AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

LODGED
CLERK, U.S. DISTRICT COURT
9/8/2023
CENTRAL DISTRICT OF CALIFORNIA
BY: JB DEPUTY

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
9/8/23
CENTRAL DISTRICT OF CALIFORNIA
BY: nne DEPUTY

United States of America

v.

SAMVEL GRIGORYAN, and
HAYK MARTIROSYAN,

Defendant(s)

Case No. 2:23-mj-04608-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

Beginning on or about a date unknown and continuing to on or about September 8, 2023, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 371, 1960	Conspiracy to Operate an Unlicensed Money Transmitting Business

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Austin Anderson
Complainant's signature

Austin Anderson, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: Septembe 8, 2023

Judge's signature

City and state: Los Angeles, California

Hon. Maria A. Audero, U.S. Magistrate Judge
Printed name and title

AUSA: J. Mark Childs x2433

AFFIDAVIT

I, Austin Anderson, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against Samvel GRIGORYAN ("GRIGORYAN") and Hayk MARTIROSYAN ("MARTIROSYAN") for violation of 18 U.S.C. §§ 371, 1960 (Conspiracy to Operate an Unlicensed Money Transmitting Business) (the "SUBJECT OFFENSES").

2. In addition, this affidavit is made in support of applications to search the following:

a. The person of GRIGORYAN, as described more fully in Attachment A-1;

b. The person of MARTIROSYAN, as described more fully in attachment A-2;

c. 1041 Elm Avenue, in Glendale, California, as described more fully in Attachment A-3 ("**SUBJECT PREMISES 1**");

d. 416 West Wilson Avenue, in Glendale, California, as described more fully in Attachment A-4 ("**SUBJECT PREMISES 2**")(collectively, **SUBJECT PREMISES 1** and **SUBJECT PREMISES 2** are referred to herein as "**SUBJECT PREMISES**").

e. A white Mercedes-Benz sedan bearing California license plate "8YBF750", with a vehicle identification number ("VIN") W1K6G7GB8MA041973, as described more fully in Attachment A-5 ("**SUBJECT VEHICLE 1**").

f. A black Mercedes-Benz sedan bearing California license plate "LIMO8", with VIN W1KEG2BB8PF014575, as described

more fully in Attachment A-6 ("**SUBJECT VEHICLE 2**")(collectively, **SUBJECT VEHICLE 1** and **SUBJECT VEHICLE 2** are referred to herein as "**SUBJECT VEHICLES**").

3. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1960 (Operating an Unlicensed Money Transmitting Business) and 18 U.S.C. §§ 371, 1960 (Conspiracy to Operate an Unlicensed Money Transmitting Business) (the "SUBJECT OFFENSES"), as described more fully in Attachment B. Attachments A-1 through A-6 and B are incorporated herein by reference.[1]

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses, as well as my conversations and analysis with more experienced agents and officers who are familiar with money laundering. This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest warrants and search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and

[1] The descriptions of the GRIGORYAN, MARTIROSYAN, **SUBJECT PREMISES** and the **SUBJECT VEHICLES** contained herein and in A-1 through A-6 are based on my own observations while conducting surveillance, my discussions with other officers and/or agents who conducted surveillance in this case, my review of reports about surveillance in this case, open source data base searches, records from government sources (e.g., CA DMV and Department of Homeland Security) and information provided by others during this investigation.

statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF SPECIAL AGENT AUSTIN ANDERSON

5. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since August 2021. As a requirement for employment as an FBI Special Agent, I successfully completed the New Agent Basic Field Training Course located at the FBI Training Academy in Quantico, Virginia. As a function of my assignment, I have received both formal and informal training from the FBI and other institutions regarding computer technology, financial investigations, cryptocurrency, and organized crime. I received Bachelor of Science Degrees in Accounting and Finance from the University of Utah. Before joining the FBI, I was employed as a staff accountant from October 2019 to May 2021.

6. As a Special Agent with the FBI, my job duties include the investigation of organized crime groups using advanced technology to conduct large scale computer-enabled and computer-facilitated crime, including violations of the SUBJECT OFFENSES.

7. I have conducted and participated in several criminal investigations for violations of federal and state laws including, but not limited to, financial crimes, computer-based financial crimes, money laundering, fraud and other organized criminal activity. I have prepared, executed, and assisted in numerous search and arrest warrants. I have also conducted and participated in criminal and administrative interviews of witnesses and suspects. I am familiar with the formal methods

of money laundering investigations, including, but not limited to, electronic surveillance, visual surveillance, general questioning of witnesses, search warrants, confidential informants, and analysis of financial records.

