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.

AMIR HOSSEIN GOLSHAN,

Defendant.

Case No. 2:23-mj-00460-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 April 13, 2022 in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1030(a)(7)	Threatening to Damage a Protected Computer

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Nicholas A. Rasch
Complainant's signature

Nicholas A. Rasch, 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: February 1, 2023

Paul L. Abrams
Judge's signature

City and state: Los Angeles, California

Hon. Paul L. Abrams, U.S. Magistrate Judge
Printed name and title

AUSA Andrew M. Roach (213) 894-0306

AFFIDAVIT

I, Nicholas A. Rasch, being duly sworn, declare and state as follows:

I. BACKGROUND OF AFFIANT

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since June 2022. I am currently assigned to the Los Angeles Cyber Fraud Task Force, where I specialize in the investigation of computer and high-technology crimes, including computer intrusions, denial of service attacks, and other malicious computer activity. During my career as an FBI Special Agent, I have received training in the investigation of violations of criminal law, such as drug trafficking, fraud, and computer crimes. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a complaint and arrest warrant for AMIR HOSSEIN GOLSHAN ("GOLSHAN") for a violation of 18 U.S.C. § 1030(a)(7): Threatening to Damage a Protected Computer.

3. This affidavit is also made in support of an application for warrants to search:

a. The person of GOLSHAN, as further described in Attachment A-1.

b. The premises of 1201 S. Hope Street, Apartment 3516, Los Angeles, CA 90015 (the "SUBJECT PREMISES"), as further described in Attachment A-2.

III. ITEMS TO BE SEARCHED

4. The person to be searched is GOLSHAN, described in Attachment A-1, and the premises to be searched is the SUBJECT PREMISES, described in Attachment A-2.

IV. ITEMS TO BE SEIZED

5. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1030 (Fraud and Related Activity in Connection with Computers), 371 (Conspiracy to Commit an Offense), 1343 (Wire Fraud), 1029 (Fraud and Related Activity in Connection with Access Devices), and 1028A (Aggravated Identity Theft) (the "Subject Offenses"), as more fully described in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

6. 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 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 statements described in this affidavit are related in substance

and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

V. BACKGROUND ON SIM SWAPPING AND INSTAGRAM

7. Based on my training and experience, and information provided to me by others, including other investigators, I am aware of the following concepts:

Background on SIM Swapping

a. The Subscriber Identity Module ("SIM") card is a chip located inside a cell phone that stores information identifying and authenticating a cell phone subscriber. The SIM card is paired to a particular cell phone via the cell phone's International Mobile Equipment Identity ("IMEI") which is a unique number to identify mobile phones on a carrier's network. Once properly paired, the SIM card and IMEI authenticate a cell phone subscriber, device, and phone number to a particular cell phone and allow the user to make calls, send texts, and use the device.

b. When a cell phone carrier reassigns a phone number from one device to another -- such as when a customer purchases a new phone but wants to retain the same number -- the carrier switches the assignment of the SIM card in the old device to the SIM card in the new device by changing the IMEI associated with that subscriber's account. This process is sometimes called "porting" a number.

c. "SIM swapping" refers to the process of inducing a carrier to reassign a cell phone number from the legitimate subscriber's device to a device controlled by another without

the legitimate subscriber or user's authorization. The purpose of a SIM swap is typically to defeat two-factor security authentication features[1] on the victim's online accounts in order to take them over. Once the SIM swap is complete, the SIM swapper causes password reset codes to be sent to the victim's cell phone number, which is now controlled by the SIM swapper. From there, the SIM swapper can access the victim's online accounts, change the passwords of the victim's accounts, and impersonate the victim in order to commit further fraud.

d. To commit a SIM swap, the fraudster must first obtain information about a victim, like a social security number and billing address, and the victim's cell phone number. The fraudster then uses this information, including personal details often gleaned from social media, to impersonate the victim to the victim's mobile network operator and deceive the network operator into assigning the victim's cell number to a cell phone in the fraudster's possession. Despite its name, this is usually done without the fraudster ever physically touching the victim's phone or SIM card. In other words, there is no physical swapping of the victim's SIM card from the victim's phone to the fraudster's new phone and, in most cases, the victims are unaware they have been SIM swapped until after it has happened and their cell phone service stops working.

