Case 2:19-sw-01155-DB Document 1 Filed 12/19/19 Page 1 of 57

FILED
DEC 19 2019
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY DEPUTY CLERK

United States District Court

EASTERN District of CALIFORNIA

In the Matter of the Seizure of

(Address or brief description of property or premises to be seized)

All funds maintained at Bank of America Account XXXX-XXXX-4003 held in the name of Lisa Chen Sole Prop DBA Chen Corner,

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

CASE NUMBER:

2:19 SW 1155 DB

I, Jason Chin, Special Agent, DEA, being duly sworn depose and say:

I am a(n) Special Agent, DEA and have reason to believe that

in the **EASTERN** District of **CALIFORNIA** there is now certain property which is subject to forfeiture to the United States, namely (describe the property to be seized)

All funds maintained at Bank of America Account XXXX-XXXX-4003 held in the name of Lisa Chen Sole Prop DBA Chen Corner,

Which is subject to seizure pursuant to 21 U.S.C. § 881(b) incorporating 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 21 U.S.C § 881(a)(6) based on violations of 21 U.S.C. § 841(a)(1) and 21 U.S.C. § 846.

The facts to support a finding of probable cause for issuance of a seizure warrant are as follows:

See attached affidavit.

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Signature of Affiant

Sworn to before me and subscribed in my presence,

12-17-19
Date

at Sacramento, California
City State

Deborah Barnes, U.S. Magistrate Judge
Name of Judicial Officer Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND SEARCH WARRANT

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

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Drug Enforcement Administration ("DEA") and have been so employed since May 2005. I am currently assigned to the DEA Sacramento District Office and am charged with investigating drug trafficking and money laundering activities in the Eastern District of California, and elsewhere. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and I am empowered by law to conduct investigations and make arrests for federal felony offenses. Additionally, 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 was trained as a DEA Special Agent at the DEA Academy, Quantico, Virginia. During my training, I received special training in the Controlled Substance Act, Title 21 United States Code, including but not limited to, Sections 841(a)(1) and 846, Controlled Substance Violations and Conspiracy to Commit Controlled Substance Violations, respectively. I have received special training regarding criminal organizations engaged in conspiracies to manufacture and/or possess with intent to distribute methamphetamine, cocaine, cocaine base, heroin, marijuana, MDMA, and other dangerous drugs prohibited by law. I received further training in search and seizure law, financial investigations and money laundering techniques, and many other facets of drug law enforcement. I have also spoken to and worked with experienced federal, state, and municipal agents and narcotics officers regarding the methods and means employed by drug manufacturers and drug traffickers including the use of express carriers and the U.S. Postal system to distribute drugs.

3. During the course of my employment as a DEA Special Agent, I have participated in numerous criminal investigations. I have participated in executing numerous Federal and State

search warrants involving the aforementioned listed controlled substances, the seizure of narcotics-related records and other types of evidence that document the activities of criminal organizations in both the manufacturing and distribution of controlled substances. To successfully conduct these investigations, I have utilized a variety of investigative techniques and resources, including physical and electronic surveillance, various types of infiltration, including undercover agents, informants, and cooperating sources. Through these investigations, my training and experience, and conversations with other agents and law enforcement personnel, I am familiar with the methods used by drug traffickers to smuggle and safeguard controlled substances, to distribute, manufacture, and transport controlled substances, and to collect and launder related proceeds.

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 warrants and does not set forth all of my knowledge about this matter. Rather, I make this affidavit in support of an application for a warrant to search:

(1) 902 33rd Street, Sacramento, California (hereafter referred to as TARGET PROPERTY #1), further described in Attachment A-1;

(2) 7891 Iona Way, Sacramento, California (hereafter referred to as TARGET PROPERTY #2), further described in Attachment A-2;

(3) 8804 Lemas Road, Sacramento, California (hereafter referred to as TARGET PROPERTY #3), further described in Attachment A-3; (Collectively referred to as the "TARGET PROPERTIES")

(4) a Toyota Prius bearing California license plate number 7DBA021 and Vehicle Identification Number ("VIN") JTDKDTB39D1052068 registered to

Liliani Fatukala (hereafter referred to as FATUKALA VEHICLE), further described in Attachment A-4;

(5) a Honda Accord bearing California license plate number 6PMY435 and VIN 1HGCS1B80BA003561 registered to Bao T. Nguyen (hereafter referred to as YAMAMOTO VEHICLE), further described in Attachment A-5;

(6) a Subaru Outback bearing California license plate number 6ZLB767 and VIN 4S4BRBGC8D3271950 registered to Iris MINA (hereafter referred to as MINA VEHICLE), further described in Attachment A-6;

(7) a Toyota Corolla bearing California license plate number 7RTH204 and VIN 2T1BR30E25C550275 registered to Nicole Marie PACHECO (hereafter referred to as PACHECO VEHICLE), further described in Attachment A-7;

(8) a Toyota Camry bearing California license plate number 7CWS281 and VIN 4T1BF1FK8EU313038 registered to Mai Xian Chen (hereafter referred to as CHEN VEHICLE), further described in Attachment A-8; (Collectively referred to as the "TARGET VEHICLES")

the seizure of the items described in Attachment B;

the issuance of seizure warrants for all proceeds contained in the following financial accounts:

(1) Bank of America Account XXXX-XXXX-4003 held in the name of Lisa Chen Sole Prop DBA Chen Corner (hereafter referred to as the "CHEN CORNER ACCOUNT");

(2) Bank of America Account XXXX-XXXX-6120 held in the name of Iris J. Mina Sole Prop DBA The Mina Exchange (hereafter referred to as the "MINA EXCHANGE ACCOUNT");

(3) Coinbase Account Number 5b77079f866e4107fb2a3abf held in the name of Lisa Chen (hereafter referred to as the "CHEN COINBASE ACCOUNT");

(4) Coinbase Account Number 5b35d17515eed809808dad33 held in the name of Iris Mina (hereafter referred to as the "MINA COINBASE ACCOUNT");

and,

a criminal complaint naming VILIAMI MOSESE FATUKALA, QUYNHMY QUOC YAMAMOTO, and IRIS JUNE MICU MINA (Collectively referred to as "THE TARGETS").

For violations of:

Title 21 U.S.C. §§ 841(a)(1), 846 (Conspiracy to Distribute, and to Possess with Intent to Distribute a Controlled Substance).

III. OVERVIEW

During this investigation, federal law enforcement officers have: (1) observed QUYNHMY QUOC YAMAMOTO (hereafter "YAMAMOTO"), IRIS JUNE MICU MINA (hereafter "MINA"), SEMISI TOPUI (hereafter "TOPUI") and NICOLE MARIE PACHECO (hereinafter "PACHECO") place parcels containing narcotics into the United States Postal Service ("USPS") mail system; (2) observed VILIAMI MOSESE FATUKALA (hereafter "FATUKALA") present with other co-conspirators at the same location where parcels containing narcotics are packaged for shipment; (3) conducted undercover purchases of cocaine and oxycodone pills through a dark web marketplace vendor account and through direct deals via an encrypted messaging account believed to be controlled by FATUKALA and his co-conspirators; and (4) traced monies used in

undercover narcotics purchases by law enforcement officers to financial accounts controlled by MINA and Lisa CHEN (hereafter "CHEN"). In doing so, FATUKALA, YAMAMOTO, MINA, TOPUI, PACHECO and CHEN[1] are conspiring to distribute controlled substances. 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." 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."

IV. TECHNICAL BACKGROUND

5. Digital currency (also known as crypto-currency) 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.

6. Bitcoin[2] is a type of digital currency. Bitcoin payments are recorded in a public ledger that is maintained by peer-to-peer verification and is thus not maintained by a single administrator or entity. Individuals can acquire Bitcoins either by "mining" or by purchasing Bitcoins from other individuals. An individual can "mine" for Bitcoins by allowing his/her computing power to verify and record the Bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created Bitcoins.

[1] This affidavit does not seek criminal complaints against CHEN, TOPUI, or PACHECO, but their apparent involvement in the described activities is relevant to the overall conspiracy and the request for warrants to search and/or seize certain vehicles, locations, and bank accounts.

[2] On December 10, 2019, one Bitcoin is equal to approximately $7,230 USD.

7. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on any type of computer, including laptop computers and smart phones.

8. Bitcoins can be stored in digital "wallets." 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.

9. 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.

10. Through the dark web or darknet, i.e. websites accessible only through encrypted and anonymized means, individuals have established online marketplaces, such as the Silk Road, for narcotics and other illegal items. These markets often only accept payment through digital currencies, such as Bitcoin. Accordingly, a large amount of Bitcoin sales or purchases by an individual is often an indicator that the individual is involved in narcotics 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 Bitcoin as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoin to convert them to fiat (government-backed) currency. Such purchases and sales are often facilitated by peer-to-peer Bitcoin exchangers who advertise their services on websites designed to facilitate such transactions.

11. Dark web sites, such as Silk Road, AlphaBay, Empire, and SamSara, operate or operated on "The Onion Router" or "TOR" network. The TOR network ("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, which are many times generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software designed to access the TOR network.

V. SEIZURE AND FORFEITURE AUTHORITY

12. 18 U.S.C. § 981(a)(1)(A) subjects to forfeiture to the United States any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of Title 18 of the U.S. Code, or any property traceable to such property.

13. 18 U.S.C. § 981(a)(1)(C) subjects to forfeiture to the United States any property, real or personal, which constitutes, or is derived from the proceeds traceable to an offense constituting "a specified unlawful activity" as defined by § 1956(c)(7). Section 1956(c)(7) states that a "specified unlawful activity" includes any act defining as a "racketeering activity" per § 1961(1). Section 1961(1) lists acts relating to §§ 1956 and 1957 as racketeering activities.