III. SUMMARY OF PROBABLE CAUSE

8. Samvel GRIGORYAN, with the assistance of co-conspirator Hayk MARTIROSYAN, is known to operate an unlicensed money service business named "Coinexchange.am", which provides cash-for-cryptocurrency exchange services in the Los Angeles area. Because this business is not registered with the United States Treasury Financial Crimes Enforcement Network ("FinCEN"), discussed below, and does not comply with the mandatory reporting requirements for money service businesses, it attracts customers interested in evading federal anti-money laundering ("AML") regulations, such as Know Your Customer ("KYC") identity verification, and obfuscating the movement of funds by preserving the anonymity of the transacting parties.[2] Over three separate occasions in August and September 2023, an FBI confidential human source ("CHS") gave GRIGORYAN and MARTIROSYAN more than $140,000 in U.S. currency in exchange for cryptocurrency. Neither GRIGORYAN nor MARTIROSYAN ever asked the CHS for identification and never reported the transactions to FinCEN as required.

---

[2] FinCEN is a bureau within the U.S. Treasury Department. The mission of FinCEN, among other things, is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

9. To date, no licensed business or corporation has been discovered relating to either GRIGORYAN or MARTIROSYAN. According to a FinCEN database, no currency transaction reports were ever filed pertaining to the transactions conducted by GRIGORYAN and the CHS. As explained below, neither GRIGORYAN nor MARTIROSYAN are licensed or registered as money services businesses with FinCEN, as required by federal statute, discussed herein. As such, based on this investigation discussed below, GRIGORYAN, along with the assistance of MARTIROSYAN, is running an unlicensed money transmitting service in violation of 18 U.S.C. § 1960.

10. There is probable cause to believe that evidence of the Subject Offenses will be located in the **SUBJECT PREMISES** and the **SUBJECT VEHICLES**. Investigating agents have observed on multiple occasions, as set forth below, GRIGORYAN and MARTIROSYAN utilizing the **SUBJECT VEHICLES** in activities directly related to exchange transactions, to include holding meetings about the cash-for-cryptocurrency scheme with a client and counting cash inside the **SUBJECT VEHICLES**. As discussed below, agents have also observed cash being taken directly from a cash-for-cryptocurrency transaction to each of the **SUBJECT PREMISES**.

IV. BACKGROUND ON VIRTUAL CURRENCY

11. Virtual currency (also known as cryptocurrency or digital 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). Virtual

currency exists entirely on the Internet and is not stored in any physical form. Virtual 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. Virtual currency is not illegal in the United States and may be used for legitimate financial transactions. However, virtual currency is often used for conducting illegal transactions, such as the sale of controlled substances or the laundering or concealment of funds.

12. Bitcoin is a type of virtual currency. Bitcoin payments are recorded on 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.

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

14. Bitcoins are 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.

15. Individuals who possess cryptocurrency as a result of illicit activity often need to convert it to fiat (government-backed) currency. Such purchases and sales are often facilitated by peer-to-peer Bitcoin exchangers who are not registered with the federal or a state government and who advertise their services on websites designed to facilitate such transactions. These unregistered exchangers often charge a higher transaction fee than legitimate, registered virtual currency exchangers. This higher fee is essentially a premium that the unregistered exchangers charge in return for not filing reports on the exchanges pursuant to the Bank Secrecy Act, such as Currency Transaction Reports and Suspicious Activity Reports, as discussed below.[3]

16. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," stored on the peer-to-peer network on which the Bitcoin system operates. The Blockchain serves to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and, therefore,

---

[3] The Bank Secrecy Act ("BSA"), 31 U.S.C. Section 5311 et seq, establishes program, recordkeeping and reporting requirements for money transmitting businesses, national banks, federal savings associations, federal branches and agencies of foreign banks. The BSA was amended to incorporate the provisions of the USA PATRIOT Act which requires financial institutions to adopt a customer identification program as part of its BSA compliance program.

cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each wallet involved in a set of transactions is it possible to meaningfully trace funds through the system.

17. Bitcoin is one example of a virtual currency; other digital currencies, such as Tether ("USDT"), Tron, Etherium, and Monero also exist. The technology underlying these currencies are similar, though some of these currencies provide more privacy and anonymity to the users.

18. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they can be located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper

wallets contain an address and a QR code[4] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

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

---

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

Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

V. BACKGROUND REGARDING REGULATIONS GOVERNING VIRTUAL CURRENCY MONEY TRANSMITTAL

20. Based on my training and experience as well as information provided by others, I am aware of the following:

a. The Bank Secrecy Act ("BSA") is codified at 31 U.S.C. §§ 5313-5326. These laws were enacted by Congress to combat the use of financial institutions to launder the proceeds of crime. Title 31 U.S.C. § 310 establishes FinCEN as a bureau within the U.S. Treasury Department, and describes FinCEN's powers and duties to, among other things, to enforce compliance with the BSA.

b. The definition of a financial institution under the statute, 31 U.S.C. § 5312(a)(2)(R), includes "a licensed sender of money or any other person who engages as a business in the transmission of funds[.]" Under the relevant federal regulations, financial institutions are also defined as "money servicing businesses," ("MSBs") which include "money

transmitters." See 31 C.F.R. § 1010.100(t)(3) (defining "financial institution" as a "money servicing business"); 31 C.F.R. § 1010.100(ff)(5) (defining money transmitters as money services businesses).

c. In 2013, FinCEN issued guidance that a money transmitter can include an individual who offers exchange services between virtual currency[5] and fiat currency. See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, issued March 18, 2013 (the "FinCEN Guidance"). This guidance was reaffirmed in May 2019. The FinCEN Guidance articulated that those who are money transmitters because they offer exchange services between virtual currency and fiat currency are also MSBs and must comply with the applicable portions of the BSA, some of which are described below.

d. Financial institutions, including MSBs and money transmitters, are required to report each deposit, withdrawal, exchange of currency, or other payment or transfer involving more than $10,000 in currency. See 31 C.F.R. §§ 1022.300, 1022.310, 1022.311, and 1022.312 (cross-referencing 31 C.F.R. §§ 1010.300, 1010.310, and 1010.311, and 1010.312); see also 31 U.S.C. § 5313(a). These reports are referred to as Currency Transaction Reports ("CTRs"). A "transaction" for purpose of filing a CTR includes "multiple currency transactions . . . if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out

[5] A brief background on virtual currency is described above.

totaling more than $10,000 during any one business day." 31 C.F.R. § 1010.313. CTRs must be filed within 15 days following the day on which the reportable transactions occurred. See 31 C.F.R. § 1010.306(a)(1). Financial institutions must verify and record the name and address of the individual who conducted the reportable transactions, and must accurately record the identity, social security number, or taxpayer identification number of any person or entity on whose behalf the reportable transaction was conducted. See 31 C.F.R. § 1010.312. CTRs are filed with FinCEN and are made available to law enforcement. It is a federal crime under Title 31 for an MSB or money transmitter to fail to file a CTR. See 31 U.S.C. §§ 5313(a) and 5322.

e. In addition to being required to file CTRs, certain MSBs, including money transmitters, are required to file suspicious activity reports ("SARs"). See 31 C.F.R. §§ 1022.320 (stating at sub-section (a)(1) that money transmitters are a type of MSB required to file SARs). SARs must be filed on transactions aggregating to at least $2,000 in value and the MSB knows or has reason to suspect: (1) the funds are derived from illegal activity or are intended to hide or disguise funds or assets derived from illegal activity to violate or evade any federal law or regulation; (2) the transaction is designed to evade the Title 31 reporting requirements; (3) the transaction services no apparent business or lawful purpose, and there is no other reasonable explanation for the transaction; and (4) the transaction involves use of the money transmitter to facilitate

criminal activity. See 31 C.F.R. §§ 1022.320(a)(2)(i)-(iv). MSBs are required to file a SAR within 30 calendar days after the date of the initial detection of the underlying facts that warrant the filing of a SAR. See 31 C.F.R. §§ 1022.320(b)(3). Lastly, MSBs are required to maintain supporting documentation for the SAR for a period of five years from the date of filing the SAR. See 31 C.F.R. §§ 1022.320(c). It is a federal crime under Title 31 for a money transmitter to fail to file a SAR. See 31 U.S.C. §§ 5318(g) and 5322.

f. Financial institutions, including MSBs and money transmitters, are required to create and maintain effective anti-money laundering compliance programs. See 31 U.S.C. § 5318(h)(1); see also 31 C.F.R. § 1010.210. The program must have written policies, procedures, and controls governing the verification of customer identification, the filing of reports such as CTRs, the creation and retention of records, responses to law enforcement requests, and other compliance with BSA requirements. The anti-money laundering compliance program must have a compliance officer who is responsible for assuring that the business complies with all BSA requirements. It is a federal crime under Title 31 for an MSB or money transmitter to fail to maintain an effective anti-money laundering compliance program. See 31 U.S.C. §§ 5318(h)(1) and 5322.

