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

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

DAREN LI,

Defendant(s)

Case No. 2:24-mj-02055-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.

On or about the date(s) of June 8, 2022 to October 25, 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. § 1956(h)	Conspiracy to Commit Money Laundering

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Chris Saunders
Complainant's signature

Chris Saunders, Special Agent, U.S. Secret Service
Printed name and title

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

Date: April 8, 2024

Patricia Donahue
Judge's signature

City and state: Los Angeles, California

Hon. Patricia Donahue, U.S. Magistrate Judge
Printed name and title

AUSAs: Nisha Chandran (x2429) and Maxwell Coll (x1785)

AFFIDAVIT

I, Special Agent Chris Saunders, 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 **DAREN LI** ("**LI**") for conspiring to commit money laundering, in violation of Title 18, United States Code, Section 1956(h).

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

II. BACKGROUND OF AGENT

3. I am a Special Agent employed by the U.S. Secret Service ("USSS"). I have been employed as a Special Agent with the USSS since 2018, and I am currently assigned to the Criminal Investigative Division. Upon entering the USSS, I completed 18 weeks of basic training. This training covered various aspects of federal law enforcement, including instruction on the investigation of financial crime. I am a Certified Public Accountant ("CPA") and have investigated numerous individuals

for a wide variety of federal and state felony offenses, including wire fraud, bank fraud, computer fraud, and access device fraud. Furthermore, I have attended more than 120 hours of USSS training pertaining to computer investigations involving cyber and electronic crimes.

III. SUMMARY OF PROBABLE CAUSE

4. USSS is investigating an international money-laundering syndicate that launders the proceeds of fraud schemes, including cryptocurrency investment scams. Victims of the schemes under investigation were fraudulently induced into transferring millions of dollars to U.S. bank accounts opened in the names of dozens of shell companies whose sole apparent purpose was to facilitate the laundering of fraud proceeds. Many of these accounts and shell companies were located in the Central District of California. A network of money launderers then facilitated the transfer of those funds to other domestic and international bank accounts and cryptocurrency platforms in a manner designed to conceal the source, nature, ownership, and control of the funds.

5. USSS reviewed complaints from and conducted interviews of over 40 fraud scheme victims. Financial analysis of fraud victim payments identified approximately 74 different shell companies that were being used to launder proceeds of the fraud. The bank accounts for the shell companies received over $80 million in victim funds. Those funds in turn were transferred to two accounts held at a bank in the Bahamas ("Bahamas Account #1" and "Bahamas Account #2").

6. Bahamas Account #2 was opened by a Los Angeles-based individual ("Co-Conspirator 1"), with his business partner ("Co-Conspirator 2").[1] Based on my review of financial records, Bahamas Account #2 received more than $35 million that came from known fraudulent shell companies. Also from my review of records, I also know that after funds were received in Bahamas Account #2, they were converted to virtual currency and transferred to two virtual-currency addresses. One of those addresses was controlled by **LI** and was associated with an account held at the virtual-currency exchange Binance in **LI**'s name, and opened using his passport. **LI**'s Binance account received approximately $4.5 million in virtual currency that represented victim proceeds from known shell companies. After **LI** received those funds, he transferred the virtual-currency fraud proceeds to a second virtual-currency address days later, which was also known to have received millions of dollars in fraud-victim funds.

7. Based on my review of records and blockchain tracing, **LI** also temporarily provided Co-Conspirator 1 with almost $1 million in virtual currency in order to facilitate the opening of Bahamas Account #2, which was in turn used to transmit fraud proceeds to **LI**'s Binance account.

8. In connection with this investigation, in December 2023, four defendants were charged in the Central District of

[1] Bahamas Account #1 was opened by an entity registered in Sihanoukville, Cambodia. Based on my participation in this investigation and reputable public reporting, I know that this location in Cambodia is a hub for, among other things, cryptocurrency investment scams.