14. 18 U.S.C. § 984 provides that where property involved in the forfeiture action is cash or monetary instruments in bearer form which are deposited into a financial institution, it shall not be necessary to identify the specific property involved in the offense and it shall not be a defense that the funds involved in the crime were deposited, removed and replaced with identical funds which were not used in the action arising to forfeiture of the funds. The forfeiture action involving the funds that is the basis of this violation must have occurred within the last one year of the offense and will be based on forfeiture of proceeds of illegal activity under 18 U.S.C. § 981(a)(1)(C).

15. Pursuant to 18 U.S.C. § 981(b)(3), and notwithstanding the provisions of Rule 41(a) of

the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against property may be filed and may be executed in any district in which the property is found.

16. Section 981(b) of Title 18 generally provides than any property subject to forfeiture under § 981(a) may be seized by the Attorney General pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure.

VI. FACTS ESTABLISHING PROBABLE CAUSE

A. Exploratory purchases of the NCIDE task force

17. I am part of the Northern California Illicit Digital Economy ("NCIDE") task force composed of DEA, Homeland Security Investigations ("HSI"), the Federal Bureau of Investigation ("FBI"), the United States Postal Inspection Service ("USPIS"), and the Internal Revenue Service Criminal Investigation Division ("IRS-CI"). As a function of this task force, investigators regularly purchase narcotics utilizing both digital and fiat currencies, from the persons operating and illegally selling narcotics on the "clear" portion of the internet, from the "dark" portion of the internet and from various social media platforms. Investigators conduct the undercover purchases of narcotics to assist in the effort to identify the suspects operating such illicit sites.

18. In or about July 2019, the NCIDE task force opened a joint investigation of Largomonkey, a dark web vendor involved in the mailing of controlled substances via the USPS. Largomonkey offers various quantities of cocaine, oxycodone pills and marijuana related products for sale via the SamSara Market, an illicit dark web marketplace, and through direct deals with customers via encrypted text messaging services such as Wickr. As is further described below, Largomonkey utilizes the Wickr moniker Sillycoconut to communicate with customers.

19. On or about July 5, 2019, an NCIDE task force investigator conducted an undercover purchase of 1/16 of an ounce of cocaine from Largomonkey and had the parcel sent to an address controlled by law enforcement in another state. The undercover order was made through direct communications with Largomonkey via the Sillycoconut Wickr account. The order was paid for with approximately .015 Bitcoin to Bitcoin address 13jS6Cw1aDnJsVFoSoERom6M3JgRyj41wv which was provided to the undercover NCIDE investigator by Largomonkey. On July 9, 2019, law enforcement received the package containing the July 5, 2019 undercover order. Investigators opened the package and discovered suspected cocaine weighing approximately two grams including the packaging. The suspected cocaine was concealed inside a wax mold of a Buddha head as shown in the picture below. The suspected cocaine was submitted to a DEA laboratory for analysis and tested positive for cocaine hydrochloride.

20. An inspection of the package revealed that it was shipped from Sacramento, California, in a USPS Priority Mail Padded Flat Rate Envelope. Based on the return label information and characteristics of the package from the July 5, 2019, undercover order, USPIS inspectors were able to determine, through an analysis of USPS databases and surveillance camera footage, that Largomonkey had established a USPS account to purchase postage and had mailed packages on a daily basis from different post offices located in the Sacramento area. Furthermore, USPIS analysis revealed that the post offices located at 2000 Royal Oaks Drive, Sacramento, California (hereinafter "Royal Oaks PO") and 2121 Broadway, Sacramento, California (hereinafter "Broadway PO") were frequently used by Largomonkey to mail packages.

21. Through continued analysis of USPS databases and surveillance camera footage, investigators identified FATUKALA, MINA and YAMAMOTO as the mailers of Largomonkey packages. On multiple occasions, MINA was captured on USPIS surveillance cameras dropping off parcels in the USPS blue bins at the Royal Oaks PO and was observed driving a Subaru Outback bearing California license plate 6ZLB767 (the "MINA VEHICLE"). On July 9, 2019, at approximately 1:40 p.m., a light blue Toyota Prius with a roof rack attached was observed on surveillance camera footage at the Royal Oaks PO. In the video, the Toyota Prius, subsequently identified in this investigation as the FATUKALA VEHICLE, stopped at the Royal Oaks PO and dropped off a female passenger, identified as YAMAMOTO. YAMAMOTO carried a grocery bag from the FATUKALA VEHICLE to the blue USPS mail bins and dropped parcels into the blue USPS mail bin before returning to the FATUKALA VEHICLE. Additionally, on July 23,

2019, YAMAMOTO was observed mailing parcels at the Royal Oaks PO and was observed driving a black Honda Accord with California license plate 6PMY435 (the "YAMAMOTO VEHICLE").

22. A public records search for MINA revealed that she was employed by the California Correctional Health Care Services located at 8260 Longleaf Drive, Elk Grove, California. On July 23, 2019, I located the MINA VEHICLE parked in the lot of MINA's place of employment. On the same date, USPIS investigators conducted surveillance on the MINA VEHICLE. During surveillance, USPIS investigators observed MINA enter the MINA VEHICLE and travel to a Bank of America branch in Elk Grove, California. MINA was observed exiting the Bank of America carrying an envelope consistent with the envelopes provided by banks for cash withdrawals. USPIS investigators maintained surveillance on MINA throughout the day and at approximately 5:08 p.m., USPIS investigators followed MINA in the MINA VEHICLE to a residence located at 902 33rd Street, Sacramento, California (TARGET PROPERTY #1). While at the residence, investigators observed the YAMAMOTO VEHICLE parked on the street in front of the residence.

23. On or about July 13, 2019, an NCIDE task force investigator conducted an undercover purchase of 7 grams cocaine and two pills of oxycodone from Largomonkey and had the parcel sent to an address controlled by law enforcement in another state. The undercover order was made through direct communications with Largomonkey via the Sillycoconut Wickr account. The order was paid for with approximately .0332 Bitcoin to Bitcoin address 15uBZU6DsfVRrpEb8EBSBAnaggBnfsucUz which was provided to the undercover NCIDE investigator by Largomonkey. On July 18, 2019, law enforcement opened the package containing the July 13, 2019 undercover order which bore USPS tracking number 9405503699300059098293. The undercover order was also shipped in a USPS Priority Mail Padded Flat Rate Envelope. Upon opening the parcel, investigators discovered suspected cocaine weighing approximately 7 grams and two blue colored pills of suspected oxycodone. The suspected cocaine and oxycodone pills were concealed inside the wax molds of two Buddha heads. The suspected cocaine was submitted to a DEA laboratory for analysis and tested positive for cocaine hydrochloride.

Largomonkey on the SamSara Marketplace

24. Largomonkey joined the SamSara marketplace on July 6, 2019 and offered cocaine, oxycodone pills and marijuana products in various forms to include extracts, resins, shatter, and marijuana buds in ounce quantities. As of November 1, 2019, Largomonkey had 264 reviews with a rating of 4.98 out of 5 stars. Under the "Terms and conditions" on Largomonkey's SamSara vendor page, Largomonkey claimed to have had "2000 transactions on Dream" with a "4.98 rating" out of 5 stars. Based on my training and experience and conversations with other law enforcement investigators knowledgeable of dark web investigations, I am aware that it is common for dark web vendors to make reference to their reviews and ratings from other dark web marketplaces as a means of gaining the customers' trust by showing to the customers that the vendor is an established and reputable seller.

Additional Undercover Purchases from Largomonkey and Surveillance of THE TARGETS

25. During the course of this investigation, NCIDE task force investigators conducted a total 16 undercover purchases of cocaine and/or oxycodone pills from Largomonkey. The undercover purchases were conducted through direct communication with Largomonkey via the Sillycoconut Wickr account and from Largomonkey's SamSara vendor page. In every instance, the undercover purchases were paid for with Bitcoin. For purchases conducted directly with Largomonkey through the Sillycoconut Wickr account, a Bitcoin address was provided by Largomonkey for payment and an NCIDE task force investigator directed the Bitcoin payment to the provided Bitcoin address. All of the undercover orders were shipped via USPS and contained fictitious sender information. Additionally, with the exception of one undercover order placed on August 22, 2019 for 2 ounces of cocaine, all of the undercover orders were shipped in USPS Priority Mail Padded Flat Rate Envelopes. Select undercover purchases are summarized in the following paragraphs. Following the undercover purchases, investigators conducted surveillance at TARGET PROPERTY #1. Agents observed FATUKALA, YAMAMOTO, and MINA entering and exiting TARGET PROPERTY #1 on numerous occasions, and I believe that they all reside at TARGET PROPERTY #1.

26. Furthermore, during the surveillances, investigators would observe the THE TARGETS mailing packages at multiple post offices in the Sacramento area often during the same trip. Based on my training and experience and conversations with other law enforcement investigators knowledgeable of dark web investigations, I am aware that it is common for dark web vendors to mail parcels at multiple post offices in an attempt to avoid the detection and seizure of their parcels by law enforcement.

27. On or about July 31, 2019, an NCIDE task force investigator conducted an undercover purchase of an eighth of an ounce of cocaine from Largomonkey's SamSara vendor page and had the package sent to a law enforcement controlled address in another state. The undercover order was paid for with Bitcoin. On August 1, 2019, law enforcement conducted surveillance at TARGET PROPERTY #1. During surveillance, law enforcement observed FATUKALA, YAMAMOTO and TOPUI at the residence. YAMAMOTO was observed carrying out a brown paper bag from the residence and entering a silver Honda sport utility vehicle bearing California license plate 5RXE168. Surveillance investigators followed YAMAMOTO from TARGET PROPERTY #1 to a post office located at 1618 Alhambra Blvd., Sacramento, California (hereinafter "Alhambra PO") and observed YAMAMOTO retrieve multiple packages from the brown paper bag and deposit the packages into a blue USPS mail bin. After YAMAMOTO departed from the Alhambra PO, a USPIS inspector responded to the Alhambra PO and located two packages mailed by YAMAMOTO inside the USPS mail bin including the package containing the undercover order placed the previous day. The USPIS inspector seized the package containing the undercover order which bore USPS tracking number 9405503699300074063788. The undercover order was also shipped in a USPS Priority Mail Padded Flat Rate Envelope. Upon opening the seized undercover package, investigators found approximately four grams of suspected cocaine concealed inside the wax mold of a Buddha head. The suspected cocaine was submitted to a DEA laboratory for analysis and tested positive for cocaine hydrochloride. The other package was not opened.