[1] Two-factor authentication is an extra layer of protection used to protect the security of online accounts beyond just a username and password. Usually, this includes a verification code which is sent via text message to the user's cell phone to confirm the user's identity.

e. After the SIM swap, all calls and texts to the victim's cell phone number are routed to the SIM swapper's cell phone, including any password resets requests for websites or applications (e.g., Instagram).

Background on Instagram

f. Instagram owns and operates a free-access social-networking website and smartphone app of the same name. Instagram allows its users to create their own profiles, which can include a short biography, or "bio," a photograph of themselves, and other information. Instagram maintains servers and computers which are used in and affect interstate and foreign commerce and communication, and they are therefore considered "protected computers" as defined by 18 U.S.C. § 1030(e)(2)(B).

8. Instagram accounts with large followings (e.g., popular accounts of social media influencers) are considered valuable because of the account holder's ability to monetize access to their followers. Some Instagram users can earn thousands of dollars or more a month by selling products, promoting sponsors, or otherwise monetizing their following. Instagram accounts with large followings tend to take many years to grow their audiences.

9. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. Instagram users are also asked to provide their cell phone for two-step authentication. This information is collected and maintained by Instagram. Instagram asks users to provide basic

identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This subscriber information may include the user's full name, e-mail addresses, and phone numbers, as well as other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram also provides recovery codes to users. Recovery codes are one-time use codes that that a user can use to gain access to her account if the user is having trouble accessing her account with the password and two-step authentication.

VI. SUMMARY OF PROBABLE CAUSE

10. The FBI is currently investigating GOLSHAN for a series of SIM swaps and subsequent social media account takeovers of multiple female social media influencers. Specifically, the victims reported being SIM swapped and having their social media accounts taken over by an unknown subject. The victims then received threats that the subject would delete their social media account unless they paid for the return of their social media accounts. Other victims reported that the subject would impersonate them on social media and dupe their online friends into sending money to the subject.

11. Through the investigation, the FBI identified GOLSHAN as the individual behind the SIM swaps based on, among other things, (1) his connection to an IP address that was used to access a victim's social media accounts when they were taken

over; (2) a victim's identification of GOLSHAN as the person who took control of her Instagram account and with whom she had a video call; and (3) a common IMEI used during the SIM swaps of multiple victims.

12. In January 2023, the FBI identified the SUBJECT PREMISES, a high-rise luxury apartment in downtown Los Angeles, as GOLSHAN's current residence. For the reasons explained below, there is probable cause to believe that GOLSHAN violated 18 U.S.C. § 1030(a)(7) (Threatening to Damage a Protected Computer) and that GOLSHAN's person and the SUBJECT PREMISES will contain evidence of the Subject Offenses committed by GOLSHAN.

VII. STATEMENT OF PROBABLE CAUSE

13. Based on my review of the case file and associated documents, interview reports, and other information, my conversations with FBI Special Agent Daniel Latham, and my own knowledge of the investigation, I am aware of the following information.

A. Victim 1 Reports SIM Swapping to FBI

14. In January 2022, the FBI received a complaint from victim L.K. ("Victim 1") stating that she had been SIM swapped in December 2021. Victim 1 is a model and social media influencer living in Los Angeles, California, with approximately 150,000 followers on Instagram.

15. Victim 1 reported that on December 26, 2021, an unknown person, now believed to be GOLSHAN, took control of her cell phone number and then her Instagram account.

16. Victim 1 believed that she was SIM swapped in the following manner, and provided the FBI with multiple screenshots, emails, and other information relating to her SIM swap:

a. At approximately 1:17 p.m. on December 26, 2021, Victim 1 received a direct message on Instagram from the account owned by one of her friends, stating "Can you do me a favor? What's your number?" Victim 1 provided her phone number to the person whom she believed was her friend.

b. Four hours later, at approximately 4:55 p.m., Victim 1 noticed that her phone was no longer connecting to the T-Mobile network. She then received an email from T-Mobile stating that her account had been changed from her personal iPhone to an iPhone 8 that she did not recognize. This is when she realized that she had been SIM swapped.

c. Victim 1 used her roommate's cell phone to call T-Mobile to attempt to get her cell phone service restored. It took Victim 1 approximately two hours to regain control of her cell phone account. Once Victim 1's cell phone service was restored, Victim 1 received numerous text messages from her friends informing her that her Instagram account was hacked and that an unknown individual was posing as Victim 1 and requesting cell phone numbers and money from Victim 1's friends. Victim 1 attempted to log into her Instagram account and discovered her password had been changed.

d. Victim 1 was unable to log into her Instagram account for 24 hours. During the 24 hours that she was locked

out of her Instagram account, Victim 1 reported that the subject collected approximately $15,000 from Victim 1's friends by pretending to be Victim 1 and requesting money from them.

e. Victim 1 also reported receiving threats from the subject on WhatsApp. Victim 1 attempted to take screenshots of these messages, but the subject deleted them after Victim 1 read them.