California with money laundering. Pursuant to warrants, the USSS seized and searched digital devices owned by defendants in that case, including an iPhone 13. The iPhone 13 included numerous communications involving the defendants in the case, and others involving co-conspirators,[2] and an individual subsequently identified as **LI**. Those communications show, among other things, that **LI** had a leadership role in determining where victim funds should be sent and in the management of the bank accounts receiving victim funds. **LI** also communicated directly with multiple co-conspirators to facilitate transactions involving victim proceeds.

IV. TECHNICAL TERMINOLOGY

9. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

10. "Digital currency" or "virtual currency" is currency that exists only in digital form; it has the characteristics of traditional money, but it does not have a physical equivalent. Cryptocurrency, a type of virtual currency, is a network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[3] Examples of cryptocurrency are bitcoin ("BTC"), Ether ("ETH"), Tether ("USDT"), and USD

[2] In addition to Co-Conspirator 1 and Co-Conspirator 2, the government has identified additional co-conspirators including a U.S.-based individual (Co-Conspirator 3) and a Chinese national (Co-Conspirator 4).

[3] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

Coin ("USDC"). Cryptocurrency can exist digitally on the internet, in an electronic storage device, or in cloud-based servers. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Most cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[4] Cryptocurrency is not illegal in the United States.

11. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. USDT, or Tether, is a type of stablecoin. USDT is pegged to the U.S. dollar, such that $1 is equal to 1 USDT.

12. An "Internet Protocol address" or "IP address" is a numerical address assigned to each computer connected to a network that uses the internet for communication. Internet Service Providers assign IP addresses to their customers. Because every device that connects to the internet must use an

[4] Some cryptocurrencies operate on blockchains that are not public.

IP address, IP address information can help to identify which computers or other devices were used to access an account. The type of application or service provider a particular customer is using often determines how long they will be assigned the same IP address. For instance, someone who rents computer servers can lease an IP address long term and maintain it for several years. In my training and experience, residential Internet Service Providers often lease the same IP address to a customer over months to a year. Cellular phone provider customer IP addresses often change more frequently due to customers being more transient. Email providers, internet providers, and even cybercrime forums often record the IP address used to register an account and the IP addresses associated with particular logins to the account. In my training and experience, when the same IP address is used to access different internet services in close temporal proximity, it tends to show the same computer or computer network was used to access those services. When several instances of this IP overlap exist over time from different service providers, it makes it very likely that the same person or group of people sharing internet infrastructure are behind the accesses.

13. A domain name is a simple, often easy-to-remember way for humans to identify computers on the internet, using a series of characters (*e.g.*, letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

14. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

V. STATEMENT OF PROBABLE CAUSE

15. Based on records, witness interviews, my review of electronic communications, and my knowledge of this investigation, I know the following:

A. Investigation into Pig-Butchering Scheme

16. In September 2022, law enforcement began an investigation into a criminal money-laundering syndicate operating cryptocurrency investment scams, also known as "pig-butchering." The term "pig butchering" (derived from the Chinese phrase used to describe this scheme) is a type of scam that involves scammers grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. In this syndicate, the scammers promoted spoofed domains and websites purporting to be legitimate cryptocurrency trading platforms to U.S. victims, including within the Central District of California. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal their money.

a. Once victim funds were obtained, the syndicate utilized various money-laundering techniques to conceal the nature and source of the victim funds. These techniques include the use of money couriers, a high volume of financial transactions with no legitimate commercial purpose, and shell accounts.

b. Structurally, the money-laundering syndicate comprised of money mules who received the fraud proceeds directly through shell company accounts, individuals who recruited, trained, and managed the money mules, intermediary companies who facilitated the conversation of the fraud proceeds into cryptocurrency, or received cryptocurrency fraud proceeds directly and transfer them on, and individuals who managed the network, connecting the organizations running the scamming operation with the laundering network.

B. Victim 1 Transferred Funds to Bahamas Account #2

17. Law enforcement traced pig-butchering proceeds from numerous individual victim accounts, including an account controlled by Victim 1 as described below, to Bahamas Account #2.