28. On or about August 6, 2019, an NCIDE task force investigator conducted an undercover purchase of 14 grams of cocaine from Largomonkey and had the parcel sent to an address controlled by law enforcement in another state. The undercover order was made through direct

communications with Largomonkey via the Sillycoconut Wickr account and paid for with Bitcoin sent to a Bitcoin address provided to the undercover investigator by Largomonkey. On August 7, 2019, at approximately 10:15 a.m., NCIDE investigators established surveillance at TARGET PROPERTY #1 and observed the FATUKALA VEHICLE parked in the driveway of the residence, and a silver Honda Pilot bearing California license plate 5RXE168 parked on the street in front of the residence. At approximately 1:03 p.m., surveillance agents observed TOPUI arrive at TARGET PROPERTY #1 in a Chevrolet Tahoe bearing California license plate 5MHF959. TOPUI exited his vehicle, retrieved a box from the passenger side of his vehicle walked to TARGET PROPERTY #1. At approximately 1:16 p.m., surveillance observed FATUKALA at TARGET PROPERTY #1. At approximately 3:00 p.m., surveillance observed YAMAMOTO walk from TARGET PROPERTY #1 carrying a brown grocery bag. YAMAMOTO walked to the silver Honda Pilot, entered the driver's seat of the vehicle along with the brown grocery bag and departed from TARGET PROPERTY #1. Surveillance agents followed YAMAMOTO to the Alhambra PO and observed YAMAMOTO entering the post office with the grocery bag. After approximately one minute, YAMAMOTO exited the post office, returned to the vehicle and departed from the post office. A USPIS Inspector responded to the Alhambra PO and identified four parcels that were mailed by YAMAMOTO including the August 6, 2019 undercover order. The USPIS Inspector also noted that three of the parcels mailed by YAMAMOTO were located in the lobby drop box and one parcel was located in a parcel locker. The USPIS Inspector seized the parcel containing the undercover order which bore USPS tracking number 9405511699000658943462. The undercover order was also shipped in a USPS Priority Mail Padded Flat Rate Envelope. Upon opening the seized undercover package, investigators found approximately 15 grams of suspected cocaine concealed inside the wax molds of two Buddha heads.

29. On August 9, 2019, a USPIS Inspector and I returned to the Alhambra PO and reviewed video surveillance footage of the post office lobby. On the video surveillance, YAMAMOTO was observed entering the post office at approximately 3:11 p.m. carrying a grocery bag and walking toward the lobby drop box before walking toward the parcel locker, opening the parcel locker and depositing one package. YAMAMOTO was then observed exiting the post office.

30. On or about August 22, 2019, an NCIDE task force investigator conducted an undercover purchase of 14 grams of cocaine from Largomonkey's SamSara vendor page and had the package sent to a law enforcement controlled address in another state. The undercover order was purchased with Bitcoin. On the same date, an NCIDE task force investigator conducted an undercover purchase of 2 ounces of cocaine via a direct deal with Largomonkey over the Sillycoconut Wickr account and had the package sent to a law enforcement controlled address in another state. The 2 ounces of cocaine was paid for with approximately .20718375 Bitcoin sent to Bitcoin address 1P889g1Grj2PonCHRMp9cXu54jFiNy9i6y which was provided to the undercover investigator by Largomonkey. On August 23, 2019, law enforcement conducted surveillance at TARGET PROPERTY #1 and observed FATUKALA, TOPUI and Nicole PACHECO (hereinafter "PACHECO") at the residence. At approximately 1:52 p.m., surveillance observed TOPUI arrive at TARGET PROPERTY #1 in a Chevrolet Tahoe bearing California license plate 5MHF959. TOPUI parked his vehicle and walked into TARGET PROPERTY #1 carrying a black colored briefcase. At approximately 3:19 p.m., PACHECO was observed by investigators arriving at the residence in the PACHECO VEHICLE. I observed PACHECO exit the PACHECO VEHICLE and retrieve two flattened Priority Mail boxes from her vehicle and carry the boxes into TARGET PROPERTY #1. After approximately 20 minutes, PACHECO exited TARGET PROPERTY #1 carrying a large plastic bag and placed the plastic bag inside the trunk of the PACHECO VEHICLE before departing from TARGET PROPERTY #1. Surveillance then observed PACHECO pick up a white male passenger standing around the corner from TARGET PROPERTY #1, later identified as Tracy Bayless (hereinafter "Bayless"). Surveillance followed PACHECO and Bayless in the PACHECO VEHICLE to a post office located at 4750 J Street, Sacramento, California (hereinafter "J Street PO"). Both PACHECO and Bayless were observed mailing multiple parcels at the J Street PO. After PACHECO and Bayless departed from the J Street PO, a USPIS inspector responded to the post office and located two parcels mailed by PACHECO and Bayless including the parcel containing the August 22, 2019 undercover order. The USPIS Inspector seized the parcel containing the undercover order which bore USPS tracking number 9405511699000866446076. The undercover order was also shipped in a USPS Priority Mail Padded Flat Rate Envelope. Upon opening the seized undercover package, investigators found approximately 15 grams of suspected cocaine concealed inside the wax molds of two Buddha heads.

31. On the same date, at approximately 4:34 p.m., surveillance observed TOPUI and FATUKALA exit TARGET PROPERTY #1. TOPUI carried out multiple grocery/shopping bags from the residence and placed the bags into the passenger side of his vehicle before departing from TARGET PROPERTY #1. Surveillance followed TOPUI from TARGET PROPERTY #1 and observed TOPUI stop at the Alhambra PO and mail two packages. Surveillance then followed TOPUI to the Broadway PO and observed TOPUI mail two additional packages. An examination of the parcels mailed by TOPUI at the Broadway PO revealed that one of parcels was addressed to the name and address used for the undercover order of 2 ounces of cocaine from Sillycoconut on August 22, 2019. An NCIDE investigator seized the parcel containing the undercover order which bore USPS tracking number 940551169900086644617 5. Upon opening the seized undercover package, investigators found approximately 59 grams of suspected cocaine concealed inside the wax molds of eight Buddha heads.

32. On or about September 5, 2019, an NCIDE investigator conducted an order of 16 pills of oxycodone via a direct deal with Largomonkey over the Sillycoconut Wickr account and had the package sent to a law enforcement controlled address in another state. The oxycodone pills were paid for with approximately .03781665 Bitcoin sent to Bitcoin address 1AoeiSrtXXqA1frzaeSaUDod83yKBoXy8h which was provided to the undercover investigator by Largomonkey. On September 16, 2019, NCIDE task force investigators opened the parcel containing the September 5, 2019 undercover order which bore USPS tracking number 940550369930010435976 8. The undercover order was also shipped in a USPS Priority Mail Padded Flat Rate Envelope. Upon opening the seized undercover package, investigators found approximately 16 blue colored pills of suspected oxycodone concealed inside the wax mold of a Buddha head.

33. On or about October 8, 2019, an NCIDE task force investigator conducted an undercover purchase of 7 grams of cocaine via a direct deal with Largomonkey over the Sillycoconut Wickr account and had the package sent to a law enforcement controlled address in another state. On October 18, 2019, NCIDE task force investigators opened the parcel containing the October 8, 2019 undercover order which bore USPS tracking number 940550369930013423076 1. The

undercover order was also shipped in a USPS Priority Mail Padded Flat Rate Envelope. Upon opening the undercover package, investigators found approximately 7 grams of suspected cocaine concealed inside the wax mold of a pineapple as shown in the picture below.

34. On October 9, 2019, law enforcement conducted surveillance at TARGET PROPERTY #1 and observed FATUKALA, YAMAMOTO and TOPUI at the residence. During surveillance, I observed TOPUI walking from the residence carrying a white plastic bag and a black briefcase style bag to a black Hyundai sedan bearing California license plate 6RMD867. TOPUI entered the Hyundai sedan and was followed by surveillance investigators to a post office located at 5930 S Land Park Drive, Sacramento, California (hereinafter "Land Park PO"). I observed TOPUI enter the Land Park PO carrying a white plastic bag and walking to the parcel drop box in the lobby of the post office. After TOPUI departed from the Land Park PO, I inspected the packages in the parcel drop box and identified four packages mailed by TOPUI that were consistent in size, shape and packaging material to Largomonkey packages previously seized by law enforcement.

35. On October 18, 2019, law enforcement installed a pole camera on a utility pole located near TARGET PROPERTY #1. The pole camera was oriented to capture video of the front of TARGET PROPERTY #1 including the driveway and street directly in front of the residence.

On October 19, 2019, at approximately 9:40 a.m., while monitoring the pole camera, I observed CHEN arrive in the CHEN VEHICLE park in front of TARGET PROPERTY #1. CHEN exited her vehicle with a backpack and walked to the front door of TARGET PROPERTY #1.