g. Any person who owns or controls an MSB is responsible for registering, and periodically re-registering, the business with FinCEN. See, 31 U.S.C. § 5330(a); see also 31 C.F.R. § 1022.380. Registration must be done on or before the

end of the 180-day period beginning on the day following the date the business was established. See, 31 C.F.R. § 1022.380(b)(3). A money transmitting business that fails to register with FinCEN is subject to criminal liability under 18 U.S.C. § 1960. Specifically, § 1960 makes criminally liable anyone who "knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business." That includes, under 18 U.S.C. § 1960(b)(1)(B), a business that "fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section[.]"[6]

---

[6] Unlicensed money remitting is prohibited by statute at 18 U.S.C. § 1960, which provides:

(a) Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

The statute includes the following:

(1) the term "unlicensed money transmitting business" means a money transmitting business which affects interstate or foreign commerce in any manner or degree and—

(A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable;

(B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or

(C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity;

(2) the term "money transmitting" includes transferring funds on behalf of the public by any and all means including but

(footnote cont'd on next page)

h. Additionally, even if a money transmitter is registered with FinCEN, 18 U.S.C. § 1960(b)(1)(C) also criminalizes money transmitting businesses that "involve . . . the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."

21. In the scheme described below, GRIGORYAN and MARTIROSYAN are engaged in unlicensed money transmitting business, in that they are exchanging cryptocurrency for funds in the form of United States currency, charging a fee as a percentage of the amount of the transfer. Neither GRIGORYAN or MARTIROSYAN are licensed or registered as money services businesses with FinCEN, as required by federal statute.

VI. STATEMENT OF PROBABLE CAUSE

22. The Federal Bureau of Investigation ("FBI"), Drug Enforcement Administration ("DEA"), Internal Revenue Service ("IRS"), United States Postal Inspection Service ("USPIS"), Homeland Security Investigations ("HSI"), and other law enforcement agencies are investigating the money laundering operation ("MLO") associated with Samvel GRIGORYAN and Hayk MARTIROSYAN, which – as an organization – engages in cash-for-cryptocurrency monetary exchanges utilizing the business name "coinexchange.am".

---

not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier; . . . .

A. Identification of GRIGORYAN and MARTIROSYAN

23. In or about December 2021, GRIGORYAN, a citizen of Armenia, attempted to cross the United States border from Mexico into San Ysidro, California using a false American passport. Upon being denied entry into the United States, GRIGORYAN and his family claimed asylum from Armenia to U.S. immigration officials and were subsequently paroled into the United States. Upon entry, GRIGORYAN provided immigration authorities with **SUBJECT PREMISES 2** as his contact address.

24. In or about March 2023, Hayk MARTIROSYAN, a citizen of Armenia, crossed the San Ysidro port of entry into the United States, claimed asylum from Armenia to U.S. immigration officials, and was paroled into the United States. MARTIROSYAN also provided **SUBJECT PREMISES 2** as his contact address.

B. Identification of Coinexchange.am

25. GRIGORYAN, MARTIROSYAN and co-conspirators, known and unknown to the investigation, are associated with an established Armenian website offering the exchange of fiat currency (e.g., United States currency) for cryptocurrency. The website URL is "CoinExchange.AM", and is available to read in Armenian, English, and Russian. The home page states the "company has been trading in cryptocurrencies since 2014." Additionally, the home page of the site states the business operates "offices abroad Los Angeles Dubai: Iran: Georgia [sic]." The phone number +374 96 14 44 44 ("Subject Phone Number") is listed on the top right of the website. It is listed three times along the banner,

adjacent to icons for the Apple phone, Viber, and WhatsApp applications.

a. I conducted additional open source research on the social media platforms, including, Instagram and Tik Tok, and found social media accounts advertising cryptocurrency exchange services under the name "coinexchange.am". Both pages on Instagram and Tik Tok displayed videos promoting cryptocurrency exchange services, one of which displayed a billboard in what appeared to be a train station with the company website on it, "Coinexchange.am". Both the Instagram and Tik Tok accounts listed the Subject Phone Number as contact information in the bio section. Furthermore, on the Instagram account which contained the advertisement for coinexchange.am, the first post was published in August 2020.

C. Coinexchange.am not licensed with FinCEN

26. To date, no licensed business or corporation has been discovered relating to either GRIGORYAN or MARTIROSYAN, or to the **SUBJECT PREMISES**. According to a FinCEN transaction report database, no currency transaction reports were ever filed pertaining to the below transactions. Additionally, I queried the FinCEN Money Service Business ("MSB") database[7] in or about September 2023 which yielded negative results for GIRGORYAN, MARTIROSYAN, and coinexchange.am.