18. On May 1, 2023, law enforcement interviewed Victim 1, who resided in New Jersey. Victim 1 said they were a victim of a cryptocurrency investment scam. More specifically, Victim 1 explained that around May 2022, an individual purporting to be "Angela" sent Victim 1 a WhatsApp message and they began communicating. Victim 1 said they eventually switched to the encrypted messaging service Telegram and after a couple of

weeks, "Angela" asked if Victim 1 was interested in cryptocurrency investments. Victim 1 further stated that "Angela" would send screenshots of her cryptocurrency profits to encourage him to invest.

19. Victim 1 stated that "Angela" then provided a link to download an application he believed to be CoinZoom, which is a known cryptocurrency service. The web address provided was coinzooma[dot]com. The legitimate web address for CoinZoom is coinzoom[dot]com. According to registration records, the fake address coinzooma[dot]com was registered in July 2022 and has since been deleted. Based on my training and experience, I know this to be a spoofed domain purporting to represent a legitimate investment platform.

20. Victim 1 began investing in supposed virtual assets on the spoofed domain using his personal account with the cryptocurrency platform Crypto.com. When he reached daily limits on spending on Crypto.com, Victim 1 stated that "Angela" began sending him bank account numbers to allow him to wire funds directly from his personal bank account to the investment platform. Victim 1 said he was making investments once or twice a week and believed he was earning significant profit. Victim 1 estimated that from approximately July to August 2022, he invested about $1.5 million.

21. Victim 1 stated that on or around August 24, 2022, he attempted to withdraw the funds from the spoofed CoinZoom platform, and the platform's supposed online customer service informed him that he needed to pay taxes and fees in order to

withdraw his money. Victim 1 realized he had been scammed and reported his losses to law enforcement.

22. Victim 1 provided screenshots from the spoofed CoinZoom website showing the supposed large profits on his investments. Victim 1 also provided bank records corroborating his losses. For example, on July 1, 2022, Victim 1 sent a $30,000 wire to a Bank of America account ending in 0871. According to bank records, the account was opened in the name of the shell company CMD Export and Import. Bank records show that on July 11, 2022, the CMD Export and Import Bank of America account ending in 0871 wired $123,000 to a U.S. bank account with instructions for further credit to Bahamas Account #2.

23. CMD Export and Import has been the subject of numerous other victim complaints. California Secretary of State records show that CMD Export and Import was incorporated in Vernon, California, within Los Angeles County, in April 2022. The company is registered to a residential address with a stated business purpose of "trading import and export." Based on my training and experience and review of documents, the company was not involved in "trading import and export" but rather was a shell company set up for the sole purpose of receiving fraud proceeds.

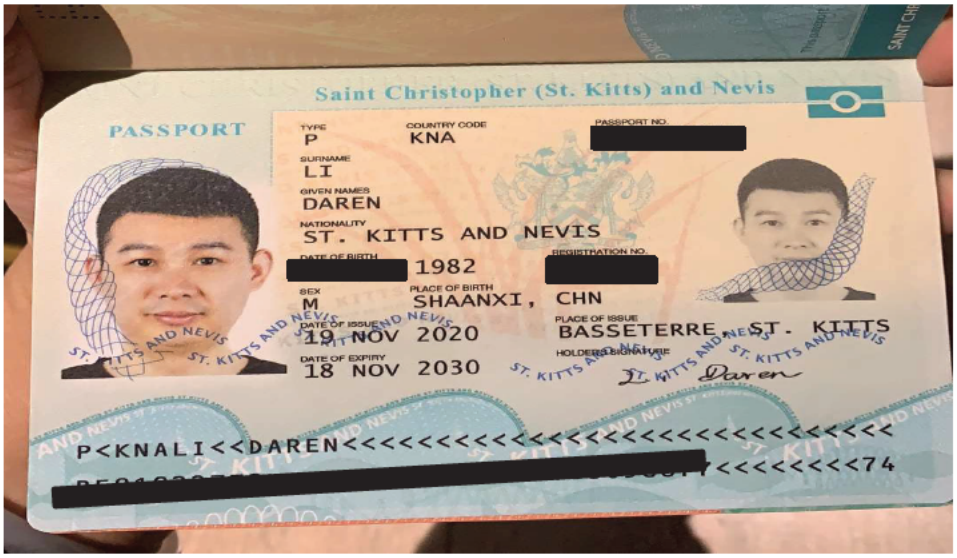
24. Victim 1's experience with the fraud is generally consistent with those of hundreds of other victims who have reported their losses to law enforcement, including victims in the Central District of California. Similarly, the set-up and operation of CMD is consistent with that of the other 73 shell