36. On October 23, 2019 at approximately 2:47 p.m., TOPUI was observed on the pole camera exiting TARGET PROPERTY #1 carrying a brown grocery bag and briefcase. TOPUI placed the grocery bag and briefcase into his vehicle and departed from the residence. At approximately 2:48 p.m., PACHECO was observed walking up to and entering TARGET PROPERTY #1 carrying a brown grocery bag. The grocery bag appeared slightly collapsed, and PACHECO was swinging the bag indicating that the bag was empty. At approximately 2:54 p.m., PACHECO exited TARGET PROPERTY #1 carrying a brown grocery bag that appeared fuller and heavier as PACHECO did not swing the bag as she walked. PACHECO walked across the street from TARGET PROPERTY #1 out of view of the camera. On the same date, at approximately 4:44 p.m., I drove by TARGET PROPERTY #3 and observed the PACHECO VEHICLE parked in the driveway of the residence.

37. On or about November 11, 2019, an NCIDE task force investigator conducted an undercover purchase of 14 grams of cocaine via a direct deal with Largomonkey over the Sillycoconut Wickr account and had the package sent to a law enforcement controlled address in another state. On November 15, 2019, NCIDE task force investigators opened the parcel containing the November 11, 2019 undercover order which bore USPS tracking number 9405503699300162161556. The undercover order was also shipped in a USPS Priority Mail Padded Flat Rate Envelope. Upon opening the undercover package, investigators found approximately 14 grams of suspected cocaine concealed inside the wax molds of two pineapples.

38. On November 14, 2019, an FBI team conducted surveillance on PACHECO. The FBI surveillance team observed PACHECO and Bayless arrive at TARGET PROPERTY #1 in a black Toyota Corolla bearing California license plate 8KYX156. From TARGET PROPERTY #1, surveillance members observed PACHECO mail multiple parcels at the Broadway PO, Land Park PO and a post office located at 4301 Brookfield Drive, Sacramento, California (hereafter referred to as the "Brookfield PO"). A member of the surveillance team entered the Brookfield PO and identified two parcels mailed by PACHECO. After observing PACHECO mail the

parcels, the FBI team maintained surveillance on PACHECO and observed PACHECO stop at a retail location and restaurant before arriving at her residence located at 8804 Lemas Road, Sacramento, California (TARGET PROPERTY #3). The surveillance team observed PACHECO park her vehicle in the driveway of TARGET PROPERTY #3 and enter the residence through the garage. Surveillance was also conducted on November 19, 2019 at TARGET PROPERTY #3 by an FBI surveillance team. PACHECO was observed by the surveillance team at TARGET PROPERTY #3. PACHECO's vehicle is also registered under the address pertaining to TARGET PROPERTY #3.

39. On or about November 24, 2019, an NCIDE task force investigator conducted an undercover purchase of 14 grams of cocaine via a direct deal with Largomonkey over the Sillycoconut Wickr account and had the package sent to a law enforcement controlled address in another state. The undercover order was paid for with Bitcoin sent to a Bitcoin address provided to the undercover investigator by Largomonkey. On November 25, 2019, investigators conducted surveillance at TARGET PROPERTY #1. During surveillance, investigators observed FATUKALA, MINA and PACHECO at TARGET PROPERTY #1. At approximately, 2:21 p.m., MINA was observed exiting TARGET PROPERTY #1 carrying a grocery bag and entering the MINA VEHICLE with the grocery bag. The surveillance team followed MINA to a post office located at 10923 Progress Court, Rancho Cordova, California (hereafter "Rancho PO") and observed MINA mail two parcels in the blue USPS mail bin located outside of the Rancho PO. After MINA left the Rancho PO, I examined the blue mail bins where MINA had deposited the two parcels and identified the two parcels mailed by MINA that were consistent in size, shape and packaging material to Largomonkey packages previously seized by law enforcement. The surveillance then followed MINA to a post office located at 7862 Winding Way, Fair Oaks, California (hereafter "Fair Oaks PO") and observed MINA mail a parcel at the Fair Oaks PO. A member of the surveillance team entered the Fair Oaks PO and identified the parcels mailed by MINA. I responded to the Fair Oaks PO and examined the parcel mailed by MINA and observed the parcel to be consistent in size, shape and packaging material to Largomonkey packages previously seized by law enforcement. Agents did not seize the package.

40. At approximately 3:05 p.m., surveillance observed PACHECO arrive at TARGET PROPERTY #1 in the PACHECO VEHICLE. About a minute later, PACHECO carried out a white colored bag from TARGET PROPERTY #1, placed the bag into the trunk of the PACHECO VEHICLE and departed from TARGET PROPERTY #1 in the PACHECO VEHICLE. Surveillance followed PACHECO to the Bel Air grocery store located at 9435 Elk Grove Boulevard, Elk Grove, California and observed PACHECO mail parcels in the USPS blue bin mailbox located at the front entrance of the Bel Air. At approximately 4:30 p.m., I responded to the Bel Air grocery store and met with the postal carrier who was at the store picking up mail. The postal carrier opened the USPS blue bin mailbox, and I observed two parcels inside the mailbox that were consistent in size, shape and packaging material to Largomonkey packages previously seized by law enforcement. A closer examination of the two parcels revealed that one of the parcels mailed by PACHECO was addressed to the name and address used for the undercover order of 14 grams of cocaine from Sillycoconut on November 24, 2019. I seized the parcel containing the undercover order which bore USPS tracking number 9405503699300174503016. Upon opening the seized undercover package, investigators found approximately 15 grams of suspected cocaine concealed inside the wax molds of two Buddha heads.

Identification of a Social Media Account for FATUKALA

41. Based on a public records and Internet search, investigators have identified a social media account for FATUKALA on Instagram. Instagram username positivepineapple_1 was identified as an Instagram account utilized by FATUKALA. The positivepineapple_1 is set as a public account and content posted to the account is freely viewable to the public. Investigators have verified that FATUKALA is the user of the positivepineapple_1 account through a review of the content posted on the account which features photographs of FATUKALA. On or about July 25, 2019, an NCIDE investigator reviewed the postings on the positivepineapple_1 Instagram account and observed a photograph of an unidentified minor sitting at a table at the Nektar Juice Bar. The photograph bore a caption of "Silly coconut" and an emoji of a hand with an extended thumb and pinky on the photo. As previously described, Sillycoconut is the Wickr moniker used by Largomonkey to conduct direct drug deals with customers. On the profile page for the

positivepineapple_1 Instagram account, FATUKALA posted the statement "Everyday Journey of the #pineapple." As previously described in paragraphs 33 and 37, the undercover cocaine orders made by NCIDE investigators on or about October 8, 2019 and November 11, 2019 from Largomonkey were concealed in wax molds of pineapples. Additionally, FATUKALA is seen wearing a fanny pack branded with pineapples in social media postings, and YAMAMOTO can be seen wearing a black hat bearing a pineapple in her social media posts. In nearly every Instagram video posted by FATUKALA, he opens the video by saying "Team Pineapple, Team Pineapple, yes yes yes yes yes."

USPS Records

42. Based on the USPS tracking numbers and sender information included on the mailing labels from the undercover drug orders, USPIS Inspectors have identified at least eight USPS shipping accounts utilized by Largomonkey to mail drug packages. In each instance, the shipping accounts were set up under fictitious names and addresses. An analysis of the total shipping activity over the eight USPS shipping accounts, USPIS Inspectors have identified a total of approximately 763 shipments made by Largomonkey from February 27, 2019 through December 9, 2019. Additionally, USPIS Inspectors identified a stamps.com shipping account used by Largomonkey. A review of the stamps.com account revealed a total of 175 shipments made by Largomonkey from January 1, 2019 through December 9, 2019.

Coinbase Records

43. During this investigation, investigators obtained records for Coinbase accounts owned by FATUKALA, CHEN and MINA. As previously described in this affidavit, all undercover purchases for drugs from Largomonkey were paid for with Bitcoin. In the instances where undercover purchases were made via direct deals through the Sillycoconut Wickr account, Largomonkey provided Bitcoin addresses to the undercover investigator for payment. After reviewing public and open records including the public Bitcoin ledger on the Bitcoin blockchain and Coinbase records obtained for Coinbase accounts held by CHEN and MINA, I have traced

the Bitcoin drug payments made by undercover investigators in whole or part to Bitcoin accounts and then to traditional bank accounts held by CHEN and MINA.

44. Coinbase Account Number 5b77079f866e4107fb2a3abf (CHEN COINBASE ACCOUNT) was created by CHEN on August 17, 2018. CHEN listed 7891 Iona Way, Sacramento, California (TARGET PROPERTY #2) as her address and linked Bank of America account XXXX-XXXX-4003, which was subsequently identified as the CHEN CORNER ACCOUNT, to the CHEN COINBASE ACCOUNT. The CHEN CORNER ACCOUNT was the only bank account associated with the CHEN COINBASE ACCOUNT. A review of the transaction history for the CHEN COINBASE ACCOUNT revealed that CHEN began conducting Bitcoin transactions in the account on March 11, 2019. From March 11, 2019 through December 11, 2019, CHEN received and sold 55.60066 Bitcoin, which is equal to approximately $419,482.70. The transaction history also showed that CHEN received Bitcoin on an almost daily basis and upon receipt of the Bitcoin, would immediately sell the Bitcoin for U.S. Currency. CHEN then immediately transfers the U.S. Currency from the CHEN COINBASE ACCOUNT to the CHEN CORNER ACCOUNT.