[7] The FinCEN MSB database allows users to query a list of licensed MSB's using individual names, Doing Business As ("DBA") names, or addresses, among other criteria for the purpose of determining whether or not said criteria are related to any licensed MSBs.

D. August 24, 2023 CHS Exchange

27. On August 21, 2023, at the direction of FBI Special Agents, an FBI Confidential Human Source ("CHS")[8] contacted the Subject Phone Number listed on coinexchange.am via WhatsApp messages and voice chat, and spoke to an individual later identified as GRIGORYAN. This communication was preserved and recorded, and I have reviewed it and it contains GRIGORYAN's voice as I am familiar with it as a result of this investigation. The recorded communications between GRIGORYAN and CHS were conducted in the English language (CHS does not speak Armenian). During the initial conversation on August 21, 2023, CHS informed GRIGORYAN that CHS found GRIGORYAN's contact information on the Coinexchange.am Instagram page. During this conversation, CHS inquired if GRIGORYAN could conduct a cash for cryptocurrency exchange, specifically, U.S. currency for Bitcoin ("BTC"). During this first recorded conversation, GRIGORYAN agreed to an exchange of $40,000 U.S. currency for BTC, plus a 5% commission rate, and requested to meet CHS in Glendale, CA, on Thursday August 24, 2023.[9]

---

[8] The CHS recently pleaded guilty to a violation of 21 U.S.C. § 841(a)(1) (Distribution of Methamphetamine) and is cooperating with the government in the interest of obtaining sentencing consideration. The CHS does not have any other prior convictions. Agents have corroborated the information provided by the CHS to the extent possible and believe the CHS to be credible to the extent the CHS's information is corroborated. Additionally, the CHS has received occasional meals purchased by the FBI during meetings between handling agents and the CHS.

[9] After this initial interaction between CHS and GRIGORYAN, I later viewed the WhatsApp messages between them and preserved the communications.

28. During the morning of August 24, 2023, GRIGORYAN communicated to CHS via WhatsApp text messages that the cash for BTC exchange would take place that day at 1 p.m. in the vicinity of Pelanconi Park, located in Glendale, California.

29. On August 24, 2023, investigators with DEA and FBI established surveillance at Pelanconi Park, located in Glendale, per GRIGORYAN's instructions, in anticipation of the meeting between GRIGORYAN and CHS. Prior to the meeting, investigators provided CHS with $42,000 in U.S. currency contained in a brown plastic bag. Investigators outfitted CHS with an audio recording device and a transmitter so that investigators could listen to the communications between CHS and GRIGORYAN real-time as they were occurring. I heard the transmitted conversations real-time on August 24, 2023 and I have read the transcript of this meeting. On August 24, 2023, at approximately 1:20 pm, investigators observed the initial meet and introduction between the CHS, GRIGORYAN, and another unknown male (UM #1) in front of (outside of) Pelanconi Park.

30. At approximately 1:27 pm, in front of Pelanconi Park, CHS, who was carrying the bag of cash, and GRIGORYAN entered **SUBJECT VEHICLE 1**. UM #1 did not enter **SUBJECT VEHICLE 1** and remained outside of the park, smoking a cigarette.

a. During the recorded meeting on August 24, 2023, CHS gave the $42,000 in U.S. currency to GRIGORYAN, who counted the cash in **SUBJECT VEHICLE 1**. GRIGORYAN told CHS that he would send the BTC to CHS. Shortly thereafter, the FBI controlled Bitcoin wallet furnished to the CHS received approximately

1.5329 Bitcoin (BTC) in exchange for the $40,000 USD. At the time, 1.5329 BTC was worth, approximately, $40,000 USD. The remaining $2,000 USD provided to GRIGORYAN was a 5% transaction fee.

b. During this meeting, GRIGORYAN made comments that demonstrated he regularly conducted cash-for-cryptocurrency transactions. For instance, GRIGORYAN showed CHS his cell phone which displayed a cryptocurrency application that detailed a series of recent transactions GRIGORYAN had conducted with his cryptocurrency wallet. According to the CHS, GRIGORYAN had conducted several cryptocurrency transactions totaling between $40,000 and $300,000 within the previous two days, the implication being that GRIGORYAN has a ready supply of cryptocurrency to exchange for high-volumes of USD. GRIGORYAN stated that he conducted cryptocurrency transactions around the world, to include the United States, Russia, and Europe. GRIGORYAN stated he had recently conducted four cryptocurrency transactions that totaled one million USD.

c. When GRIGORYAN asked about the nature of CHS's business, CHS stated "I'll tell you next time." CHS indicated their business was buying something from China to bring to the United States. GRIGORYAN stated that he had "more friends who want dollar in China", and implied that he was interested in conducting additional business with CHS in the future. GRIGORYAN also advised CHS to use the cryptocurrency United