companies that law enforcement has identified as connected to this scheme, including numerous other companies incorporated in or associated with the Central District of California.

C. Victim 1's Proceeds Converted to USDT and Transferred to LI

25. Tracing of Victim 1's transfers shows that after the funds arrived in Bahamas Account #2, they were converted to USDT and transferred to **LI**'s account at Binance.

26. Financial records show that on July 15, 2022, $800,000, which included Victim 1's wire to CMD Export and Import, was converted into 798,403.19 USDT and deposited into a Binance account opened in **LI**'s name. Binance records show that on July 23, 2022, 1,649,999 USDT, including Victim 1's funds, was transferred from **LI**'s Binance account to a virtual currency address beginning with "TRteo" (the "TRteo Address"). Binance records also show that **LI** opened his Binance account in his name, using the email address 1575687@qq.com and a Saint Kitts and Nevis passport shown below:



27. Based on review of Binance records for **LI**'s Binance account and blockchain tracing, 4.5 million USDT of victim proceeds was deposited into **LI**'s Binance account and was all sent to the TRteo Account within days of the funds being deposited.[5] Based on my training and experience, individuals involved in organized money laundering commonly send proceeds to a common address after the proceeds have been laundered through other accounts to ultimately return the proceeds to the syndicate leaders who control the funds.

28. Based on review of Binance records for **LI**'s Binance account and blockchain tracing, **LI** also sent funds to and received funds from the TRteo Address. Based on my training and experience, individuals are commonly associated with the accounts they send funds to and receive funds from, and I believe that **LI** and/or his co-conspirators control the TRteo Address.

D. Victim 1 Funds Transferred to a Financial-Technology Company that LI Accessed

29. In addition to **LI**'s Binance account, pig-butchering proceeds also flowed to Wise Payments Limited ("Wise"), an international financial-technology company that **LI** accessed.

30. On July 20, 2022, Victim 1 again followed the scammer's instructions and sent a $5,000 wire to a bank account at Evolve Bank and Trust. Bank records show the Evolve Bank and

[5] A significant amount of the USDT from Bahamas Account #1 also was eventually deposited into the TRteo Address after first being deposited and withdrawn from another cryptocurrency wallet.

Trust account belongs to Jingshun International Corporation, a known shell company. Financial records show the $5,000 was then transferred from the Evolve Bank and Trust account to Wise. Based on records provided by Wise, the most common login to the Wise account from July to September of 2022 came from the IP address 91.75.209.125. Binance records show that **LI** logged into to his Binance account using the exact same IP address during the same timeframe, including at least once on the same day. Based on the foregoing, I believe **LI** had access to the Wise account that received fraud proceeds from Victim 1.

D. LI Provided Funding to Open Bahamas Account #2

31. According to Bahamas Account #2 records, a Los Angeles-based individual, Co-Conspirator 1, was the account owner of the Bahamas Account #2, which received approximately $35.4 million in pig-butchering and fraud proceeds from shell companies. As part of the account-opening process, Co-Conspirator 1 provided verification of funds. On or around July 15, 2022, Co-Conspirator 1 provided the Bahamas bank housing Bahamas Account #2 with a screenshot of his Binance.US account balance, which showed the balance as $1,016,730.79 as of June 8, 2022.