45. Coinbase Account Number 5b35d17515eed809808dad33 (MINA COINBASE ACCOUNT) was created by MINA on June 28, 2018. MINA listed 4510 Careyback Avenue, Elk Grove, California as her address and on or about March 26, 2019, linked Bank of America account XXXX-XXXX-6120, which was subsequently identified as the MINA EXCHANGE ACCOUNT, to the MINA COINBASE ACCOUNT. A review of the transaction history for the MINA COINBASE ACCOUNT revealed that MINA began conducting Bitcoin transactions in the account on July 6, 2018. From July 6, 2018 through December 5, 2019, MINA received and sold 19.15016 Bitcoin, which is equal to approximately $146,928.60. An analysis of the transaction history showed MINA frequently received small amounts of Bitcoin, typically equivalent to less than $500, into her account from July 2018 through March 19, 2019. After MINA added the MINA EXCHANGE ACCOUNT to the MINA COINBASE ACCOUNT on March 26, 2019, the value of the Bitcoin transactions received in her account increased to values exceeding $1,000. For example, from July 6, 2018 through March 19, 2019, there were 39 transactions where Bitcoin was received and converted to U.S. Currency for a total of $12,816.45

and an average transaction value of $328. In contrast, from March 27, 2019 through December 5, 2019, there were 82 transactions where Bitcoin was received and converted to U.S. Currency for a total of $134,112.16 and an average transaction value of $1,635.51. Like the activity in the CHEN COINBASE ACCOUNT, MINA would sell the Bitcoin for U.S. Currency and then immediately transfer the U.S. Currency her linked bank account. From March 26, 2019 through September 28, 2019, MINA withdrew the U.S. Currency from the MINA COINBASE ACCOUNT to the MINA EXCHANGE ACCOUNT.

46. On or about July 5, 2019, an NCIDE task force investigator sent approximately .015 Bitcoin to a Largomonkey provided Bitcoin address of 13jS6Cw1aDnJsVFoSoERom6M3JgRyj41wv as payment for an undercover purchase of 1/16 of an ounce of cocaine. The undercover order was made through direct communications with Largomonkey via the Sillycoconut Wickr account. By analyzing the undercover transaction on the Bitcoin blockchain, I traced approximately .014 Bitcoin sent to the MINA COINBASE ACCOUNT and approximately .001 Bitcoin sent to the CHEN COINBASE ACCOUNT. Following receipt of the Bitcoin into the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT, CHEN and MINA converted the Bitcoin to U.S. Currency and withdrew the U.S. Currency to their linked bank accounts. For CHEN, the U.S. Currency was transferred to the CHEN CORNER ACCOUNT while MINA withdrew the U.S. Currency to the MINA EXCHANGE ACCOUNT.

47. On or about July 13, 2019, an NCIDE task force investigator sent approximately .0332 Bitcoin to a Largomonkey provided Bitcoin address of 15uBZU6DsfVRrpEb8EBSBAnaggBnfsucUz as payment for an undercover purchase of 7 grams of cocaine and two pills of oxycodone. The undercover order was made through direct communications with Largomonkey via the Sillycoconut Wickr account. By analyzing the undercover transaction on the Bitcoin blockchain, I traced approximately .02877496 Bitcoin sent to the CHEN COINBASE ACCOUNT on or about July 16, 2019. Following receipt of the Bitcoin into the CHEN COINBASE ACCOUNT, CHEN converted the Bitcoin to U.S. Currency and withdrew the U.S. Currency to the CHEN CORNER ACCOUNT.

48. On or about August 22, 2019, an NCIDE task force investigator sent approximately .20718375 Bitcoin to a Largomonkey provided Bitcoin address of 1P889g1Grj2PonCHRMp9cXu54jFiNy9i6y as payment for an undercover purchase of 14 grams of cocaine. The undercover order was made through direct communications with Largomonkey via the Sillycoconut Wickr account. By analyzing the undercover transaction on the Bitcoin blockchain, I traced approximately .236432 Bitcoin sent to the CHEN COINBASE ACCOUNT on or about August 22, 2019. It is believed that the .20718375 Bitcoin payment made by the NCIDE task force investigator was combined with another Bitcoin transaction and comprised part of the .236432 Bitcoin that was sent to the CHEN COINBASE ACCOUNT.

49. On or about September 5, 2019, an NCIDE task force investigator sent approximately .03781665 Bitcoin to a Largomonkey provided Bitcoin address of 1AoeiSrtXXqA1frzaeSaUDod83yKBoXy8h as payment for an undercover purchase of 16 pills of oxycodone. The undercover order was made through direct communications with Largomonkey via the Sillycoconut Wickr account. By analyzing the undercover transaction on the Bitcoin blockchain, I traced the .03781665 undercover payment in parts to the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT. The .03781665 payment was combined and split through a series of Bitcoin transfers before being received in the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT. Specifically, I identified three Bitcoin deposits into the CHEN COINBASE ACCOUNT that I believe consisted of parts of the undercover Bitcoin payment including a .209498 Bitcoin deposit on September 5, 2019, and two Bitcoin deposits on September 9, 2019 in the amounts of .247159 Bitcoin and .225935 Bitcoin. Furthermore, I identified a .156672 Bitcoin deposit on September 6, 2019 in the MINA COINBASE ACCOUNT that I believe consists of a part of the undercover Bitcoin payment based by my analysis of the transaction through the Bitcoin blockchain. Following receipt of the Bitcoin into the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT, CHEN and MINA converted the Bitcoin to U.S. Currency and withdrew the U.S. Currency to their linked bank accounts. For CHEN, the U.S. Currency was transferred to the CHEN CORNER ACCOUNT while MINA withdrew the U.S. Currency to the MINA EXCHANGE ACCOUNT.

50. Coinbase Account Number 5b488667df6dca0d3637897b (hereafter referred to as the "FATUKALA COINBASE ACCOUNT") was created by FATUKALA on July 13, 2018. FATUKALA listed 7790 19th Street, Sacramento, California as his address and linked Chase Bank account XXXXX7803. A review of the transaction history for the FATUKALA COINBASE ACCOUNT revealed that FATUKALA began conducting Bitcoin transactions in the account on July 13, 2018. From July 13, 2018 through June 6, 2019, FATUKALA received 134.3490889 Bitcoin and sold 129.5704514 Bitcoin in his account. The value of the Bitcoin sold by FATUKALA was equal to approximately $624,718.11. The transaction history also showed the same pattern of activity as the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT in that Bitcoin was received at an average frequency of every two to three days and would be sold for U.S. Currency. FATUKALA would then immediately transfer the U.S. Currency to his linked bank account. In or around February 2019, the frequency at which FATUKALA received Bitcoin into the FATUKALA COINBASE ACCOUNT began to taper off. This coincides with the time period in which CHEN and MINA began experiencing an increase in Bitcoin activity in their Coinbase accounts. It is my belief that during this time, FATUKALA began transitioning more responsibility of receiving Bitcoin from Largomonkey drugs sales to MINA and CHEN.

51. Based on the above, it is my belief that the foregoing evidence shows that Bitcoin received into the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT are proceeds of illegal drug trafficking earned through illicit Largomonkey drug sales. It is also my belief that the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT were utilized to convert the illegal drug proceeds in the form of Bitcoin into U.S. Currency and to transfer the U.S. Currency to additional financial accounts thereby laundering the illegal drug proceeds in violation of Title 18 U.S.C. §§ 1956 (Money Laundering). I hereby respectfully request that seizure warrants be issued for the CHEN COINBASE ACCOUNT and MINA COINBASE ACCOUNT.

Bank Records for Lisa CHEN and Iris MINA

52. During the course of this investigation, records for bank accounts controlled by MINA and CHEN were obtained from Bank of America including account XXXX-XXXX-4003 held in the name of Lisa Chen Sole Prop DBA Chen Corner (CHEN CORNER ACCOUNT) and account XXXX-XXXX-6120 held in the name of Iris J. Mina Sole Prop DBA The Mina Exchange (MINA EXCHANGE ACCOUNT). The time period of account records from Bank America were from March 2019 through August 2019.

53. The CHEN CORNER ACCOUNT was opened on or about March 7, 2019 by CHEN with an opening deposit of $100. CHEN is the sole owner and signer of the CHEN CORNER ACCOUNT. TARGET PROPERTY #2 is listed as the mailing address for the CHEN CORNER ACCOUNT. The CHEN CORNER ACCOUNT is also the bank account linked to the CHEN COINBASE ACCOUNT. I have examined the deposit and withdrawal activity for the CHEN CORNER ACCOUNT from March 7, 2019 through August 30, 2019. With the exception of the account opening deposit, the only source of deposits into the CHEN CORNER ACCOUNT are transfers from the CHEN COINBASE ACCOUNT. There were a total of 123 deposits totaling $245,073.61 into the CHEN CORNER ACCOUNT that originated from the CHEN COINBASE ACCOUNT. The frequency of the deposits and withdrawals for the CHEN CORNER ACCOUNT were such that CHEN was making trips to a Bank of America branch on an average of approximately every one to two days. In each instance, CHEN would withdrawal an amount in cash that was almost equal to the amount deposited into the account from the CHEN COINBASE ACCOUNT. As an example, on August 30, 2019, there were two deposits totaling $4,491 into the CHEN CORNER ACCOUNT originating from the CHEN COINBASE ACCOUNT. On the same date, CHEN conducted a cash withdrawal totaling $4,500 from the CHEN CORNER ACCOUNT. This pattern of activity was consistent during the observed time period.

54. On November 4, 2019, an FBI team conducted surveillance on CHEN at TARGET PROPERTY #2. During surveillance, CHEN was observed leaving TARGET PROPERTY #2 in the CHEN VEHICLE. Surveillance followed CHEN to the Bank of America located at 8842

Calvine Road, Sacramento, California and observed CHEN enter the bank. A surveillance member followed CHEN into the bank and observed CHEN at the counter interacting with the bank teller. The surveillance team member overheard CHEN tell the bank teller "Four thousand" and an additional unknown number to which the teller responded and said "That's pretty consistent for you." The teller was then observed handing CHEN multiple one hundred-dollar bills. Surveillance was maintained on CHEN until she returned to TARGET PROPERTY #2. During the four days prior to CHEN's cash withdrawal on November 4, 2019, CHEN conducted three withdrawals totaling $7,126 from the CHEN COINBASE ACCOUNT to the CHEN CORNER ACCOUNT.