States Dollar Tether (USDT) instead of BTC as it was more convenient for transferring money overseas.[10]

d. Upon completing the cash for cryptocurrency exchange, GRIGORYAN indicated the CHS had good reason to trust him, as exchanging was his business and how he provided for his children. GRIGORYAN stated "Trust me, don't worry . . . it's my business. I have kids, you understand? … If I lie, I can't help . . ." Based on the context of the entire conversation, GRIGORYAN was attempting to gain CHS's trust for future cryptocurrency transaction by inferring to CHS that cryptocurrency transactions are GRIGOYAN's main source of revenue.

e. At approximately 1:30 pm, the investigative team observed GRIGORYAN handing the aforementioned brown plastic bag containing $42,000 from inside **SUBJECT VEHICLE 1** to UM #1, who took the bag and entered a white Kia sedan, CA license plate 9CBX945 (white Kia), registered at **SUBJECT PREMISES 2**.[11] UM #1 drove away alone from Pelanconi Park in the white Kia and,

---

[10] Based on my training and experience, USDT is often used in illicit transactions as it is widely considered less volatile than other cryptocurrencies. As such, it can be a preferred method of transferring cryptocurrency funds that would otherwise be difficult to execute, such as transactions across borders or transactions that would typically be subject to anti-money laundering regulations.

[11] Per records from the CA Department of Motor Vehicles ("CA DMV"), **SUBJECT VEHICLE 1** is registered to Lessee Dealmakers Group Inc./Aram Markaryan at location 6627 Colbath Ave, Van Nuys CA 91405. Per records from the CA DMV, **SUBJECT VEHICLE 2** is registered to Arpine Dadrian or Tigran Petrosyan, address 1229 Viola Avenue 7, Glendale, CA. Per records from CA DMV, the White Kia sedan is registered to Galina Zargaryan (believed to be GRIGORYAN's mother), at address 416 W. Wilson Avenue, Apt D, Glendale CA (**SUBJECT PREMESIS 2**).

approximately, five minutes later was observed by a law enforcement agent pulling into the driveway at **SUBJECT PREMISES 1**. During this same time period, GRIGORYAN and CHS walked into Pelanconi Park.

f. At approximately 1:35 pm, **SUBJECT VEHICLE 2** was observed leaving the driveway of **SUBJECT PREMISES 1**, and a few minutes later **SUBJECT VEHICLE 2** arrived at Pelanconi Park with UM #1 driving and MARTIROSYAN travelling as a passenger in the vehicle. Thereafter, law enforcement agents observed MARTIROSYAN and UM #1 exit **SUBJECT VEHICLE 2** at Pelanconi Park, near GRIGORYAN and CHS, who were still in the park.

g. At approximately, 1:40 pm, law enforcement agents observed MARTIROSYAN, GRIGORYAN, CHS and UM #1 all meet-up in Pelanconi Park.

h. During the recorded meeting on August 24, 2023, CHS asked GRIGORYAN if he was available to conduct another cash for BTC exchange in the coming weeks, to which GRIGORYAN replied "For next time, uh, bro, for next time. Uh, You give all this brother or my, another brother. . . You give him, uh, dollar. I send. . . Okay, you give him dollar, he go. I send it. It's okay for you, we can work."

i. During the meeting between MARTIROSYAN, GRIGORYAN, CHS and UM #1, in Pelanconi Park, GRIGORYAN introduced MARTIROSYAN as his "brother" to the CHS, and indicated to CHS that CHS would be working with MARTIROSYAN in future cash-for-cryptocurrency deals. GRIGORYAN indicated, however, that CHS should continue to contact GRIGORYAN at the

Subject Phone Number in order set up the logistics in advance. GRIGORYAN stated "my another brother now come. You see him face. Okay? . . . For next time . . . You give him, if I . . . can't see you, you see him", referring to MARTIROSYAN. GRIGORYAN also indicated he had an office in Armenia and that he was well-known in the Armenian cryptocurrency exchange market, saying, "I have office in my country. . . every people who . . . selling or buying crypto know who I am."

31. At approximately 1:50 pm, the meeting between CHS, GRIGORYAN, MARTIROSYAN, and UM #1 concluded. CHS departed the meeting location and the rest of participants left. Approximately two minutes later, **SUBJECT VEHICLE 2**, with MARTIROSYAN and UM#1 in the vehicle, was observed by a law enforcement agent arriving at **SUBJECT PREMISES 1**.