32. Binance.US records reveal that prior to June 8, 2022, Co-Conspirator 1 had less than $100 in his Binance.US account. Records show that on June 8, 2022, Co-Conspirator 1 received 999,383 USDT from **LI**'s Binance account and another 17,862 USDT from Co-Conspirator 4. On June 8, 2022, and on June 10, 2022, presumably after creating the account balance screenshot, Co-

Conspirator 1 returned the 999,383 USDT to **LI** at his Binance account. The timing of the funds sent by and returned to **LI** indicates that the only purpose of the transfer from **LI** was to intentionally provide false assets for Co-Conspirator 1 to facilitate the opening of Bahamas Account #2.

E. LI Directly Communicated with and Directed U.S. Money Launderers

33. On December 6, 2023, in Case No. 23-CR-596-RGK, a federal grand jury in the Central District of California charged four defendants ("Defendants 1 through 4") with conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h), concealment money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), and international money laundering, in violation of 18 U.S.C. § 1956(a)(2)(B)(i). As part of the investigation of that case, USSS agents determined that Defendant 1 managed and controlled bank accounts used to launder pig-butchering proceeds, including funds that were transferred to Bahamas Account #2.

34. On December 12, 2023, USSS agents executed federal search and arrest warrants on Defendant 1. USSS agents seized, among other things, Defendant 1's iPhone 13. During the review of Defendant 1's iPhone 13, USSS agents seized multiple Telegram chats showing **LI**'s involvement in the laundering of pig-butchering proceeds conducted by Defendants 1 through 4, as well as other individuals.

1. LI was Involved in Money Laundering by Defendants 1 Through 4

35. USSS agents' review of Defendant 1's iPhone 13 revealed that Defendant 1 corresponded with numerous individuals to launder victim funds. Some of the participants in those chats used monikers that included the letters "KG" followed by another name (e.g., "KG JASON"). Defendant 1 also participated in group chat messages on Telegram that had Telegram users with "KG" in the username, discussed content referencing "KG," and displayed a similar, unique icon, stating "KG Pay." Based on my training and experience, I believe that these individuals are associated with a common money laundering syndicate referred to as "KG." The icon associated with those communications is shown below.

36. One participant in the chats with Defendant 1 was Telegram user "KG71777." Subsequent investigation, discussed below, has shown that KG71777 was an account controlled by **LI**. In Defendant 1's iPhone 13, Telegram user KG71777 was listed as "KK" and displayed a Las Vegas icon.

37. In a September 4, 2023 Telegram chat between Defendant 1 and Defendant 2, Defendant 1 provided a screenshot of a Telegram chat she had with Telegram user "KK." The screenshot showed a September 4, 2023 Telegram chat that shows that **LI** is aware that law enforcement was looking for Defendant 2 and

suggests that **LI** helped Defendant 2 flee to Mexico.[6] In response to this screenshot, Defendant 2 informed Defendant 1 that **LI** was helping Defendant 2 pay for living expenses. Also in the screenshot, **LI** told Defendant 1 that if she was going to flee, that she should "give [him] a few accounts," and that she could coordinate if the bank needed a verification code.[7]

2. **LI** Facilitated Money Laundering by Defendant 1 and Co-Conspirator 2

38. USSS agents seized another Telegram group chat from Defendant 1's iPhone 13 that included Co-Conspirator 1 and Co-Conspirator 2 (who managed Bahamas Account #2) and **LI**, using the "KK" username. In that chat, Defendant 1 informed the group that she was depositing checks and referenced the Los Angeles area. In the chat, **LI** asked Co-Conspirator 2 how the check is being deposited.