17. I have personally reviewed multiple screenshots and emails that Victim 1 provided to the FBI corroborating the takeover of her social media accounts. Here are a few examples:

a. An Instagram direct message the subject sent from Victim 1's Instagram account to a friend stating, "Can you zelle someone for me? My limit is reached, i'll pay you back plus an extra $100 by tomorrow." After the friend agreed to send the payment, the subject told the friend to send payment to an unknown email address. I saw multiple messages with language and requests similar to this example among Victim 1's messages.

b. Multiple T-Mobile emails indicating that the IMEI associated with Victim 1's account was changed.

c. Multiple emails from Instagram and Snapchat indicating that Victim 1's accounts had new logins and the passwords were changed.

18. Victim 1 reported that several other women's Instagram accounts were SIM swapped in a similar manner in the week after hers. Specifically, Victim 1 stated that the "hacker" contacted other people from her account and used the same questions —- "Can you do me a favor? What's your number?" —- that she

received from the person whom she believed was her friend on December 26, 2021. Victim 1 provided the names of five other victims (including Victim 2, discussed below) and said that she and the other victims all had T-Mobile cell phone service.

19. The FBI received records from Snapchat showing IP addresses used to login to Victim 1's Snapchat account during the time it was taken over by the subject. Those IP address records showed that an IP address of 104.35.115.130 accessed Victim 1's Snapchat account on December 26, 2021.[2]

B. Victim 2 is SIM Swamped

20. The FBI interviewed victim A.F. ("Victim 2"), a female model and social media influencer residing in Rancho Palos Verdes, California. Victim 2 has over 100,000 Instagram followers. Victim 2 reported that she was friends with Victim 1 and that they had worked together in the past.

21. Victim 2 reported that she noticed there was a problem with her T-Mobile cell phone when she went to check her Instagram account at approximately 7 p.m. on January 2, 2022. Victim 2 stated that her Instagram account was signed out from her phone, and she was unable to log back in. Victim 2 attempted to recover her password using two-step authentication through a text to her phone. But she noticed that the password was not sent to her phone, which indicated to her that her phone number was removed as a recovery method.

[2] This same IP address was also used to access GOLSHAN's Coinbase account, as discussed below.

22. Victim 2 called T-Mobile around 8 or 9 p.m. to try to restore the service on her cell phone. She reported being on the phone with T-Mobile for four to five hours to restore her cell phone service. However, it took Victim 2 at least a day to regain access to her Instagram account.

23. While Victim 2 was locked out of her Instagram account, she received a call on WhatsApp from a man, now believed to be GOLSHAN or an accomplice, who demanded $5,000 to restore Victim 2's access to her Instagram account. Victim 2 stated that the caller sounded like a very young man. The caller said if Victim 2 did not pay, he would delete her account.

24. Victim 2 ultimately recovered access to her Instagram account without paying the subject. After she regained control of the account, she saw that numerous messages had been sent from her account to her friends asking them to send money to her through Venmo to accounts that Victim 2 did not recognize or control.[3]

C. Victim 3 is SIM Swapped[4]

25. The FBI interviewed victim K.M. ("Victim 3"), a woman residing in Ontario, California. Victim 3 has nearly 60,000 followers on Instagram. Victim 3 provided the following chronology of events and communications to the FBI. Victim 3 also provided the FBI with corroborating information, including

[3] The FBI requested copies of these messages from Victim 2 but has not yet received them.

[4] The Complaint alleges a violation of 18 U.S.C. § 1030(a)(7) for the threats made to Victim 3.

a screenshot of communications she had with the subject along with an audio recording she took during a call with the subject.

26. Victim 3 reported that her SIM swap began with issues with her cell phone service. Specifically, Victim 3 reported that her cell phone stopped connecting to the T-Mobile network on April 13, 2022. Shortly thereafter, an unknown person, now believed to be GOLSHAN, reset her password and took control of her Instagram account.