32. At approximately 2:55 pm, surveillance units observed **SUBJECT VEHICLE 1** in the alleyway behind **SUBJECT PREMISES 2**. GRIGORYAN then exited the vehicle and walked into the unit closest to the alley at **SUBJECT PREMISES 2**.

E. August 28, 2023 CHS Exchange

33. On August 28, 2023, CHS contacted GRIGORYAN over a WhatsApp communication and arranged for another cash-for-crypto transaction. During this communication, according to the CHS, GRIGORYAN agreed to provide CHS with $60,000 worth of cryptocurrency in exchange for $60,000 USD currency with an additional transaction fee of 5% to be paid to GRIGORYAN, for a total amount of $63,000. According to CHS, during these communications, GRIGORIAN agreed with CHS to do the cash-for-

crypto transaction at 2:00 pm at Pelanconi park in Glendale, California.

a. Prior to the meeting between GRIGORYAN and CHS, FBI agents equipped the CHS with an audio recording device and transmitter, and counted the $63,000 USD before it was provided to the CHS.

34. At approximately 2:00 pm, law enforcement agents observed **SUBJECT VEHICLE 2** arrive at Pelanconi Park. Surveillance units observed MARTIROSYAN and GRIGORYAN exit the vehicle. Shortly thereafter, CHS arrived at Pelanconi Park and met with MARTIROSYAN and GRIGORYAN. CHS, MARTIROSYAN and GRIGORYAN then entered **SUBJECT VEHICLE 2**. CHS was seen entering **SUBJECT VEHICLE 2** holding a white pastry box containing the $63,000 previously provided to the CHS by agents. The cash was then counted in the car and the transaction commenced.

a. During this meeting CHS stated to MARTIROSYAN and GRIGORYAN, in summary, that the cash provided for the exchange was derived from proceeds of illicit drug transactions, which MARTIROSYAN and GRIGORYAN acknowledged during the transaction. At one point, after CHS described the drug dealing business, GRIGORYAN, in the presence of MARTIROSYAN and the CHS, asked "Your people, uh . . . ship here drugs?", to which the CHS replied "No, no, not here. Mexico." Later, in the conversation, CHS stated "so Mexico, they-they know how to make it 'cause right now, you can't do anything. It's just the chemical, but in Mexico, they make it into a pill and then the pill, they send over here. And then, once they send it, right, it's completely

. . . people buy it just like that. One deal, it's over. I get a whole bunch of cash and then, we have to send more money to China to buy the chemicals there." Subsequently, GRIGORYAN and MARTIROSYAN conversed in a foreign language (likely, Armenian), after which GRIGORYAN said to the CHS "Everything is good."[12]

b. At the conclusion of the transaction, the FBI controlled Bitcoin wallet furnished to the CHS received approximately 2.307 Bitcoin (the approximate value of $60,000 USD, at the time) in exchange for the $60,000 cash.

c. Once the transaction was completed, CHS exited **SUBJECT VEHICLE 2** empty-handed. Shortly thereafter, MARTIROSYAN and GRIGORYAN departed the area in **SUBJECT VEHICLE 2**. A law enforcement surveillance team followed **SUBJECT VEHICLE 2**, which was last observed in the vicinity of **SUBJECT PREMISES 2**.

F. September 6, 2023 CHS Exchange

35. On September 4, 2023, CHS contacted GRIGORYAN over a WhatsApp communication and arranged for another cash-for-crypto transaction. During these communications (text messaging was preserved), GRIGORYAN agreed to conduct a cash-for-crypto exchange in the amount of $40,000 to be executed on September 6, 2023, plus a fee of 5% to GRIGORYAN, for total amount of $42,000. GRIGORYAN agreed to conduct the cash-for-crypto on September 6, 2023 in Pelanconi Park in Glendale, California.

---

[12] At the conclusion of this discussion, CHS stated to GERGORIAN and MARTIROSYAN, "I mean, you know my business, I mean I-I don't wanna scare you, you know what I mean", to which GRIGORYAN replied, "I'm more scared than you."

36. Prior to the September 6, 2023 meeting, investigating agents supplied CHS with a brown paper bag containing $42,000 in cash and equipped the CHS with an audio recording device and a transmitter. The investigative team conducted surveillance of the meeting location in the park as well as **SUBJECT PREMISES 1** and **2**.

37. At approximately 2:00 pm, **SUBJECT VEHICLE 2** was observed departing **SUBJECT PREMISES 1**. At approximately 2:04 pm, **SUBJECT VEHICLE 2**, arrived at Pelanconi Park in Glendale. MARTIROSYAN was observed exiting the vehicle and walked to the park. MARTIROSYAN and GRIGORYAN met near a staircase near the baseball fields. MARTIROSYAN and GRIGORYAN subsequently walked to the east side of the park and met with CHS.