From	Body[8]	Time
Defendant 1	I have two deposited, please check	4/15/2023 6:49:03 PM(UTC+0)
Co-Conspirator 2	It hasn't been recorded yet but it's a reality	4/15/2023 10:09:03 PM(UTC+0)
Co-Conspirator 2	show	4/15/2023 10:09:06 PM(UTC+0)

[6] USSS executed a federal search warrant on Defendant 2's residence in March 2023. USSS agents have since learned that Defendant 2 fled to Mexico days after the execution of the search warrant. As of the date of this affidavit, Defendant 2 remains a fugitive and his whereabouts are unknown.

[7] This screenshot was translated from Mandarin to English by a Mandarin-speaking USSS special agent.

[8] Translated from Chinese to English using Google Translate.

KK (**LI**)	[Co-Conspirator 2], do you need to bring this check to the bank to deposit? Or can she just issue it, then you deposit it online.	4/16/2023 3:47:16 AM(UTC+0)
Co-Conspirator 2	It's better to go to a bank to deposit in person. Large amounts online may not be approved. Even I'm not in the Los Angeles area	4/16/2023 6:47:43 AM(UTC+0)
Defendant 1	did the cashier's check go into the account?	4/18/2023 1:53:31 AM(UTC+0)
Co-Conspirator 2	not that fast, usually about two weeks	4/18/2023 5:00:13 AM(UTC+0)
Defendant 1	Hmm, I thought it would be faster if we go together	4/18/2023 5:00:45 AM(UTC+0)
Co-Conspirator 2	Oh Bank of America?	4/18/2023 5:01:32 AM(UTC+0)
Co-Conspirator 2	That will be faster	4/18/2023 5:01:36 AM(UTC+0)
Co-Conspirator 2	I look everyday	4/18/2023 5:01:52 AM(UTC+0)

39. From my review of the attachments to the Telegram group chat, Defendant 1 deposited the checks into a bank account opened within the Central District of California for a business named "Crestview Services, Inc." Florida Secretary of State Records show that Crestview Services Inc. was owned by Co-Conspirator 2 and bank records show that the bank account was opened by Co-Conspirator 2. Bank records for Bahamas Account #2 and USSS victim interviews show that known shell companies sent fraud proceeds directly to Crestview Services, Inc., and that

Crestview Services, Inc. in turn sent money to Bahamas Account #2.

40. Later in the chat, on April 22, 2023, Defendant 1 posted images of three checks worth $19,533 and indicated she was depositing those checks as well. Bank statements for the Crestview Services, Inc. account show that these checks were successfully deposited on April 24, 2023.

a. The checks were sent from companies titled "Kais Tea Set Supplies," "KQQ Trading LLC," and "KQQ Kitchen Appliance Wholesale LLC."

b. California Secretary of State Records reveal that "KQQ Trading LLC" and "KQQ Kitchen Appliance Wholesale LLC" are registered to the same individual, and that "Kais Tea Set Supplies" and "KQQ Kitchen Appliance Wholesale LLC" are registered to the same residential address in Diamond Bar, California, located in the Central District of California.

41. Based on my training and experience and knowledge of this money laundering syndicate, it is common for individual money mules to register multiple businesses with similar names and at similar addresses. Law enforcement has received complaints from fraud victims who sent money to each of the entities identified in paragraph 40.b above. USSS has interviewed two of those victims, who confirmed they sent money directly to "KQQ Kitchen Appliance Wholesale LLC" and "Kais Tea Set Supplies."

42. Additionally, Co-Conspirator 2 indicated he will "look everyday" for the check deposit, which, based on my training and

experience and knowledge of the investigation, reveals Co-Conspirator 2's desire to quickly withdraw the funds once deposited. **LI**'s participation in these chats indicates his involvement in laundering fraud victim proceeds through shell companies in the Central District of California and with Defendant 1, Co-Conspirator 1, and Co-Conspirator 2.