55. On December 2, 2019 at approximately 6:27 p.m., I drove by TARGET PROPERTY #2 and observed CHEN in the CHEN VEHICLE arrive at TARGET PROPERTY #2 and park in the garage of the residence.

56. Based on the above, it is my belief that the foregoing evidence shows that funds received into the CHEN CORNER ACCOUNT and MINA EXCHANGE ACCOUNT are proceeds of illegal drug trafficking. Additionally, it is my belief that the accounts were opened solely to transfer the proceeds earned through illicit Largomonkey drug sales from the CHEN COINBASE ACCOUNT and the MINA COINBASE ACCOUNT and to convert the illegal drug proceeds into U.S. Currency thereby laundering the illegal drug proceeds in violation of Title 18 U.S.C. § 1956 (Money Laundering). I hereby respectfully request that seizure warrants be issued for the CHEN CORNER ACCOUNT and MINA EXCHANGE ACCOUNT.

Employment and Wage Information for FATUKALA, MINA and CHEN

57. I obtained records from the California Employment Development Department ("EDD") concerning employer and wage information for FATUKALA, MINA and CHEN. According to EDD records, there were no reported wages for FATUKALA from January 1, 2017 through August 2019. MINA had reported wages totaling $72,364.49 in 2017, $88,751.33 in 2018 and $36,242.94 from January 1, 2019 through August 2019. The employer listed for MINA was the California Correctional Health Care Services. CHEN had reported wages totaling $1,059 in

2017, $14,527 in 2018 and $3,056 from January 1, 2019 through August 2019. The employer listed for CHEN was Bista Co. of Elk Grove, California.

VII. METHODS AND MEANS OF USING THE UNITED STATES MAIL

58. Based on my experience, training, and discussions with other law enforcement officers experienced in drug investigations, I know that certain indicators exist when persons use the United States Mail to ship controlled substances from one location to another. Indicators for parcels that contain controlled substances and/or proceeds from controlled substances include, but are not limited to, the following:

a. It is common practice for shippers of the controlled substances to use Express Mail and Priority Mail because the drugs arrive at the destination more quickly and on a predictable date. Express Mail and Priority Mail, when paired with a special service such as delivery confirmation, allow traffickers to monitor the progress of the shipment of controlled substances. Traffickers pay for the benefit of being able to confirm the delivery of the parcel by checking the Postal Service Internet website and/or calling the local post office.

b. Packages containing controlled substances or proceeds have, in many instances, a fictitious return address, incomplete return address, no return address, a return address that is the same as the addressee address, or a return address that does not match the place from which the parcel was mailed. These packages are also sometimes addressed to or from a commercial mail receiving agency (*e.g.*, Mail Boxes Etc.). A shipper may also mail the parcel containing controlled substances from an area different from the return address on the parcel because: (1) the return address is fictitious or (2) the shipper is attempting to conceal the actual location from which the parcel was mailed. These practices are used by narcotics traffickers to hide from law enforcement officials the true identity of the persons shipping and/or receiving the controlled substances or proceeds.

c. Individuals involved in the trafficking of controlled substances through the United States Mail will send and receive Express or Priority mailings on a more frequent basis than a normal postal customer. Drug traffickers use Express Mail and Priority Mail at a higher rate due to their frequent exchanges of controlled substances and the proceeds from the sale of these controlled substances.

d. In order to conceal the distinctive smell of controlled substances from narcotics detection dogs, these packages tend to be wrapped excessively in bubble-pack and wrapping plastic, and are sometimes sealed with the use of tape around all seams. In addition, the parcels often contain other smaller parcels which are carefully sealed to prevent the escape of odors. Perfumes, coffee, dryer sheets, tobacco, or other substances with strong odors are also sometimes used to mask the odor of the controlled substances being shipped. Drug traffickers often use heat/vacuum sealed plastic bags, and/or re-sealed cans in an attempt to prevent the escape of orders.

e. California is typically a source state for drugs. It is common for individuals in California to mail parcels containing narcotics to other states and then receive mail parcels containing cash payments in return.

59. Based on my training and experience and discussions with other law enforcement officers, I know that parcels shipped by drug traffickers sometimes contain information and documentation related to the sales and distribution of controlled substances. The documentation can include, but is not limited to, information and instructions on the breakdown and distribution of the controlled substances at the destination; information on the use and effects of the various controlled substances; information about the actual sender; pay/owe sheets; and information and instructions for ordering future controlled substances.

60. Drug traffickers who use the United States Mail and other carriers as a means of distributing controlled substances, paraphernalia, and proceeds, and as a means of communicating with co-conspirators often include the following in parcels relating to their

trafficking activity, all of which are evidence, fruits, proceeds, and/or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1), 843(b), and 846:

a. Controlled substances, including heroin, cocaine, methamphetamine, and marijuana.

b. Packaging, baggies, and cutting agents, including items used to conceal the odor of narcotics, such as perfumes, coffee, dryer sheets, tobacco, or other substances with a strong odor.

c. Records reflecting the mailing or receipt of packages through Express Mail, Priority Mail, Federal Express, UPS or any other common carrier.

d. United States and foreign currency, securities, precious metals, jewelry, stocks, bonds, in amounts exceeding $500, including financial records related to the laundering of illicitly obtained monies and/or other forms of assets, including United States currency acquired through the sales, trafficking, or distribution of controlled substances.

e. Records reflecting or relating to the transporting, ordering, purchasing, and/or distribution of controlled substances, including but not limited to books, receipts, notes, ledgers, pay and owe sheets, correspondence, records noting price, quantity, date and/or times when controlled substances were purchased, possessed, transferred, distributed, sold or concealed.

f. Records reflecting or relating to co-conspirators, including but not limited to personal notes, correspondence, cables, telegrams, personal address lists, listings of telephone numbers, and other items reflecting names, addresses, telephone numbers, communications, and illegal activities of associates and conspirators in controlled substance trafficking activities.

g. Indicia or other forms of evidence showing dominion and control, or ownership of mail parcels, locations, vehicles, storage areas, safes, lock boxes, and/or containers related to the storage of controlled substances or proceeds.

VIII. SEARCH OF DIGITAL INFORMATION

61. Your affiant is aware that users and vendors of online black markets use a computer to access the dark web where online black markets are located. Your affiant is also aware that individuals must use an electronic device to locate and communicate with bitcoin exchangers and purchase bitcoins. Users have to establish an account on an online black market's website to purchase goods and also establish accounts to initiate initial trades with bitcoin exchangers. Users also must establish electronic wallets to receive and send bitcoins to purchase drugs. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, and/or computers. Your affiant is aware that once contact is made with a bitcoin exchanger on a digital currency exchange platform such as localbitcoins.com, all subsequent contact and transactions can be conducted from one phone to the other during a face to face transaction, exchanging currency for bitcoins. Your affiant is also aware that users can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access to online black markets, as well as for electronic wallets, are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. Your affiant believes that these are located in the TARGET PROPERTIES, TARGET VEHICLES and on the person of THE TARGETS.

62. As described above and in Attachment B, your affiant submits that computers, smart phones, and possibly other storage media will be found within the TARGET PROPERTIES, TARGET VEHICLES and on the person of THE TARGETS and there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. Furthermore, your affiant submits that sufficient probable cause has been established to search and seize any online black-market vendor accounts, online digital currency

exchange platform accounts, and the data contained therein. Due to the inherent illicit and anonymous nature of these accounts, and that there is no identified service provider for these accounts, legitimate, compliant or not, to which legal process may be served; your affiant believes this to be the only manner to recover said evidence.

63. For example, based on my knowledge, training, and experience, your affiant is aware that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

64. Based on my knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little to 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 computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—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.

65. Also, again based on your affiant's training and experience, wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from

operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium 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). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

66. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

67. Thus, the forensic analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

68. In cases of this sort, laptop computers and/or smartphones are also used as instrumentalities of the crime to commit offenses involving interstate drug sales and movement of drug proceeds. Devices such as modems and routers can contain information about dates,

frequency, and computer(s) used to access the Internet. The laptop or smart phone may also have fingerprints on them indicating the user of the computer and its components.

69. Similarly, files related to the purchasing and selling of controlled substances, as well as, the movement of currency found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the data, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary internet directory or "cache". The browser often 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 viewed internet pages or if a user takes steps to delete them. 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 user's operating system, storage capacity, and computer habits.

70. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Your affiant knows from training and experience and discussions with other law enforcement officers that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of internet connection at the residence.

71. Searching the computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or internet use is located in various operating system log files that are not easily located or

reviewed. In addition, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this location (the computer) for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

72. Based upon knowledge, training and experience, your affiant knows that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

73. The nature of evidence: As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

74. The volume of evidence and time required for an examination: Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

75. Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off- site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

76. Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

77. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

IX. REQUEST FOR SEALING

78. Finally, your affiant respectfully requests that this Court issue an order restricting, until further order of the Court, this case, to include, the Application and Search Warrant. I believe that restricting these documents are necessary to protect the identity of cooperating individuals, because the items and information to be seized are relevant to an ongoing investigation into a criminal organization, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, your affiant has learned that online criminals actively search for criminal Affidavits and Search Warrants via the Internet and disseminate them to others actively seeking out information over the Web and other sources concerning law enforcement activity in this arena. Accordingly, premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

X. CONCLUSION

79. Based on the facts set forth in this Affidavit, I believe there is probable cause that evidence, fruits, proceeds, or instrumentalities of violations of 21 U.S.C. § 846 (Conspiracy to Manufacture, to Distribute, and to Possess with Intent to Distribute a Controlled Substance), are concealed in the locations identified in Attachments A-1 through A-8. Accordingly, I respectfully request the issuance of search warrants authorizing the search of the locations described in Attachments A-1 through A-8, as well as the seizure of items described in Attachment B.

