation, I have observed that some of the drugs fraudulently acquired by LAZENBY discussed above were paid for via cash, whereas others are paid for via insurance. As to the latter, I submit that LAZENBY has engaged in insurance fraud, that is, that he has caused insurers to pay for the filling of fraudulent prescriptions.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

22. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical

manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35′ x 35′ x 10′ rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[3] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular

---

[3] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive 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 digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and

the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt"

to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

h. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. Moreover, I believe that LAZENBY possesses cellular telephones that include one or more Apple iPhones: records that I have obtained for the cellular service provider (AT&T) for (424) xxx-2288, which as noted above is subscribed to LAZENBY, identifies two separate Apple iCloud e-mail addresses as LAZENBY's email contact information for the account, including

from records that investigators received from AT&T as recently as September 6, 2018.

i. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

j. 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 Inc. ("Apple") offers a feature on some of its phones and laptops 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 on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later),

iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

k. 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. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature

"Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

l. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

m. 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 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.

23. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the SUBJECT PREMISES and reasonably believed by law enforcement to be a user of the device to unlock the device using biometric features in the same manner as discussed in the following paragraph.

24. 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 have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. 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. I do not know the passcodes of the devices likely to be found during the search.

25. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located at the SUBJECT

PREMISES during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the SUBJECT PREMISES and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

V. CONCLUSION

26. For all the reasons described above, there is probable cause to believe that LAZENBY has committed a violation of 21 U.S.C. § 843(a)(3) (obtaining a controlled substance by misrepresentation, fraud, forgery, deception, or subterfuge), including or about September 5, 2018.

27. Also for all the reasons described above, there is probable cause to believe that evidence of violations of 21 U.S.C. §§ 841(a)(1) and 846 (distribution of a controlled substance, possession of a controlled substance with intent to distribute, and related attempt and conspiracy), 21 U.S.C. § 843(a)(3) (obtaining a controlled substance by

misrepresentation, fraud, forgery, deception, or subterfuge), 18 U.S.C. §§ 1341, 1347, and 1349 (mail fraud, health care fraud, and related conspiracy), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1028(a) (unlawful possession, trafficking, production, and use of false identification documents and document-making implements), as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachments A(1) and A(2) of this affidavit.

/s/

Erwin M. Benedicto
Special Agent
Drug Enforcement
Administration

Subscribed to and sworn before me
this 2 day of October, 2018.

STEVE KIM

UNITED STATES MAGISTRATE JUDGE