3. Defendant 1 and Co-Conspirator 3 Discussed Working for **LI**

43. USSS agents also seized a Telegram group chat from Defendant 1's iPhone 13 between Defendant 1 and Co-Conspirator 3. In these chats, dated between April 2023 and October 2023, Defendant 1 and Co-Conspirator 3 often spoke about working for a "Master" or "Boss" to keep bank accounts open. For example, the chat discussed multiple bank account closures due to fraud. In that context, Defendant 1 and Co-Conspirator 3 discussed how to obtain the money from the closed accounts and to communicate any issues to the "boss." For example, on October 25, 2023, Defendant 1 had trouble keeping an account open and Co-Conspirator 3 told Defendant 1 to send evidence to "[her] master".

From	Body[9]	Time
Co-Conspirator 3	Even if all of that stuff comes to pass, if you just make a videotape for me outside the bank, if you just cooperate with me a little bit, it will make it easier for me to	10/25/2023 8:02:51 PM(UTC+0)

[9] Translated from Mandarin to English using a certified translator.

	explain things to the customer	
Co-Conspirator 3	It is 200k, not 20k. How much do we make in a month?	10/25/2023 8:03:18 PM(UTC+0)
Co-Conspirator 3	You should tell your master about the conditions on your end. You see, that 200,000, you and your master need to figure out how to resolve that thing. Let me report a bit, I will contact you later to get the cell phone	10/25/2023 8:05:38 PM(UTC+0)

44. In another Telegram chat, Defendant 1 and Co-Conspirator 3 discussed an issue with a bank account and how to inform the "master" of the problems. In the chat, Co-Conspirator 3 sent Defendant 1 a screen shot of a chat he was having with Defendant 1's "boss."

From	Body[10]	Date
Defendant 1	Then we'll keep asking the bank why the check cannot be returned?	10/25/2023 9:37:14 PM(UTC+0)
Defendant 1	How should we say it?	10/25/2023 9:37:22 PM(UTC+0)
Co-Conspirator 3	But you must send it over. Now we got to be careful with our reply. He's really a big brother in Cambodia; he's lying.	10/25/2023 9:37:30 PM(UTC+0)
Co-Conspirator 3	Now it is really difficult to handle.	10/25/2023 9:37:50 PM(UTC+0)

[10] Translated from Mandarin to English by a certified translator.

Defendant 1	I've never failed to make call for you.	10/25/2023 9:37:59 PM(UTC+0)
Defendant 1	Why did I call on Tuesday? Because that banker had said previously that the account will be closed on Monday.	10/25/2023 9:38:19 PM(UTC+0)
Defendant 1	So I called on Tuesday.	10/25/2023 9:38:29 PM(UTC+0)
Co-Conspirator 3	[Chat Screen Shot (see below)]	10/25/2023 9:38:51 PM(UTC+0)
Defendant 1	Think about how to talk with the bank.	10/25/2023 9:38:54 PM(UTC+0)
Co-Conspirator 3	He is courteous and gentle to you. That's definitely not the way my master treats me.	10/25/2023 9:39:09 PM(UTC+0)
Co-Conspirator 3	I've been scolded several times about this matter.	10/25/2023 9:39:18 PM(UTC+0)
Defendant 1	He's pretty modest	10/25/2023 9:39:24 PM(UTC+0)
Co-Conspirator 3	Make a phone call.	10/25/2023 9:39:30 PM(UTC+0)
Defendant 1	He said I've had bad luck recently...	10/25/2023 9:39:37 PM(UTC+0)

45. The screenshot below was embedded in the above chat.[11] The "Big Boss" has the same "Las Vegas" Telegram profile image as the one saved in Defendant 1's contact for **LI**'s Telegram profile (as Telegram username "KK" and Telegram user handle "KG71777"). I thus believe that Telegram user "KK" (Telegram user handle "KG71777") from Defendant 1's iPhone 13 is the "boss" or "master" to whom Defendant 1 and Co-Conspirator 3 report bank transaction updates that are part of the money-laundering scheme.

[11] Translated from Mandarin to English by a certified translator.

F. LI is Telegram User "KK" (Telegram Handle "KG71777") in Defendant 1's iPhone 13

46. Based on my review of Defendant 1's iPhone 13, I know that Defendant 1 saved the "KK" Telegram username to be associated with Telegram user handle "KG71777" and a Cambodian phone number ending in 1777. The profile picture for "KK" also matches the Las Vegas profile picture for the "boss." Co-Conspirator 3 also discussed that Defendant 1's "boss" is "in Cambodia." I thus believe that Telegram user "KK" (Telegram user handle "KG71777") resides in or is frequently located in Cambodia.

47. Binance records for **LI** show geolocation IP login data for the IP addresses that **LI** used to log in to his Binance account. Those IP addresses show frequent logins from Cambodia. A Cambodia IP address was used to send the funds from **LI**'s Binance Account to the TRteo Account. The same IP address was used to log in **LI**'s Binance account more than 100 times between June 2022 and at least January 2024. That IP address was also used in 2022 to submit a U.S. visa application in **LI**'s true name. In a subsequent U.S. visa application, **LI** used the same Saint Kitts and Nevis passport shown in paragraph 26 and used to open **LI**'s Binance account.

48. WhatsApp records for the Cambodian phone number ending in 1777 show that the phone number is associated with a WhatsApp account with the username of "KG Perfect." That WhatsApp account also lists an email address of darren1575687@gmail.com." Google records for Co-Conspirator 4's Google account reveal the

same Cambodian phone number ending in 1777 saved under the contact name "KG Perfect Mr. Li".

49. Google records for "darren1575687@gmail.com" show that the subscriber's name is "Darren KG." Binance records reveal that the email address linked to **LI**'s Binance account (which was opened using **LI**'s passport) is "1575687@qq.com." That address and the email address linked to LI's WhatsApp number both use the same arbitrary string of numbers "1575687."

50. From the search of Defendant 1's iPhone 13, I know that Defendant 1 saved a WeChat contact as "Mr. Li's wife." In Defendant 1's communications with "Mr. Li's wife," Defendant 1 and the user discuss picking up cash from an address in Temple City, California (the "Temple City Address") on three occasions in April 2023, September 2023, and October 2023. Based on my review of Defendant 1's Telegram communications with Co-Conspirator 3,[12] I know that Co-Conspirator 3 referenced dropping off money to "Xiaolan" on October 14, 2023. In another Telegram chat, Defendant 1 and Co-Conspirator 3 discussed a "lump sum of money," and Co-Conspirator 3 referenced "Sister Cai."

51. USSS conducted physical surveillance outside the Temple City Address on February 15, 2024. USSS agents observed Co-Conspirator 3 arrive, walk toward the garage door, leave with a medium size black bag in his hand, and enter Co-Conspirator 3's vehicle. USSS agents also later observed a vehicle parked in the Temple City Address garage on March 14, 2024.

[12] These communications were translated from Mandarin to English by a certified translator.

52. Based on my review of California DMV records, I know that the vehicle parked in the Temple City Address garage was registered to Xiaoyan Cai.[13] Based on my review of **LI**'s U.S. visa applications, **LI** states that he is married to Xiaoyan Cai.

53. Based on the evidence discussed above, I believe that the Telegram user "KK" (Telegram handle "KG71777") is **LI** and that **LI** is a high-level member of Defendant 1's money laundering syndicate.

VI. CONCLUSION

54. For all of the reasons described above, there is probable cause to believe that **DAREN LI** has committed violations of Title 18, United States Code, Section 1956(h) (conspiracy to commit concealment money laundering) involving the proceeds of wire fraud, in violation of Title 18, United States Code, Section 1343.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 8th day of April, 2024.

Patricia Donahue

THE HONORABLE PATRICIA DONAHUE
UNITED STATES MAGISTRATE JUDGE

[13] Based on my discussions with a USSS Mandarin-speaking agent, I understand that the "y" in the name "Xiaoyan" may be translated to be an "l" depending on the dialect of the translator.