80. I also request that any vehicles under the control of the FATUKALA, MINA, YAMAMOTO, PACHECO, TOPUI, and CHEN are to be searched at the time these warrants are served, as evidenced by Department of Motor Vehicle registration information, possession of keys to the vehicle, observations of the utilization of those vehicle by the occupants, and witness statements or admissions. Based on my training and experience, and through interaction with other experienced law enforcement officers, I know that drug traffickers commonly transport and store

the evidentiary items listed in Attachment B in their vehicles. I also know that these vehicles are not commonly registered to the person who has control over them.

81. I request that all bulk marijuana seized during execution of the search warrants be disposed of, except for representative samples taken in accordance with standard DEA policy and procedures.

82. Furthermore, I believe that there is probable cause that VILIAMI MOSESE FATUKALA, QUYNHMY QUOC YAMAMOTO, and IRIS JUNE MICU MINA committed those same crimes, thus supporting the legal basis for the Court to issue arrest warrants based on a criminal complaint.

I swear, under the penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information, and belief.

Jason Chin
Special Agent
Drug Enforcement Administration

Sworn and Subscribed to me on December 17, 2019

The Honorable Deborah Barnes
United States Magistrate Judge

Approved as to form:

Paul Hemesath
Assistant U.S. Attorney

ATTACHMENT A-1

LOCATION TO BE SEARCHED

902 33rd Street, Sacramento, California (TARGET PROPERTY #1)

A single family residential property with a light colored exterior. The address numbers "902" are affixed to the front exterior of the house to the north of front door area. The property is located on the west side of 33rd Street. The property to be searched is depicted in the photograph below.

The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on TARGET PROPERTY #1; any computer, digital devices, and digital media located therein, where the items specified in Attachment B may be found; all vehicles located at TARGET PROPERTY #1 which fall under the dominion and control of FATUKALA, MINA, YAMAMOTO, PACHECO, TOPUI, and CHEN; and all internal and external compartments and all containers that may be associated with the storage of controlled substances or the proceeds of the sales of controlled substances or their instrumentalities contained within the aforementioned places or vehicles.

ATTACHMENT A-2

LOCATION TO BE SEARCHED

7891 Iona Way, Sacramento, California (TARGET PROPERTY #2)

A single family residential property with a white colored exterior and peach colored trim. The address numbers "7891" are affixed to the front exterior of the house to the north of the garage door. The property is located on the east side of Iona Way. The property to be searched is depicted in the photograph below.

The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on TARGET PROPERTY #2; any computer, digital devices, and digital media located therein, where the items specified in Attachment B may be found; all vehicles located at TARGET PROPERTY #2 which fall under the dominion and control of FATUKALA, MINA, YAMAMOTO, PACHECO, TOPUI, and CHEN; and all internal and external compartments and all containers that may be associated with the storage of controlled substances or the proceeds of the sales of controlled substances or their instrumentalities contained within the aforementioned places or vehicles.

ATTACHMENT A-3

LOCATION TO BE SEARCHED

8804 Lemas Road, Sacramento, California (TARGET PROPERTY #3)

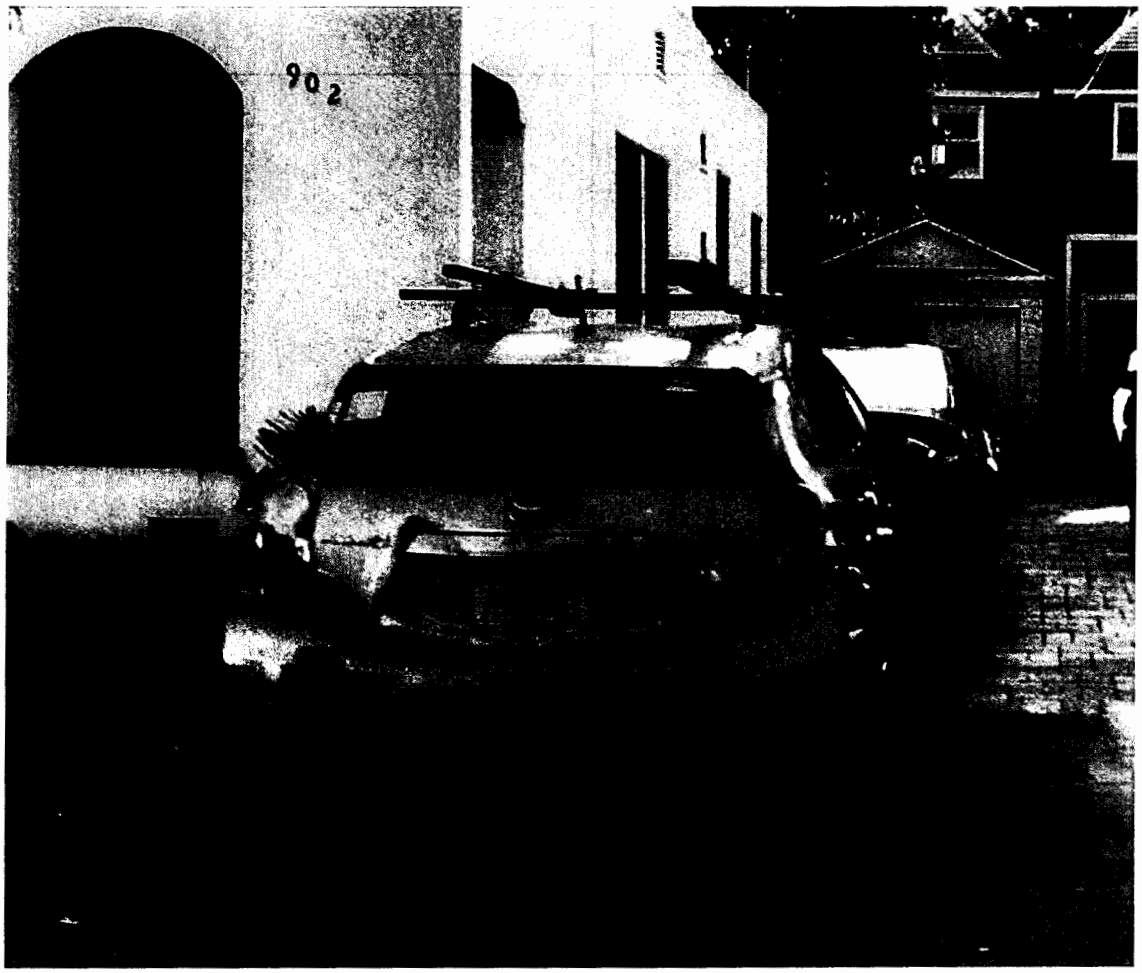
A single family residential property with a pink colored exterior and light brown colored trim. The address numbers "8804" are affixed to the front exterior of the house to the east of the garage door. The property is located on the south side of Lemas Road. The property to be searched is depicted in the photograph below.

The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on TARGET PROPERTY #3; any computer, digital devices, and digital media located therein, where the items specified in Attachment B may be found; all vehicles located at TARGET PROPERTY #3 which fall under the dominion and control of FATUKALA, MINA, YAMAMOTO, PACHECO, TOPUI, and CHEN; and all internal and external compartments and all containers that may be associated with the storage of controlled substances or the proceeds of the sales of controlled substances or their instrumentalities contained within the aforementioned places or vehicles.

ATTACHMENT A-4

LOCATION TO BE SEARCHED

FATUKALA VEHICLE – Toyota Prius bearing California license plate number 7DBA021 and Vehicle Identification Number ("VIN") JTDKDTB39D1052068 registered to Liliani Fatukala.

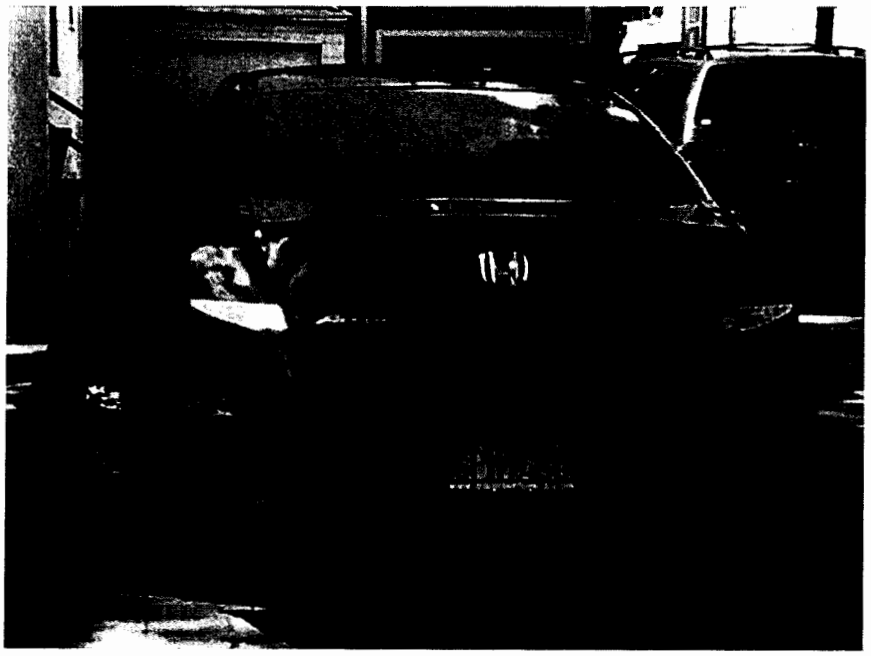


The search of the FATUKALA VEHICLE is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.

ATTACHMENT A-5

LOCATION TO BE SEARCHED

YAMAMOTO VEHICLE – Honda Accord bearing California license plate number 6PMY435 and Vehicle Identification Number ("VIN") 1HGCS1B80BA003561 registered to Bao T. Nguyen.



The search of the YAMAMOTO VEHICLE is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.