38. At approximately 2:06 pm, agents conducting surveillance observed, in the park, CHS hand the bag containing the $42,000 cash to MARTIROSYAN, who then walked back to **SUBJECT VEHICLE 2** and departed the park.

a. The investigative team, utilizing aerial surveillance, observed MARTIROSYAN drive **SUBJECT VEHICLE 2** directly to **SUBJECT PREMISES 1**. **SUBJECT VEHICLE 2** arrived at **SUBJECT PREMISES 1** at approximately 2:12 pm. Upon arrival at **SUBJECT PREMISES 1**, MARTIROSYAN exited **SUBJECT VEHICLE 2** and walked between the buildings in the rear of **SUBJECT PREMISES 1**, toward the entrance to the detached unit, as described in Attachment A-3. After approximately six (6) minutes, MARTIROSYAN was observed walking out of the space between the

two buildings of **SUBJECT PREMISES 1** and entered **SUBJECT VEHICLE 2.**

39. Meanwhile, after MARTIROYSAN departed the park, CHS and GRIGORYAN finished conducting the transaction in the park, in which GRIGORYAN charged 5% commission on an exchange of $40,000 cash for USDT cryptocurrency.

a. At the conclusion of the transaction, the FBI controlled USDT wallet furnished to the CHS received approximately 39,850 USDT in exchange for the $40,000 cash, roughly the value of 39,850 USDT at the time.

b. During the meeting, GRIGORYAN stated that all further business would likely be handled by MARTIROSYAN as GRIGORYAN planned to leave United States and return to Armenia on either September 10 or 12, 2023.

40. Based on conversations with an HSI agent, once an individual with a pending asylum status departs the United States, that individual would not typically be granted entry into the United States upon their return.

VII. TRAINING AND EXPERIENCE REGARDING EVIDENCE ASSOCIATED WITH MONEY LAUNDERING AND VIRTUAL CURRENCY

106. I know from my training and experience that unlicensed money transmitters, engaged in exchanging virtual currency for cash, and money launderers in general, also keep records of finances of their customers, including logs of transactions of money provided to them and money provided in exchange, and in some cases, the commission or fee earned for the transaction. Particularly in cases where these individuals engage in peer-to-

peer transactions (i.e., transactions on a customer-to-customer basis), exchangers and launderers keep records, either digitally or manually, of the volume of exchanges they have conducted. These exchangers may also retain information regarding their Bitcoin wallets, the Bitcoin wallets of their customers/clients, and other information regarding Bitcoin accounts. (This would apply to other virtual currencies as well.)

107. Individuals involved in virtual currency, including those who launder funds by using virtual currency, use a variety of digital devices, such as phones and computers. These individuals also use multiple digital devices in order to maintain anonymity and to compartmentalize communication, or use encrypted forms of communication in speaking with criminal associates. These digital devices are frequently carried on the person themselves.

68. Also, based on my experience and training and knowledge of virtual currency and money laundering, I am aware that unlicensed money transmitters also store wealth in other forms, such as gift cards (also known as cash cards), precious metals, or casino chips. Because launderers prefer to stay outside of the regulated banking and financial system (to avoid detection), these forms of wealth are other mediums to exchange and/or store money.

69. Money launderers who deal with significant amounts of cash and/or other illicit contraband also have more than one location where they store such contraband or records of contraband. I believe the **SUBJECT PREMISES 1 and 2** are such

locations based on funds from CHS transactions being taken directly to both locations.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[13]

70. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been

[13] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

71. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data

during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

72. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a

user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress GRIGORYAN's and MARTIROSYAN's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of GRIGORYAN's and MARTIROSYAN's faces with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

IX. CONCLUSION

73. For all of the reasons described above, there is probable cause to believe that GRIGORYAN and MARTIROSYAN have

committed a violation of 18 U.S.C. §§ 371, 1960 (Conspiracy to Operate an Unlicensed Money Transmitting Business) and there is probable cause to believe that GRIGORYAN has committed a violation of 18 U.S.C. § 1960 (Operating an Unlicensed Money Transmitting Business).

74. In addition, for all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES, will be found in a search of GRIGORYAN and MARTIROSYAN, and at **SUBJECT PREMISES 1** and **SUBJECT PREMISES 2**, as well as in **SUBJECT VEHICLE 1 and SUBJECT VEHICLE 2**, as described in Attachments A-1 through A-6.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 8th day of September, 2023.

THE HONORABLE MARIA A. AUDERO
UNITED STATES MAGISTRATE JUDGE