27. Victim 3 used another Instagram account to send a message to her Instagram account. The person controlling her account demanded $5,000 from Victim 3 to return her Instagram account. Victim 3 responded that she did not have that amount of money, and she asked if the subject would accept $1,000. The subject agreed.

28. Victim 3 asked to send a test payment to ensure the money would go to the correct person. The subject instructed Victim 3 to send $1 via Zelle to Individual 1. Victim 3 complied and sent the $1 payment as instructed. Victim 3 took a screenshot of this payment, and later sent the screenshot to Victim 4, who provided it to FBI.

29. The subject then asked Victim 3 to continue the discussion on Telegram, which she did.[5] The subject communicated with Victim 3 using the Telegram username "@Drake." Victim 3 ultimately decided that she would not pay the $1,000 to the subject and relayed this to the subject. The subject then said

[5] Telegram is an encrypted communications application. Based on my training and experience, I understand that Telegram servers are located outside the United States.

he would return Victim 3's Instagram account if she initiated a video call and stripped for him. The subject told Victim 3 that every time "he hacks girls, he makes them show themselves."

30. Victim 3 agreed to a video call. Victim 3 described the person on the video call as a dark-skinned man, possibly of Indian descent, with an accent. Victim 3 noted the man appeared to be around 23 or 24 years old and had distinctive eyes that were far apart. On the call, the subject instructed Victim 3 to strip for him. Victim 3 complied while the subject masturbated.

31. Victim 3 said that she spoke with the subject for about an hour and was trying to be nice to him so that he would give her account back. During their conversation, the subject told Victim 3 that he hacked his neighbor when he lived at the Orsini Apartments in downtown Los Angeles.[6] He said that he was able to get into his neighbor's bank account and get copies of her medical records. He told Victim 3 that the neighbor ultimately paid him thousands of dollars to get her accounts back.

32. In the end, the subject gave Victim 3 her Instagram account back for a short period of time. However, the subject continued to text and call Victim 3, including asking her out to dinner. Victim 3 declined and did not respond further. The subject ultimately retook control of Victim 3's account and deleted her Instagram account. Based on my training and

[6] The FBI determined that GOLSHAN's neighbor at the Orsini Apartments was another female social media influencer operating under a pseudonym. The neighbor has over 106,000 followers on her Instagram account.

experience, I believe that the subject retook Victim 3's Instagram account using a recovery code that he most likely saved when he was in control of the account.

33. Victim 3 provided the FBI with the following, all of which I have personally reviewed:

a. A screenshot of Telegram messages she exchanged with the subject after he deleted her Instagram account. In the chat message Victim 3 stated, "You logged in and changed my pass word." The subject responded, "Cause you never responded to my messages."

b. A screenshot of the Telegram username "@Drake," which was the moniker that the subject used to communicate with Victim 3.

c. A recording of phone call that Victim 3 had with the subject after he deleted her Instagram account. In the recording Victim 3 asked the subject why he was doing this to her. She further stated that the subject had said he was not going to mess with her account anymore and that she did everything he asked of her.

D. Victim 4 is SIM Swapped

34. The FBI interviewed victim S.S. ("Victim 4"), a woman residing in Los Angeles, California, who provided the below information.

35. Victim 4 received an Instagram message from her friend Victim 3's account on April 12, 2022 (i.e., around the time Victim 3 reported that her Instagram account was compromised). Victim 4 began conversing with a person she thought was

Victim 3. During the conversation, the person asked for Victim 4's phone number, first name, last name, and Instagram handle. Victim 4 provided the information, believing she was talking to Victim 3.

36. Shortly thereafter, Victim 4's cell phone stopped connecting to the T-Mobile network. The passwords to Victim 4's Instagram and Snapchat accounts were also changed.

37. At the time, Victim 4 thought her phone was broken, so she visited an Apple store and purchased a new phone. This new phone was able to receive and make phone calls after it was activated.

38. Victim 4 started receiving phone calls from a male subject after her new phone was activated. The subject stated he was in control of Victim 4's social media accounts, email accounts, and photos. He demanded $4,000 in exchange for not deleting Victim 4's social media accounts. Victim 4 refused to pay the subject and the subject proceeded to delete her Instagram account.

39. Victim 4 provided the FBI with the following information, all of which I have personally reviewed:

a. An email from Snapchat showing the IP addresses that were used to log into her account during the period it was taken over. The email showed that the IP address 104.34.71.230 was used to log into Victim 4's Snapchat account on April 13, 2022 from Los Angeles, California. Victim 4 told the FBI that she did not log into her Snapchat account on that day, because she was locked out.

b. Several screenshots of Instagram messages that were sent from Victim 4's account while she was locked out. In the messages, the person using the account asked Victim 4's friends to send money to various email addresses. In one conversation, the subject wrote to Victim 4's friend, saying, "I'm trying to zelle someone but my limit is reached can you send it for me i'll pay you back +50 by tomorrow morning."

c. Three recordings that Victim 4 made of phone calls she had with the subject. In one of the recordings, the subject discussed the amount Victim 4 would pay for the return of her accounts. The subject then stated he would change something on her account to show her that he had control of her account. In another recording, the subject asked if Victim 4 wanted to make a deal and get her page back. The subject said if she did not pay him then he would delete all her videos and her page would be permanently deleted.

E. The FBI Traces the IP Address Used to Access Victim 4's Instagram Account to GOLSHAN

40. Charter Communications records show that on April 13, 2022, IP address 104.34.71.230 was assigned to an account subscribed to by Amir Mansor Golshan at 19448 Victory Boulevard, Reseda, California 91335 (the "Reseda Address").

41. The FBI conducted a database[7] query of Amir Mansor Golshan and determined that that he was 55 years old and that he had a 24-year-old son named Amir Hossein Golshan (GOLSHAN).

[7] The database is a public information database used by law enforcement that provides names, addresses, telephone numbers, and other identifying information.

42. I reviewed GOLSHAN's California Department of Motor Vehicles records and determined that his driver's license photo and details matched the age, sex, and possible ethnicity of Victim 3's description of the subject. Additionally, I observed that GOLSHAN's eyes were set notably apart in his driver's license photo, which also matched the description that Victim 3 provided.

43. FBI Special Agent Daniel Latham later showed GOLSHAN's driver's license photo to Victim 3 to determine if GOLSHAN was the person with whom she spoke during the video chat. Victim 3 said that she was "1000%" sure that the man in the picture (GOLSHAN) was the male she spoke with on the video chat.

44. Records from the Orsini Apartments in Los Angeles showed that GOLSHAN lived at the Orsini Apartments from April 3, 2020 to September 21, 2020. Those records also showed that GOLSHAN listed the Reseda Address as his prior address. No driver's license was provided with GOLSHAN's tenant application; however, his reported date of birth matches the date listed on GOLSHAN's California driver's license.

F. T-Mobile Data and an Internal T-Mobile Investigation Confirm Victims Were SIM Swapped

45. The FBI received IMEI, subscriber, and other records for the victims' T-Mobile accounts. The IMEI records of the victims' cell phone accounts were also consistent with SIM swapping based on my training and experience and information I learned from other agents. For example, the victims' accounts show quick changes in the IMEI associated with their accounts,

sometimes lasting for just a few hours. Based on my training and experience and that of other agents, I know these quick changes in IMEIs are consistent with a subject temporarily changing the IMEI of a victim's account for a short period until the victim is finally able to retake their account and transfer service back to their original IMEI or a new IMEI.

46. T-Mobile records also showed that certain victims' cell phone accounts were transferred over to the same suspect IMEI ending in 8550 ("the 8550 IMEI"), believed to correspond to a device controlled by GOLSHAN. Specifically, those records showed the following:

a. From December 21, 2021 to January 2, 2022, Victim 2's T-Mobile account was associated with an IMEI ending in 8370. Around the timeframe Victim 2 reported that her phone stopped working, on January 2, 2022, the IMEI associated with her T-Mobile account changed to the 8550 IMEI. Approximately three hours later, the IMEI associated with her account changed back to the IMEI ending in 8370, consistent with Victim 2 regaining control of her phone number

b. From April 1, 2022 through April 12, 2022, Victim 3's T-Mobile account was associated with the IMEI ending in 1570. On April 12, 2022, around the time Victim 3 reported she was SIM swapped, the IMEI on Victim 3's account changed to the 8550 IMEI. About three hours later, the IMEI changed back to the IMEI ending in 1570, consistent with Victim 3 regaining control of her phone number.

c. From April 10, 2022 through April 13, 2022, Victim 4's T-Mobile account was associated with the IMEI ending in 2440. On April 13, 2022, around the time Victim 4 reported she was SIM swapped, the IMEI on Victim 4's account changed to the 8550 IMEI. Within approximately two hours, Victim 4's IMEI was changed to the IMEI ending in 8110, consistent with Victim 4 obtaining a new phone.

47. Based on my training and experience and discussions with other agents, I know the IMEI changes discussed above are consistent with a SIM swapper using the same device (and thus the same IMEI) to SIM swap multiple victims at different times.

48. FBI Special Agent Daniel Latham reviewed the T-Mobile IMEI data relating to the SIM swamps of several victims and identified the suspected IMEI used for the SIM swaps based on the abrupt changes in IMEI, as described above. Agent Latham sent those IMEIs to a T-Mobile investigator to investigate whether they were connected to a database breach or potential inside actor. The T-Mobile investigator determined that Victims 1 and 2 had been SIM swapped in a similar manner. Specifically, investigator determined that the subject was able to SIM swap Victims 1 and 2 by calling T-Mobile retail stores and impersonating Victims 1 and 2 to the store employees. The subject then requested that the store employees switch Victims 1's and 2's cell phone numbers to other devices.

G. The FBI Finds GOLSHAN's Coinbase Account

49. The FBI received documents from Coinbase, a cryptocurrency exchange platform, for GOLSHAN's Coinbase

account. A review of the records for the Coinbase account revealed the following:

a. The accountholder was listed as GOLSHAN.

b. The Reseda Address was listed as one of the accountholder's addresses.

c. (424) 313-4277 was listed as the user's phone number, and dailyuser2000@gmail.com was listed as the user's email address.[8]

d. The account was accessed from IP address 104.35.115.130 on December 6, December 23, and December 31, 2021. This is the same IP address that was used to access Victim 1's social media accounts on December 26, 2021, when Victim 1 reported that she was SIM swapped.

e. There were multiple bank accounts in Golshan's name linked to the Coinbase account, including accounts at Wells Fargo, Chase, Bank of America, Citi, and Bank of the West.

f. The account's various virtual currency wallets received approximately $423,575 and sent approximately $340,615 during the period of December 2018 to April 2022. During this same period, approximately $176,550.06 was withdrawn from the Coinbase account to GOLSHAN's linked bank accounts.

g. GOLSHAN's California driver's license was provided to Coinbase to verify his identity.

[8] Verizon records show that this phone number was assigned to an Apple iPhone with an IMEI ending in 1535. Records from Apple for the IMEI ending in 1535 showed that the phone was registered to GOLSHAN, using an iCloud account username of "dailyuser2000@gmail.com."

H. GOLSHAN's Bank Records Show More Evidence of Fraud

50. Wells Fargo records for a checking account ending in 3049, held in GOLSHAN's name and linked to his Coinbase account, showed the following:

a. Between April 12, 2019, and May 1, 2019, GOLSHAN received approximately 165 Zelle payments totaling $23,790 from different people. Most of these Zelle payments referenced Instagram account names and the word "verification."

b. Wells Fargo closed GOLSHAN's bank account on May 19, 2019.

c. On April 25, 2019, the account received three Zelle payments totaling $300 from the same sender. Two payments were for $100 each and they had an accompanying note referencing an Instagram account name. A third payment of $100 referenced "verification." The following day, the same Zelle account sent a $1 payment with a note attached that read, "You fucking creep stealing money from a 14" (presumably meaning a 14-year-old person).

51. The FBI identified and interviewed the holder of the Zelle account who sent the $301 discussed above to GOLSHAN's account ("Victim 5"). Victim 5 stated that the Instagram account name referenced in her initial payments was the Instagram account for Victim 5's teenage daughter. Victim 5's teenage daughter was trying to be a model. Victim 5 saw an advertisement on Instagram saying that for a fee, the poster

could get any Instagram account verified.[9] Victim 5 sent a message to the account and requested that her daughter's modeling Instagram page be verified. Victim 5 sent the $300 via Zelle as compensation for this service. Almost as soon as Victim 5 sent the Zelle payments, the Instagram account she was communicating with was deactivated. At this point, Victim 5 realized she fell for a scam. Victim 5 said she then sent the $1 Zelle payment with the note, "You fucking creep stealing money from a 14," as described above, in the hopes of making the fraudster feel bad.

I. The FBI's Attempts to Locate GOLSHAN

52. The FBI conducted searches of numerous law enforcement and publicly available databases in an attempt to determine GOLSHAN's whereabouts. No address was found during those searches, suggesting that GOLSHAN was likely living somewhere that was not rented in or associated with his name.

53. The FBI conducted surveillance at the Reseda Address to see if GOLSHAN was currently living there, but did not see him during surveillance.

54. On September 30, 2022, in Case No. 2:22-MJ-3890, United States Magistrate Judge Alexander F. MacKinnon authorized a warrant for prospective location information for GOLSHAN's cell phone.

---

[9] A verified Instagram badge is a check that appears next to an Instagram account's name. It means Instagram has confirmed that an account is the authentic presence of the public figure, celebrity, or brand it represents. Because of this, verification tends to be coveted and is a source of prestige and cachet. Instagram is the only entity that can verify an account.

55. The location data from GOLSHAN's phone indicated that GOLSHAN was primarily located near the L.A. Live entertainment complex in downtown Los Angeles. However, the FBI was unable to pinpoint his location using technological means because of the urban density and numerous large apartment towers in the area. FBI agents also canvassed the residential apartment towers in the area with photographs of GOLSHAN and contacted building management to see if GOLSHAN was staying at any of the buildings. The building managers and security guards that were contacted had no records of GOLSHAN as a registered tenant and did not recall seeing him.

J. The FBI Traces GOLSHAN to the SUBJECT PREMISES Through His IP Address

56. The FBI reviewed the IP address records from GOLSHAN's Coinbase account and his Apple iCloud account. The IP address of 162.203.153.103 was found to have accessed GOLSHAN's Coinbase account and found on Apple IP address records relating to GOLSHAN's iPhone. AT&T records, in turn, showed that this IP address resolved to a home network registered to K.D. at the SUBJECT PREMISES. The SUBJECT PREMISES was located within the area previously identified by way of the phone location warrant.

57. Subsequent Google searches and other online queries into the SUBJECT PREMISES revealed that it was an apartment located at the Hope + Flower apartment complex at 1201 S. Hope Street, Los Angeles, CA 90015.

58. On January 10, 2023, FBI agents visited the Hope + Flower apartment complex and spoke with a front desk concierge.

Agents showed him a picture of GOLSHAN without providing GOLSHAN's name. The concierge recognized GOLSHAN and stated that he had seen GOLSHAN at the apartment the day before with GOLSHAN's parents. The concierge did not know GOLSHAN's name, but believed he lived in one of the apartments "in the 30s," which was a reference to the floor range.

59. Agents then asked the concierge for information about the tenant for Apartment 3516 (the SUBJECT PREMISES, and the particular apartment to which the IP address described above was assigned). The concierge advised agents that a female named C.V. was on the lease, and GOLSHAN was listed as a registered guest for the apartment. Additional records received from the Hope + Flower apartment complex confirmed that GOLSHAN was listed as a registered guest for the SUBJECT PREMISES.

K. GOLSHAN Is Recently Seen Touring New Downtown Apartments

60. On January 13, 2023, an apartment manager at 1133 Hope Apartments contacted the FBI to inform them that he had recently seen GOLSHAN at his apartment building.[10] The apartment manager reported that GOLSHAN and unknown white male visited the apartment complex on January 10, 2023 to tour available apartments.

61. According to the apartment manager, GOLSHAN appeared to be assisting the man find a new apartment and he claimed to be the man's business partner. As part of the application

[10] FBI agents had previously spoken with this apartment manager during their canvassing. At that time, the manager did not recognize GOLSHAN's photo.

process, GOLSHAN showed the apartment manager a statement from a cryptocurrency account with a balance of over $400,000 as proof of income.

62. The investigation to date has shown that GOLSHAN has no stable job, occupation, or income. Indeed, the location data from his cell phone showed that he keeps odd hours, including apparently residing at the SUBJECT PREMISES all day while spending the night at various locations through Los Angeles. Based on GOLSHAN's lack of current or past employment, I believe that the cryptocurrency balance that GOLSHAN showed the apartment manager was likely derived from fraud and extortion schemes like those described in this affidavit.

63. In addition, based on these recent events, I believe that GOLSHAN may be attempting to move from the SUBJECT PREMISES to another apartment and is attempting to rent an apartment in the name of the unknown person.

VIII. TRAINING AND EXPERIENCE CONCERNING THE USE OF ELECTRONIC DEVICES BY SIM-SWAP FRAUDSTERS

64. Based upon my training and experience, and my conversations with other investigators, I know that SIM-swap fraud is carried out with the use of computers, SIM cards, and cell phones. I also know that SIM-swap fraudsters receive proceeds from their crimes in a variety of forms, including cryptocurrency. Fraudsters often use technological means to obfuscate the origin of funds.

65. Based on my knowledge, training, and experience, and through extensive discussions with other investigators, I have

learned the following regarding the retention of evidence, fruits, and/or instrumentalities of criminal activity:

a. Individuals, including those involved in fraud and financial-related crimes, commonly maintain records and documents. The records are necessary for the individual to keep track of their fraudulent schemes, track their income and expenses, manage their cash flow and assets, track their investments, and pay their bills. Additionally, individuals involved in fraud and financial-related crimes may maintain records and documents pertaining to their criminal activity and/or records and documents pertaining to the use and disposition of proceeds obtained through the scheme.

b. Individuals involved in fraud and financial-related crimes often maintain records for a long period of time, particularly when they are involved in ongoing criminal conduct for the following reasons:

i. To the offender, the evidence may seem innocuous on its face (e.g., financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, video recordings and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software). However, to law enforcement, such items may have significance and relevance when considered in light of other evidence.

ii. The criminal offender may no longer realize they still possess the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that they have deleted, hidden, or further destroyed evidence, such as computer-related evidence, when, in fact, the evidence may be retrievable by a trained computer forensic expert.

iii. Criminal offenders may also retain those records, in digital and/or hard copy format, when moving from one residence to another residence.

iv. Finally, I know that individuals who are engaged in fraud and/or money laundering as their primary or sole source of income are likely to continue to engage in that criminal conduct, absent an intervening factor, such as an arrest. Even after contact with law enforcement, such criminal offenders often continue to engage in fraud and/or money laundering offenses.

66. As described above, I have learned during this investigation that GOLSHAN, and his potential co-conspirators, have used email, text messages, and social media messages to communicate in furtherance of fraudulent schemes described herein. Based on my knowledge, training, and experience, and through discussions with other investigators, I have also learned the following regarding the existence of evidence on digital devices:

a. Texts, email, and online communications are integral to online fraud scams, as fraudsters often communicate

online with unwitting victims while using false identities and personas. Thus, relevant information can be expected to be located on the digital devices used for accessing texts, email, and social media applications, including cell phones, tablet computers, laptop computers, and desktop computers.

b. SIM swappers often back up electronic data to cloud-based storage systems (i.e., virtual storage located on remote servers and not on the device itself). SIM swappers then often download their data onto new electronic devices when purchased. Thus, based on my training and experience and consultations with other agents, I know that data contained on the old device could be accessible from any new digital devices purchased later. Thus, during a search of any digital devices currently in GOLSHAN's possession, agents could obtain not only new data but also any data existing at the time of the frauds previously committed in this case that had been backed up to the cloud and restored to the device.

c. Based on my training and experience, and my knowledge of this investigation, I also know that text messages and other digital communications can remain on a digital device for years. Oftentimes, whether such messages remain on a phone can depend on whether the individual using the phone has deleted the messages; if the individual has not deleted the messages or set messages to automatically delete, then the messages can remain on the phone indefinitely. In addition, when a messaging application account is activated on a new digital device, some messaging applications can download onto the new digital device

earlier conversations associated with the messaging application account conducted using other digital devices.

IX. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[11]

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

68. 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.

69. 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

[11] 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.

70. 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.

71. 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.

72. 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.

73. 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 GOLSHAN's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of GOLSHAN's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

X. CONCLUSION

74. For all the reasons described above, there is probable cause to believe that GOLSHAN violated 18 U.S.C. § 1030(a)(7) (Threatening to Damage a Protected Computer).

75. Further, 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 on GOLSHAN's person and the SUBJECT PREMISES, as described in Attachments A-1 and A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 1st day of February, 2023.

Paul L. Abrams

THE HONORABLE PAUL L. ABRAMS
UNITED STATES MAGISTRATE JUDGE