ATTACHMENT A-6

LOCATION TO BE SEARCHED

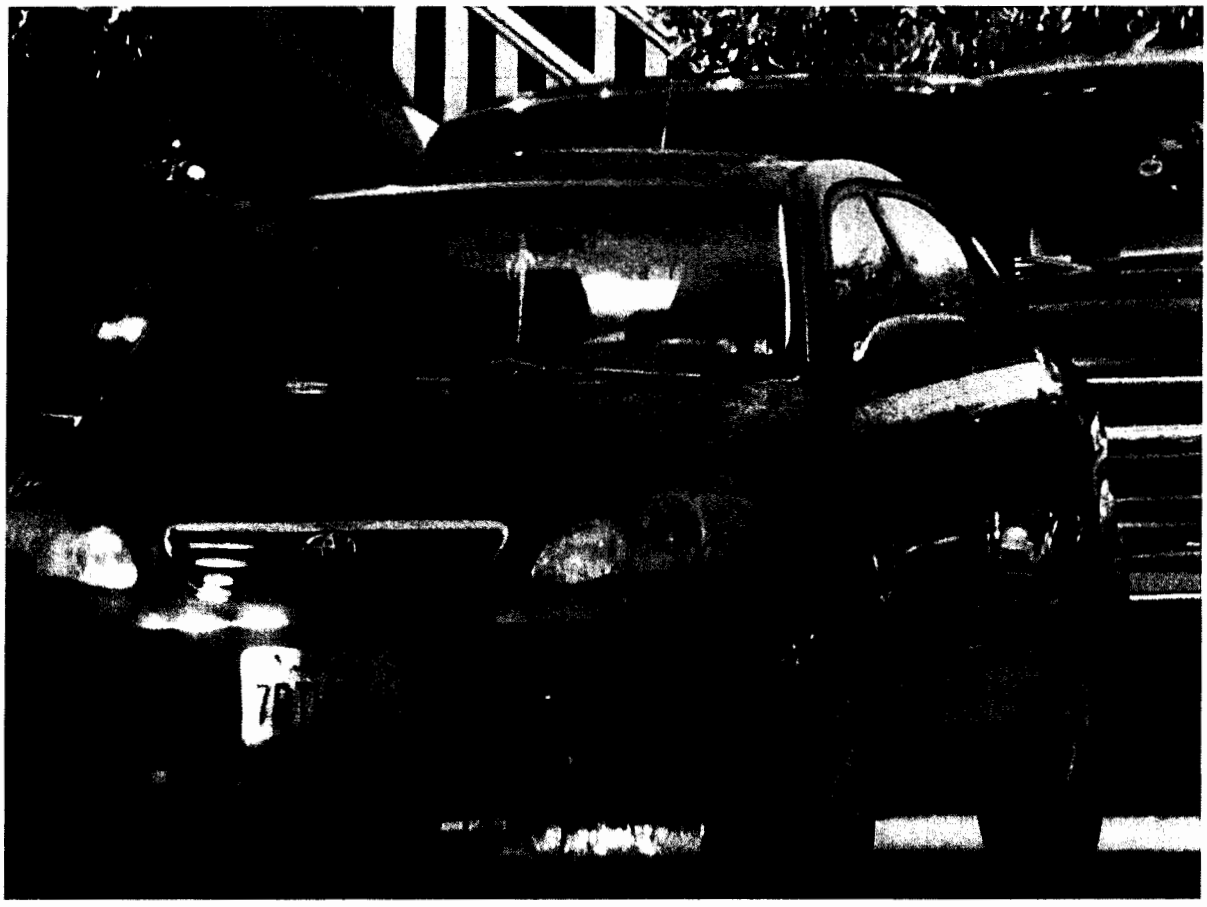
MINA VEHICLE – Subaru Outback bearing California license plate number 6ZLB767 and Vehicle Identification Number ("VIN") 4S4BRBGC8D3271950 registered to Iris MINA.

The search of the MINA VEHICLE is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.

ATTACHMENT A-7

LOCATION TO BE SEARCHED

PACHECO VEHICLE – a Toyota Corolla bearing California license plate number 7RTH204 and Vehicle Identification Number ("VIN") 2T1BR30E25C550275 registered to Nicole Marie PACHECO.



The search of the PACHECO VEHICLE is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.

ATTACHMENT A-8

LOCATION TO BE SEARCHED

CHEN VEHICLE – a Toyota Camry bearing California license plate number 7CWS281 and Vehicle Identification Number ("VIN") 4T1BF1FK8EU313038 registered to Mai Xian Chen.

The search of the CHEN VEHICLE is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as computers, hard drives, flash drives, tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute or contain evidence, instrumentalities, or fruits of violations of 21 U.S.C. §§ 841, 846 (Conspiracy to Distribute and to Possess with Intent to Distribute a Controlled Substance).

1. All records relating to the violations described above, including:

a. any and all documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of controlled substances;

b. any and all documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of packaging materials;

c. any and all documents, records or information relating to the purchase, sale, tracking, delivery or distribution of postage or express mail consignment;

d. any and all documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;

e. any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;

f. any and all documents, records, or information relating to email accounts used in furtherance of these offenses;

g. any and all records or other items which are evidence of ownership or use of computer equipment, including, but not limited to, sales receipts, bills for internet access, handwritten notes and handwritten notes in computer manuals.

h. any and all records relating to indicia of occupancy, residency, and ownership or use of the TARGET PROPERTIES and TARGET VEHICLES, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents, and keys;

i. any and all records of any address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices and the memory thereof, and any papers, records or electronic data reflecting names, addresses, telephone numbers, pager numbers of co-conspirators, sources of controlled substances and/or virtual currency, identifying information for customers purchasing controlled substances and/or virtual currency;

j. all bank records, checks, credit card bills, account information, safe deposit box information and other financial records;

k. all copies of income tax returns filed with the Internal Revenue Service (IRS) or the California Franchise Tax Board;

l. all records related to the purchase of real estate or other assets, or the leasing of storage units,

m. financial records for including foreign and domestic banking records, ledger books, wire transfer instructions, and receipts for wire transfers,

n. bulk cash in excess of $2,000.

2. Any digital devices or other electronic storage media and/or their components used as a means to commit the violations described above, including:

a. any digital device or other electronic storage media capable of being used to commit, further, or store evidence or fruits of the offenses listed above;

b. any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. any passwords, password files, seed words, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, seed words, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:

a. routers, modems, and network equipment used to connect computers to the internet;

b. records of Internet Protocol addresses used;

c. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

5. Any and all hidden services accounts or encrypted chat applications used in furtherance of the offenses described above, including, but not limited to, darknet market accounts, associated darknet forum accounts, Tor-based email accounts, and Wickr handles and logins.

6. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above, including, but not limited to, localbitcoins.com accounts or bitcoin-otc internet relay chat channel accounts.

7. Virtual currency in any format, including but not limited to, wallets (digital and paper), seed words, usernames and passwords, public keys (addresses) and private keys.

8. Fiat currency (U.S. dollars or other government issued currency).

9. Keys to storage units, suites, lockers and safe deposit boxes.

10. Firearms or other prohibited weapons that are not registered to VILIAMI MOSESE FATUKALA, QUYNHMY QUOC YAMAMOTO, IRIS JUNE MICU MINA, SEMISI TOPUI, NICOLE MARIE PACHECO and LISA CHEN or any of their cohabitants.

11. Controlled substances, associated paraphernalia and/or contraband, and any equipment or devices used in the manufacturing, storage and processing of controlled substances.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIME.

SEARCH PROCEDURE FOR DIGITAL DEVICES

12. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government

may retain the digital device and any forensic copies of the digital device but may not access data falling outside the scope of the other items to be seized absent further court order.

g. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

h. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

i. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

ii. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

iii. Any magnetic, electronic, or optical storage device capable of storing digital data;

iv. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

v. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

vi. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

vii. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

viii. Agents shall attempt to determine, in good faith, the ownership and/or control of electronic devices subject to seizure—if agents determine that a device does not fall under the ownership or control of one of the individuals identified in the underlying affidavit (e.g., the devices is clearly under the ownership and control of another person in the subject

property), then the agent shall exercise reasonable discretion whether or not to seize the device, subject to the restrictions of this Attachment B.

ix. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

United States District Court

EASTERN District of **CALIFORNIA**

In the Matter of the Seizure of

(Name, address or brief description of person, property or premises to be seized)

All funds maintained at Bank of America Account XXXX-XXXX-4003 held in the name of Lisa Chen Sole Prop DBA Chen Corner,

SEIZURE WARRANT

CASE NUMBER:

2:19 SW 1155 DB

TO, Jason Chin, Special Agent, DEA and any Authorized Officer of the United States

Affidavit(s) having been made before me by Jason Chin, Special Agent, DEA who has reason to believe
Affiant

in the **EASTERN** District of **CALIFORNIA** there is now certain property which is subject to forfeiture to the United States, namely (describe the property to be seized)

All funds maintained at Bank of America Account XXXX-XXXX-4003 held in the name of Lisa Chen Sole Prop DBA Chen Corner,

Which is subject to seizure pursuant to 21 U.S.C. § 881(b) incorporating 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 21 U.S.C § 881(a)(6).

I am satisfied that the affidavit(s) and any record testimony establish probable cause to believe that the property so described is subject to seizure and that grounds exist for the issuance of this seizure warrant.

YOU ARE HEREBY COMMANDED to seize within 14 days the property specified, serving this warrant and making the seizure in the daytime — 6:00 AM to 10:00 P.M., leaving a copy of this warrant and receipt for the property seized, and prepare a written inventory of the property seized and promptly return this warrant to DEBORAH BARNES or Any U.S. Magistrate in the Eastern District of California as required by law.
U.S. Judge or Magistrate

12-17-19 @ 9:46am at Sacramento, California
Date and Time Issued City and State

Deborah Barnes, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer