

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN JOSE

CR 26-00071-NW (NC)

FILED
Feb 18 2026
Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

(1) SAMANEH GHANDALI,

(2) MOHAMMADJAVAD KHOSRAVI,
a/k/a Mohammad Khosravi, and

(3) SOROOR GHANDALI,

DEFENDANT(S).

INDICTMENT

Count One: 18 U.S.C. § 1832(a)(5) – Conspiracy to Commit Trade Secret Theft;
Counts Two through Thirteen: 18 U.S.C. § 1832(a)(1), (2), (3), and (4) – Theft and
Attempted Theft of Trade Secrets;

Count Fourteen: 18 U.S.C. § 1512(c)(1) – Obstruction of Official Proceedings;
18 U.S.C. §§ 981(a)(1)(C), 982(b)(1), 1834, and 2323 and 28 U.S.C. § 2461(c) –
Forfeiture Allegations

A true bill.

/s/ Foreperson of the Grand Jury

Foreman

Filed in open court this 18th day of

February 2026.

Christine Farling
Clerk

L B

Bail, \$ No Bail

Hon. Laurel Beeler, U.S. Magistrate Judge

1 CRAIG H. MISSAKIAN (CABN 125202)
United States Attorney

FILED

Feb 18 2026

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN JOSE DIVISION

CR 26-00071-NW (NC)

11 UNITED STATES OF AMERICA,)	CASE NO. 5:26-cr-00071 NW
12 Plaintiff,)	<u>VIOLATIONS:</u>
13 v.)	18 U.S.C. § 1832(a)(5) – Conspiracy to Commit
14 (1) SAMANEH GHANDALI,)	Trade Secret Theft;
(2) MOHAMMADJAVAD KHOSRAVI,)	18 U.S.C. § 1832(a)(1), (2), (3), and (4) – Theft and
15 a/k/a Mohammad Khosravi, and)	Attempted Theft of Trade Secrets;
(3) SOROOR GHANDALI,)	18 U.S.C. § 1512(c)(1) – Obstruction of Official
16 Defendants.)	Proceedings;
)	18 U.S.C. §§ 981(a)(1)(C), 982(b)(1), 1834, and 2323
)	and 28 U.S.C. § 2461(c) – Forfeiture Allegations
)	SAN JOSE VENUE

18
19 INDICTMENT

20 The Grand Jury charges:

21 Introductory Allegations

22 At all times relevant to this Indictment unless otherwise specified, with all dates being
23 approximate and date ranges inclusive:

24 The Defendants

25 1. Defendant **SAMANEH GHANDALI** (“**SAMANEH**”) was an Iranian national who
26 became a U.S. citizen in or around 2018. After receiving bachelor’s and master’s degrees in computer
27 engineering and pursuing Ph.D. candidacy from universities in Iran, **SAMANEH** pursued further
28 postgraduate studies at the University of Massachusetts Amherst beginning in or around 2015 and

INDICTMENT

1 received a Ph.D. in computer engineering from this institution in or around September 2019 with a thesis
2 in “Stealthy Parametric Hardware Trojans in VLSI Circuits of Arithmetic and Cryptography Circuits.”

3 2. Defendant **MOHAMMADJAVAD KHOSRAVI** (“**KHOSRAVI**”) was an Iranian
4 national who became a U.S. legal permanent resident (“LPR”) in or around 2019. **KHOSRAVI**
5 previously served in the army of Iran, achieving the rank of Lieutenant. After receiving bachelor’s and
6 master’s degrees in computer engineering from universities in Iran with a thesis in “Secure Joint Secret
7 Sharing and Wavelet based Image Steganography Methodology,” **KHOSRAVI** pursued further
8 postgraduate studies at the University of Massachusetts Amherst beginning in or around 2017 and
9 received a Ph.D. in Computer Hardware Engineering from this institution in or around 2021.

10 **KHOSRAVI** was the husband of **SAMANEH**.

11 3. Defendant **SOROOR GHANDALI** (“**SOROOR**”) was an Iranian national present in the
12 United States on a nonimmigrant student visa. After receiving bachelor’s and master’s degrees from
13 universities in Iran in the area of computer science, **SOROOR** pursued postgraduate studies in the
14 Department of Computer Engineering from Santa Clara University beginning in or around 2020.

15 **SOROOR** was the sister of **SAMANEH** and sister-in-law of **KHOSRAVI**.

16 4. **SAMANEH, KHOSRAVI, and SOROOR** (collectively, “Defendants”) resided together
17 in San Jose, in the Northern District of California.

18 The Scheme to Commit Trade Secret Theft

19 5. Defendants **SAMANEH, KHOSRAVI, and SOROOR** conspired and agreed together
20 with each other, and others known and unknown to the Grand Jury, to knowingly:

21 a) steal, and without authorization appropriate, take, carry away, conceal, and by
22 fraud, artifice, and deception obtain trade secrets;

23 b) without authorization copy, duplicate, download, upload, alter, destroy, replicate,
24 transmit, deliver, send, communicate, and convey trade secrets; and/or

25 c) without authorization receive and possess trade secrets, knowing the same to have
26 been stolen and appropriated, obtained, and converted without authorization;

27 all with intent to convert trade secrets related to a product or service used in or intended for use in
28 interstate or foreign commerce to the economic benefit of anyone other than the owner; and intending or
knowing that the offense would injure the owner of those trade secrets.

Manner and Means

1
2 6. As part of the scheme to commit trade secret theft, Defendants gained employment at
3 leading technology companies in the area of mobile computer processors, including within the Northern
4 District of California and elsewhere.

5 7. As a further part of the scheme, Defendants obtained access to confidential and sensitive
6 information, including trade secrets related to processor security and cryptography and other
7 technologies, through their employment at technology companies, including the victim technology
8 companies described below.

9 8. As a further part of the scheme, Defendants exfiltrated confidential and sensitive
10 documents, including trade secrets related to processor security and cryptography and other
11 technologies, from certain of the victim technology companies described below to unauthorized third-
12 party and personal locations, including to locations outside the United States.

13 9. As a further part of the scheme, Defendants provided such confidential and sensitive
14 information, including trade secrets related to processor security and cryptography and other
15 technologies, without authorization to each other and/or other co-conspirators for the benefit of those
16 other than the owner of the trade secrets, and intending or knowing that doing so would injure the owner
17 of the trade secrets. For instance, Defendants accessed certain trade secrets while employed by a
18 competitor, or potential competitor, to the owner of the trade secrets.

19 10. As a further part of the scheme, Defendants utilized a third-party communications
20 application based outside of the United States (“Messenger 1”) to exfiltrate confidential and sensitive
21 documents, including trade secrets.

22 11. As a further part of the scheme, Defendants concealed and hid, and caused to be
23 concealed and hidden, the acts done and the purpose of the acts done in furtherance of the scheme,
24 including to further perpetuate the scheme. These concealments included:

- 25 a) Destroying exfiltrated files and other records of the acts from electronic devices;
- 26 b) Submitting false, signed affidavits to victim technology company representatives
27 or others about the conduct and the stolen trade secrets; and
- 28 c) Concealing the methods of exfiltration to avoid detection by the victim
technology companies (for example, manually photographing screens containing the documents’
contents instead of exfiltrating complete documents).

Victim Company 1: Google

12. Google LLC (“Google”) was a technology company headquartered in Mountain View, California. Google was a subsidiary of Alphabet Inc., one of the world’s largest technology companies by revenue. Google offered to the public a variety of products and services, including search, maps, email, cloud storage, digital payments, and productivity applications. Google also served many technology industries, offering a variety of products and services including search engine technology, online advertising, e-commerce, cloud computing, computer software, consumer electronics, artificial intelligence, and quantum computing, among other things.

13. Google’s electronic consumer products included the Google Pixel mobile smartphone, which it sold worldwide. Upon the release of the Pixel mobile smartphones in or around 2016, Google conducted significant research and development of custom silicon for the devices. In or around 2021, Google integrated and launched its custom system-on-chip (“SoC”) processors, known as Google Tensor, in its Pixel mobile smartphones.

14. Google took numerous measures to safeguard its confidential technology, information, and trade secrets. For instance, Google secured its physical space and restricted access to its buildings, including further restricting certain floors or areas within buildings. Google also secured its computer systems and network, including by restricting access to Google’s corporate network, requiring multifactor authentication, implementing access controls for certain databases or files, and monitoring certain data transfers to and from Google’s network using data loss prevention (“DLP”) systems. Google’s DLP systems logged employee computer activity, including with respect to file transfers to third-party communications platforms such as Messenger 1.

15. In or around June 2018, **SAMANEH** began work at Google as a hardware engineering intern. The internship ended in or around December 2018. In or around June 2019, **SAMANEH** began working at Google full-time as a hardware engineer. In or about April 2021, **SAMANEH** transferred within Google to a silicon security engineering role.

16. **SAMANEH** repeatedly referred **KHOSRAVI** to Google as a candidate for employment, including in or around December 2019, April 2021, August 2021, and April 2022. Beginning in or around January 2019, **KHOSRAVI** applied to Google more than forty times for various roles, including

1 in the area of processor design engineering and verification. He was not hired by Google.

2 17. **SAMANEH** also repeatedly referred **SOROOR** to Google as a candidate for
3 employment in a hardware security role, including in or around February 2021, July 2021, and March
4 2022. In or around March 2022, **SOROOR** began working at Google as an intern in an engineering
5 role.

6 18. **SAMANEH** and **SOROOR** were required to sign, and did sign, an employment
7 agreement upon their hiring at Google in or around May 2019 and March 2022, respectively. Among
8 other things, they acknowledged and agreed:

9 a) “During and after my Google employment, I will hold all Google Confidential
10 Information in strict confidence and trust. I will take all reasonable precautions to prevent any
11 unauthorized use or disclosure of Google Confidential Information, and I will not (i) use Google
12 Confidential Information . . . for any purpose other than for the benefit of Google in the scope of
my employment, or (ii) disclose Google Confidential Information to any third party without the
prior written authorization of Google.”

13 b) “Upon termination of my Google employment, I will not take with me or retain
14 any documents or materials or copies thereof containing any Google Confidential Information. I
15 agree to return all Google Property and Google Confidential Information (original, hard and
electronic copies) in my possession on or before my last day of employment and will not keep,
recreate, or deliver to any other party any Google Confidential Information or Google Property. ”

16 c) “In the scope of my Google employment, Google may release to me items
17 (including software, technology, systems, equipment, and components) subject to the Export
18 Administration Regulations (‘EAR’) or the International Traffic in Arms Regulations (‘ITAR’). I
certify that I will not export, re-export, or release these items in violation of the EAR or ITAR
and I will not disclose, export, or re-export these items to any person other than as required in the
scope of my Google employment.”

19 19. **SAMANEH** and **SOROOR** were required to sign, and did sign, a “Code of Conduct”
20 agreement upon their hiring at Google in or around July 2019 and March 2022, respectively. Among
21 other things, they agreed to “Preserve Confidentiality,” including because “company information that
22 leaks prematurely into the press or to competitors can hurt our product launches, eliminate our
23 competitive advantage and prove costly in other ways.” Specifically, they agreed to “[P]roperly secure,
24 label, and (when appropriate) dispose of Confidential Google material[.]”; “[T]ake steps to keep our
25 trade secrets and other confidential intellectual property secret.”; and “Make sure that confidential
26 company material stays that way; don’t disclose it outside of Google without authorization.”

27 20. **SAMANEH** and **SOROOR** also agreed in the “Code of Conduct” to “Obey the Law,”
28 including a section on “Trade Controls” describing that “U.S. and international trade laws control where

1 Google can send or receive its products and/or services.” Specifically, they agreed under “What
2 constitutes an . . . ‘export,’” that “transporting technical data or software on your laptop . . . in your
3 luggage . . . may be an export[.]”

4 21. **SAMANEH** and **SOROOR** received multiple trainings about Google’s policies,
5 including with respect to Google’s Code of Conduct and “Privacy and Information Security Training,”
6 among others.

7 22. During **SOROOR**’s internship, she applied for full-time employment but was not hired
8 in a full-time capacity by Google. **SOROOR**’s internship ended in or around June 2022. Later that
9 month, Google’s internal security systems detected that **SOROOR** had downloaded internal Google
10 files to a personal USB drive. **SOROOR** subsequently acknowledged in a signed affidavit that, among
11 other things:

12 a) “I have carefully and thoroughly searched all device(s), computer(s), portable
13 drives, hard copy documents, and cloud, email, and other accounts in my custody or control for
14 any documents, files, emails, and materials originating from my provision of services to Google,
without regard to whether such files or documents may or may not constitute confidential
information.”

15 b) “I have permanently removed any and all such materials from my possession by
16 permanently deleting and/or destroying all copies of such material.”

17 c) “As a result of the process described above, I no longer have access to or
18 possession, custody, or control of any copy of any documents, files, emails, and materials
originating from my provision of services to Google... If for any reason I later discover that my
19 representation on this point was not correct, I will promptly contact Google... to discuss the
situation.”

20 d) “Other than in the scope of my work duties at Google, I have not sent or
21 otherwise transferred any document, file, email, or other material originating from Google to any
other person or entity outside Google”

22 e) “I agree and promise to never use or disclose Google non-public information.”

23 23. However, **SOROOR** had transferred over 35 unique files to Messenger 1, including
24 Google trade secrets described below, from her corporate Google account between in or around March
25 2022 and in or around June 2022.

26 24. In or around July 2023, Google’s internal security systems detected that **SAMANEH** had
27 uploaded Google internal files to Messenger 1, and **SAMANEH** was interviewed by a Google
28 investigator. Google subsequently revoked **SAMANEH**’s access to Google’s systems. On or about

1 August 18, 2023, **SAMANEH** acknowledged in a signed affidavit that “I have previously uploaded
2 work-related information to [Messenger 1], including non-public Google information. I understand that
3 this was in violation of Google policies and my continuing duties as an employee. I did not share these
4 files with any other person and did not provide electronic access to these files to any other person.” She
5 further stated, among other things:

6 a) “I have not shared any non-public Google information with any third parties.”

7 b) “I have carefully and thoroughly searched all of my personal possessions,
8 including all devices, computers, portable devices, hard copy documents, and accounts
9 (including email, cloud, photo-storage, and other accounts in my custody or control) for any on-
10 public information originating from my job at Google.”

11 c) “I confirm that the information, including non-public Google information,
12 uploaded to [Messenger 1] has not been transferred, copied, downloaded, or stored beyond what
13 I have disclosed to Google representatives.”

14 d) “I have not sent or otherwise transferred any document, file, photo, email, or other
15 material originating from my provision of services to Google or otherwise learned during my
16 employment at Google to any other person or entity outside Google”

17 e) “If for any reason I later discover that I still have any documents, files, emails,
18 photos and/or materials originating from my provision of services to Google or otherwise learned
19 during my employment at Google, I will promptly contact Google to discuss and remediate the
20 situation.”

21 25. However, between in or around August 2021 and in or around July 2023, **SAMANEH**
22 had transferred more than three hundred unique files to Messenger 1, including Google trade secrets
23 described below. **SAMANEH** exfiltrated Google’s files using Messenger 1 channels titled “Samaneh’s
24 Project”, “Soroor’s Project” and/or “Sooror Asal” (term of endearment), “Mohammad’s Project” and/or
25 “Mohammad Joonam” (term of endearment).

26 26. Google did not restore **SAMANEH**’s access to Google’s systems. Google terminated
27 **SAMANEH**’s employment in or around September 2023.

28 27. Google’s trade secrets related to the Google Tensor SoC in its Pixel mobile smartphones
included the following categories, among others:

a) Architecture and design specifications pertaining to hardware security and
cryptography (“Category A”);

b) Pre-silicon evaluation materials pertaining to hardware security and cryptography
 (“Category B”);

c) Security analysis documentation, including threat models and attack plans
 (“Category C”);

1 d) Training materials describing technical details of SoC components, including the
2 machine learning accelerator (“Category D”).

3 28. Google’s Category A, B, C, and D trade secret information derived independent
4 economic value from not being generally known to, and not being readily ascertainable through proper
5 means by, other persons, such as Google’s competitors, who could obtain economic value from the
6 disclosure or use of the information.

7 Victim Company 2

8 29. Company 2 was a technology company headquartered in San Diego, California, with
9 facilities around the United States (including the Northern District of California) and world. Company 2
10 developed and commercialized foundational technologies and products used in mobile devices and other
11 wireless products, including network equipment, broadband gateway equipment and consumer
12 electronic devices, including smartphones.

13 30. Company 2’s consumer products included system-on-chip (“SoC”) platforms for
14 smartphones and other mobile devices known as “Snapdragon X1 Elite” and “Snapdragon SM8750”
15 (collectively, “Snapdragon SoCs”), which it sold worldwide.

16 31. Company 2 took numerous measures to safeguard its confidential technology,
17 information, and trade secrets. For instance, Company 2 secured its physical space and restricted access
18 to its buildings, including further restricting certain areas within buildings with badge access. Company
19 2 also secured its computer systems and network, including by restricting access to Company 2’s
20 corporate network, requiring two-factor authentication, implementing access control to certain databases
21 or files—including the Snapdragon SoC trade secret information information—and monitoring certain
22 data transfers to and from Company 2’s network using data loss prevention (“DLP”) systems. Company
23 2’s DLP systems logged employee computer activity, including with respect to tracking employee
24 Internet Protocol (“IP”) addresses used to login to company systems, and monitoring file transfers.

25 32. In or around February 2022, Company 2 hired **KHOSRAVI** in an engineering role in San
26 Diego, California. **KHOSRAVI** began working at Company 2 in or about April 2022.

27 33. **KHOSRAVI** was required to sign, and did sign in or about February 2022, an “Invention
28 Disclosure, Confidentiality & Proprietary Rights Agreement” upon his hiring at Company 2. Among

1 other things, **KHOSRAVI** acknowledged and agreed:

2 a) “I will have access to secret or confidential information, knowledge or data,
3 whether trade secrets or not, from [Company 2], including without limitation . . . matters of a
4 technical nature (such as, without limitation, any methods, know-how, formulae, compositions,
5 processes, discoveries, machines, models, devices, specifications, inventions, computer programs
6 and similar items or research projects)”

7 b) “I agree that I will not during or at any time after the termination of my
8 employment with the Company, directly or indirectly, use for myself or others, or disclose or
9 convey to others, any Confidential Information of [Company 2] . . . except as may be authorized
10 and required by the Company in the course of my employment with the Company”

11 c) “I represent and warrant that I have not brought, and will not bring or use in the
12 performance of my duties at the Company, any proprietary or confidential information, whether
13 or not in writing, of a former employer or any third party without such employer’s or third
14 party’s written authorization. I further agree not to disclose to [Company 2] in the course of my
15 employment with the Company any confidential information or trade secrets of any former
16 employer or any other third party.”

17 d) “I will not engage in any activity (including, but not limited to, outside
18 employment, . . . outside business activities or investments) that would create or give the
19 appearance of any conflict of interest between me and [Company 2]’s interest.”

20 34. **KHOSRAVI** was required to sign, and did sign in or about February 2022, a “Terms of
21 Employment” upon his hiring at Company 2. Among other things, **KHOSRAVI** identified “Iran” as his
22 country of birth and citizenship, and further acknowledged and agreed:

23 a) “The Company and its employees worldwide have a responsibility to comply with
24 all applicable export laws of the U.S. and countries where the Company conducts business. . . .
25 During my term of employment at the Company, I understand that I am required to use approved
26 [Company 2] information technology systems and processes to engage in exports, reexport, or
27 transfers, and must obtain permission from the [Company 2] Export Compliance group prior to
28 engaging in any export, reexport, or transfer of export-controlled Products.”

b) “In accordance with [Company 2]’s Export Compliance established processes, [I]
will not export, directly or indirectly, any Products obtained from [Company 2], or direct
products thereof, to any destination, person, entity or end use, prohibited or restricted under US
law without prior US government authorization (to the extent required by regulation).”

c) “[I] agree[] not to knowingly directly or indirectly export any product received
from [Company 2] to any party . . . subject to U.S. sanctions or trade restrictions, without prior
U.S. government authorization, to the extent required by regulation. The U.S. government
currently maintains comprehensive embargoes and sanctions against Cuba, Iran, North Korea,
Sudan (N), Syria and Crimea region of Ukraine, but any amendments to these controls shall
apply.”

d) “Failure to comply with U.S. export control laws may subject [Company 2] to
loss of export privileges, fines and/or criminal prosecution.”

35. **KHOSRAVI** was required to sign, and did sign in or about April 2022, a “Hand Carry
Policy for International Travel” as an employee of Company 2. Among other things, **KHOSRAVI**

1 acknowledged and agreed:

2 a) “No Company owned item may be taken into or accessed from an embargoed or
3 sanctioned country. This includes laptops, smartphones, or any other Company issued item.
4 Also, you may not conduct any Company business (including participation in a business-related
5 phone call or responding to email) while in an embargoed country. Embargoed destinations
6 currently include: Cuba; Iran; North Korea; Sudan; Syria; Crimea region of Ukraine.”

7 b) “Failure to comply with international customs laws, regulations, and/or this Policy
8 may subject [Company 2] and its employees to fines, penalties, forfeiture of items, the loss of
9 import privileges, and/or criminal prosecution.”

10 36. **KHOSRAVI** received multiple trainings about Company 2’s policies, including “The
11 [Company 2] Way: Our Code of Business Conduct” and “Export & Sanctions Compliance Engineering
12 & Program Management Course,” which specifically called out Iran as a sanctioned destination.

13 37. In or around August 2023, Company 2 approved **KHOSRAVI**’s request for a location
14 change from San Diego to Santa Clara, California, within the Northern District of California.

15 38. Company 2 terminated **KHOSRAVI**’s employment in or around August 2025.

16 39. Company 2’s trade secrets related to the Snapdragon SoCs included, among other things:
17 (i) hardware architecture and microarchitecture specifications relating to performance, security, and
18 other features (“Category i”); and (ii) security high-level architecture specifications relating to
19 cryptography and other features (“Category ii”). This Snapdragon SoC trade secret information derived
20 independent economic value from not being generally known to, and not being readily ascertainable
21 through proper means by, other persons, such as Company 2’s competitors, who could obtain economic
22 value from the disclosure or use of the information.

23 Victim Company 3

24 40. Company 3 was a technology company headquartered in Santa Clara, California.
25 Company 3 designed and manufactured advanced integrated digital technology platforms consisting of a
26 microprocessor and chipset that may be enhanced by additional hardware, software, and services.

27 Company 3’s platforms were used in a wide range of applications, such as personal computers, servers,
28 tablets, smartphones, automobiles, automated factory systems, and medical devices. Company 3 also
developed and sold software and services focused on security and technology integration.

41. In or around November 2022, **SOROOR** began working as a hardware engineer at
Company 3. In or around May 2024, **SAMANEH** began working as a security research engineer at

1 Company 3.

2 42. **SOROOR** and **SAMANEH** received multiple trainings about Company 3’s Code of
3 Conduct and protecting Company 3 confidential information, including because such information “gives
4 [Company 3] a competitive advantage.” Company 3’s Code of Conduct stated, among other things:
5 “We don’t misuse or steal [Company 3] assets (including scrap or obsolete material) or confidential
6 information or those of our business partners, disclose confidential information entrusted to us without
7 proper authorization, or put the security of our assets in jeopardy” and “You must protect [Company 3]’s
8 confidential information as well as the confidential information of our customers and business partners.
9 Disclosure of confidential information requires a clear business need and authorization.”

10 43. **SOROOR**’s employment with Company 3 ended in or around November 2024.
11 **SAMANEH**’s employment with Company 3 ended in or around April 2025.

12 Overt Acts

13 *Overt Acts During Google Employment*

14 44. Between in or around August 2021 and in or around November 2021, **SAMANEH**
15 uploaded and transmitted Google confidential information without authorization from Google to
16 “Samaneh’s Project” in Messenger 1, including documents in Google trade secret Category A (A-1, A-2,
17 A-4, A-5, A-6, A-7, A-8) and Category C (C-1, C-5).

18 45. Between in or around March 2022 and in or around April 2022, **SAMANEH** uploaded
19 and transmitted Google confidential information without authorization from Google to Messenger 1,
20 including to “Samaneh’s Project” documents in Google trade secret Category A (A-1), Category C (C-4,
21 C-5); and to “Soroor’s Project” including documents in Category C (C-3, C-6).

22 46. On or about April 10, 2022, **SOROOR** uploaded and transmitted Google confidential
23 information without authorization from Google to “Soroor’s Project” in Messenger 1, which was
24 accessible by **SAMANEH** and/or **KHOSRAVI**, including documents in Google trade secret Category C
25 (C-2, C-3).

26 47. On or about the same day, April 10, 2022, a personal laptop with the username “mjkho”
27 associated with **SAMANEH** and **KHOSRAVI** accessed Google confidential information stored in the
28 Messenger 1 “Downloads” folder of the device, including documents in Google trade secret Category C

1 (C-2).

2 48. On or about May 5 and 6, 2022 **SOROOR** uploaded and transmitted Google confidential
3 information without authorization from Google to “Soroor’s Project” and “Sooror Asal” in Messenger 1,
4 which were accessible by **SAMANEH** and/or **KHOSRAVI**, including Google trade secret Category D
5 (D-1, D-2).

6 49. On or about May 6, 2022, while employed by Company 2, **KHOSRAVI** received and
7 possessed Google confidential information without authorization from Google on his Company 2 work
8 laptop, including filenames matching documents in Google trade secret Category A (A-1).

9 50. On or about June 7, 2022, **SOROOR** signed an affidavit attesting that she had searched
10 all devices and accounts for Google materials, permanently removed such materials such that she no
11 longer had access to such materials, and that if she later discovered anything to the contrary she would
12 promptly contact Google, among other things.

13 51. On or about July 14, 2022, **SAMANEH** uploaded and transmitted Google confidential
14 information without authorization from Google to “Samaneh’s Project” in Messenger 1, including
15 documents in Google trade secret Category C (C-2).

16 52. On or about August 18, 2022, while employed by Company 2, **KHOSRAVI** received and
17 possessed Google confidential information without authorization from Google on his Company 2 work
18 laptop, including filenames matching documents in Google trade secret Category D (D-1).

19 53. On or about December 1, 2022, while employed by Company 2, **KHOSRAVI** received
20 and possessed Google confidential information without authorization from Google on his Company 2
21 work laptop, including filenames matching documents in Google trade secret Category C (C-1, C-4, C-
22 5).

23 54. On or about January 4, 2023, **SAMANEH** uploaded and transmitted Google confidential
24 information without authorization from Google to “Samaneh’s Project” in Messenger 1, including
25 documents in Google trade secret Category A (A-1, A-3) and Category C (C-5, C-6).

26 55. Between in and around January 2023 and in or around February 2023, **KHOSRAVI**
27 received and possessed Google confidential information without authorization from Google on his
28 Company 2 work laptop, including filenames matching documents in Google trade secret Category A

1 (A-1, A-3).

2 56. On or about April 24, 2023, while employed by Company 2, **KHOSRAVI** received and
3 possessed Google confidential information without authorization from Google on his Company 2 work
4 laptop, including filenames matching documents in Google trade secret Category C (C-2, C-3).

5 57. Between on or about July 12, 2023 and on or about July 25, 2023, **SAMANEH** uploaded
6 and transmitted Google confidential information without authorization from Google to Messenger 1 to
7 “Samaneh’s Project” including documents in Google trade secret Category B (B-1, B-2, B-3) and
8 Category C (C-1); and to “Soroor’s Project” including documents in Google trade secret Category C (C-
9 5).

10 58. On or about July 16, 2023, while employed by Company 3, **SOROOR** received and
11 possessed Google confidential information without authorization from Google on her Company 3 work
12 laptop, including documents in Google trade secret Category B (B-1, B-2, B-3) and Category C (C-1).

13 59. Between on or about July 21, 2023 and July 25, 2023, **SAMANEH** uploaded and
14 transmitted Google confidential information without authorization from Google to “Samaneh’s Project”
15 in Messenger 1.

16 *Overt Acts Following Google’s Detection of Theft*

17 60. In or around August 2023, **KHOSRAVI** requested a Company 2 location change from
18 San Diego to Santa Clara, California, which was approved on or about August 16, 2023.

19 61. Following an interview with a Google investigator on or about July 27, 2023,
20 **SAMANEH** signed an affidavit on or about August 18, 2023 attesting that she had searched all devices
21 and accounts for Google materials, that she had not sent such materials to anyone outside Google, and
22 that if she later discovered she still had Google materials she would promptly contact Google, among
23 other things.

24 62. On or about August 18, 2023, the same date that **SAMANEH** signed the Google affidavit
25 described above, the personal laptop with the username “mjkho” associated with **SAMANEH** and
26 **KHOSRAVI** conducted online searches about, among other things, deleting Messenger 1, “how to clear
27 history of app on iphone,” “how to remove phone from my device google,” how many days Messenger 1
28 kept deleted files, and how long a cell phone provider kept “messages to print out for court.”

1 63. On or about that same day, the same laptop also visited web sites regarding, among other
2 things, “does deleting a [Messenger 1] account immediately ...,” and “how to clear [Messenger 1] cache
3 on your Mac and iPhone.” In the following days, the same laptop visited sites regarding, among other
4 things, “can [cell phone provider] print out messages,” “does deleting a [Messenger 1] account
5 immediately delete all the data about a user in [Messenger 1]’s cloud/database.”

6 64. On or about August 23, 2023, over several hours, the same laptop with the username
7 “mjkho” associated with **SAMANEH** and **KHOSRAVI** accessed Google confidential information
8 stored in the Messenger 1 “Downloads” folder, including documents in Google trade secret Category A
9 (including A-4, A-5, A-6, A-7) and Category C (including C-6).

10 65. Beginning on or about the same day, August 23, 2023 and continuing through in or
11 around March 2024, **SAMANEH**’s Apple iPhone manually photographed **KHOSRAVI**’s physical
12 computer screens showing Company 2 confidential information. For instance, at least approximately 20
13 photographs of physical computer screens showing Company 2 materials were captured on
14 **SAMANEH**’s Apple iPhone between August 23 and August 24, 2023.

15 66. In or about September 2023, the personal laptop with the username “mjkho” associated
16 with **SAMANEH** and **KHOSRAVI** conducted online searches about, among other things, “command
17 windows to prevent data recovery,” “when type a program in search windows some files are shown as
18 recently how I can clear this list,” “clear list of recent filename windows 11,” and “microsoft one drive
19 how many days store deleted data.”

20 67. On December 6, 2023, between approximately 10:30 pm and 11:15 pm, **SAMANEH**’s
21 Apple iPhone was used to manually capture approximately 24 photographs of **KHOSRAVI**’s computer
22 screens containing Company 2 confidential information related to Company 2’s Snapdragon SoCs,
23 including Company 2 Category ii trade secret information.

24 68. The next day, on December 7, 2023, **SAMANEH** and **KHOSRAVI** traveled from San
25 Francisco to Iran via Istanbul, Turkey. While in Iran, on or about December 16, 2023, at least
26 approximately 19 of photographs previously captured of **KHOSRAVI**’s Company 2 computer screens
27 were accessed from **SAMANEH**’s Apple Macbook Pro laptop device, including Company 2 Category ii
28 trade secret information. While in Iran, including between on or about December 14 and on or about

1 December 19, **KHOSRAVI** further accessed and/or downloaded Company 2 confidential information,
2 including trade secrets contained in Company 2 Category i.

3 69. On or about December 21, 2023, while **SAMANEH** and **KHOSRAVI** remained in Iran,
4 another personal laptop associated with **SAMANEH** retained screenshots of Windows prompts
5 regarding deleting the device's files and storage, and reinstalling Windows.

6 *Court-Authorized Search Warrant in March 2024*

7 70. On March 26, 2024, the Federal Bureau of Investigation (FBI) executed a court-
8 authorized search warrant at the residence of **SAMANEH**, **KHOSRAVI**, and **SOROOR**, seizing their
9 electronic devices and other evidence. Among other things, a personal laptop seized by the FBI with the
10 username "mjkho" associated with **SAMANEH** and **KHOSRAVI** contained Google confidential
11 information including documents in Google trade secret Category A (A-1, A-2, A-4, A-5, A-6, A-7, and
12 A-8), Category C (C-1, C-2, C-3, C-4, C-5, C-6), and Category D (D-1, D-2). The device further
13 contained computer system artifacts associated with a Messenger 1 "Downloads" folder showing Google
14 confidential information had been accessed from the device, including on or about April 10, 2022 and on
15 or about August 24, 2023.

16 71. A personal laptop seized by the FBI with the username "samanehghandali" contained
17 more than 800 manually-captured photographs of computer screens containing Google or Company 2
18 material, including the photographs captured the night before **SAMANEH** and **KHOSRAVI** traveled to
19 Iran on December 6, 2023 (containing Company 2 Category ii trade secret information).

20 72. An external hard drive seized by the FBI from the closet of **SAMANEH** and
21 **KHOSRAVI**'s bedroom contained Google confidential information, including documents in Google
22 trade secret Category C (C-2, C-3, C-6) and Category D (D-1, D-2).

23 73. The non-Google work laptop of **SOROOR** seized by the FBI contained Google
24 confidential information including documents in Google trade secret Category B (B-1, B-2, B-3) and
25 Category C (C-1).

26 74. The non-Google work laptop of **KHOSRAVI** seized by the FBI contained artifacts
27 indicating the prior presence of Google confidential information including documents in Google trade
28 secret Category A (A-1, A-3), Category C (C-1, C-2, C-3, C-4, C-5), and Category D (D-1).

1 75. The mobile phones of **SAMANEH, SOROOR,** and **KHOSRAVI** seized by the FBI each
2 contained partially matching gaps in communications amongst one another between the dates of August
3 and December 2023.

4 76. **SAMANEH**'s mobile phone also contained numerous manually-captured photographs of
5 computer screens showing Company 2 confidential information, including one or more of the
6 photographs taken the evening of December 6, 2023 containing trade secrets in Company 2 Category ii.

7 77. **SOROOR**'s mobile phone also previously contained at least one document marked
8 "[Company 3] Confidential," which was recovered from deleted data.

9
10 COUNT ONE: (18 U.S.C. § 1832(a)(5) – Conspiracy to Commit Trade Secret Theft)

11 78. Paragraphs 1 through 77 of this Indictment are re-alleged and incorporated herein.

12 79. Beginning on a date unknown, but no later than in or around August 2021, and
13 continuing through at least in or around March 2024, in the Northern District of California and
14 elsewhere, the defendants,

15 **SAMANEH GHANDALI,**
16 **MOHAMMADJAVAD KHOSRAVI, and**
SOROOR GHANDALI,

17 together with others known and unknown to the Grand Jury, knowingly and with intent to convert a
18 trade secret that was related to a product and service used in and intended for use in interstate and
19 foreign commerce, conspired to:

20 a) steal, and without authorization appropriate, take, carry away, conceal, and by
21 fraud, artifice, and deception obtain trade secrets;

22 b) without authorization copy, duplicate, download, upload, alter, destroy, replicate,
transmit, deliver, send, communicate, and convey trade secrets; and

23 c) without authorization receive and possess trade secrets, knowing the same to have
24 been stolen and appropriated, obtained, and converted without authorization;

25 to the economic benefit of anyone other than the owner of those trade secrets, and intending and
26 knowing that the offense would injure any owner of those trade secrets, all in violation of Title 18,
27 United States Code, Section 1832(a)(5).
28

1 COUNTS TWO THROUGH THIRTEEN: (18 U.S.C. § 1832(a)(1), (2), (3), and (4) – Theft and
2 Attempted Theft of Trade Secrets)

3 80. Paragraphs 1 through 77 of this Indictment are re-alleged and incorporated herein.

4 81. On or about the dates set forth below, all being approximate, in the Northern District of
5 California and elsewhere, the defendant(s) set forth below, intending to convert a trade secret that was
6 related to a product and service used in and intended for use in interstate and foreign commerce, to the
7 economic benefit of anyone other than the owner of that trade secret, and intending and knowing that the
8 offense would injure the owner of that trade secret, a) knowingly stole, and without authorization
9 appropriated, took, carried away, concealed, and by fraud, artifice, and deception obtained trade secrets;
10 b) knowingly and without authorization copied, duplicated, downloaded, uploaded, altered, destroyed,
11 replicated, transmitted, delivered, sent, communicated, and conveyed trade secrets; and c) knowingly
12 and without authorization received and possessed trade secrets, knowing the same to have been stolen
13 and appropriated, obtained, and converted without authorization; and attempted to do so, as specifically
14 alleged in each of the counts below:

Count	Defendant(s)	Date(s)	Action(s)	Trade Secret(s)
2	SAMANEH GHANDALI	Between August 2021 and July 2023	Uploaded to Messenger 1 and transmitted	Google Category A (A-1 through A-8)
3	SAMANEH GHANDALI	July 2023	Uploaded to Messenger 1 and transmitted	Google Category B (B-1 through B-3)
4	SAMANEH GHANDALI	Between August 2021 and July 2023	Uploaded to Messenger 1 and transmitted	Google Category C (C-1 through C-6)
5	SOROOR GHANDALI	April 10, 2022	Uploaded to Messenger 1 and transmitted	Google Category C (including C-2, C-3)
6	SOROOR GHANDALI	May 5 and 6, 2022	Uploaded to Messenger 1 and transmitted	Google Category D (D-1 through D-2)
7	MOHAMMADJAVAD KHOSRAVI	Between May 2022 and February 2023	Received, duplicated, and possessed on non-Google work laptop	Google Category A (including A-1, A-3)
8	MOHAMMADJAVAD KHOSRAVI	August 18, 2022	Received, duplicated, and possessed on non-Google work laptop	Google Category D (including D-1)

Count	Defendant(s)	Date(s)	Action(s)	Trade Secret(s)
9	MOHAMMADJAVAD KHOSRAVI	Between December 2022 and April 2023	Received, duplicated, and possessed on non-Google work laptop	Google Category C (including C-1, C-2, C-3, C-4, C-5)
10	SOROOR GHANDALI	July 16, 2023	Received, downloaded, and possessed on non-Google work laptop	Google Category B (including B-1, B-2, B-3)
11	SOROOR GHANDALI	July 16, 2023	Received, downloaded, and possessed on non-Google work laptop	Google Category C (including C-1)
12	SAMANEH GHANDALI and MOHAMMADJAVAD KHOSRAVI	Between December 6 and 16, 2023	Duplicated and accessed on non-Company 2 devices	Company 2 Category ii
13	MOHAMMADJAVAD KHOSRAVI	Between December 14 and 19, 2023	Downloaded and accessed	Company 2 Category i

All in violation of Title 18, United States Code, Section 1832(a)(1), (2), (3), and (4).

COUNT FOURTEEN: (18 U.S.C. § 1512(c)(1) – Obstruction of Official Proceedings)

82. Paragraphs 1 through 77 of this Indictment are re-alleged and incorporated herein.

83. Between in or around August 2023 and in or around December 2023, in the Northern District of California and elsewhere, the defendants,

**SAMANEH GHANDALI,
MOHAMMADJAVAD KHOSRAVI, and
SOROOR GHANDALI**

did corruptly alter, destroy, mutilate, and conceal a record, document, and other object, to wit, communications and documents on electronic devices, and attempt to do so, with the intent to impair the object’s integrity and availability for use in an official proceeding, to wit, proceedings before a district court of the United States and grand jury proceedings regarding the theft of trade secrets, in violation of Title 18, United States Code, Section 1512(c)(1).

1 FORFEITURE ALLEGATION: (18 U.S.C. § 981(a)(1)(C), 982(b)(1), 1834, 2323, and 28 U.S.C.
2 § 2461(c))

3 84. The allegations contained above are hereby re-alleged and incorporated by reference for
4 the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C),
5 982(b)(1), 1834, and 2323, Title 21, United States Code, Section 853(a), and Title 28, United States
6 Code, Section 2461(c).

7 85. Upon conviction of any of the offenses alleged in Counts One through Thirteen above,
8 the defendants,

9 **SAMANEH GHANDALI,**
10 **MOHAMMADJAVAD KHOSRAVI, and/or**
11 **SOROOR GHANDALI**

12 shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 1834 and 2323, any
13 property used, or intended to be used, in any manner or part to commit or facilitate the commission of
14 the offenses, and any property constituting or derived from any proceeds obtained directly or indirectly
15 as a result of the commission of the offenses, including but not limited to the following property:

- 16 a) One Apple iPhone 14 Pro, serial number JJ726XH9LY;
- 17 b) One Apple iPhone 14 Pro, serial number P2GHQK7GGN;
- 18 c) One HP Envy laptop, serial number 8CG94122OZ;
- 19 d) One Apple Macbook Pro, serial number M2NY2XF126;
- 20 e) One Dell XPS laptop, serial number 6BBRGH2;
- 21 f) One Lenovo Slim 7 laptop, serial number PF4GSJLC;
- 22 g) One HP laptop, serial number 5CG2287LTW;
- 23 h) One Lenovo Thinkpad laptop, serial number PC296RJ2 ;
- 24 i) One Apple iPhone, serial number VMDGNWXF22;
- 25 j) One ASUS laptop, serial number DAN0CX583711439;
- 26 k) One Seagate hard drive, serial number NAD31YBR; and
- 27 l) One Apple Macbook laptop, serial number FVFHJ32CQ6LC.

28 86. Upon conviction of the offense alleged in Count Fourteen above, the defendants,

SAMANEH GHANDALI,
MOHAMMADJAVAD KHOSRAVI, and
SOROOR GHANDALI

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: [] COMPLAINT [] INFORMATION [X] INDICTMENT [] SUPERSEDING

OFFENSE CHARGED

- 18 U.S.C. § 1832(a)(5) - Conspiracy to Commit Trade Secret Theft (Count 1);
18 U.S.C. § 1832(a)(1), (2), (3), and (4) - Theft and Attempted Theft of Trade Secrets (Counts 2-4, 12);
18 U.S.C. § 1512(c)(1) - Obstruction of Official Proceedings (Count 14)
[] Petty
[] Minor
[] Misdemeanor
[X] Felony

PENALTY: Counts 1, 2-4, 12 (each): 10 years of imprisonment, \$250,000 fine, 3 years of supervised release; \$100 mandatory special assessment
Count 14: 20 years of imprisonment, \$250,000 fine, 3 years of supervised release; \$100 mandatory special assessment

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DEFENDANT - U.S.

Samaneh GHANDALI

DISTRICT COURT NUMBER
5:26-cr-00071 NW

CR 26-00071-NW (NC)

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Federal Bureau of Investigation

[] person is awaiting trial in another Federal or State Court, give name of court

[] this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

[] this is a reprosecution of charges previously dismissed which were dismissed on motion of:
[] U.S. ATTORNEY [] DEFENSE } SHOW DOCKET NO.

[] this prosecution relates to a pending case involving this same defendant } MAGISTRATE CASE NO.

[] prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under }

Name and Office of Person Furnishing Information on this form Craig Missakian

[X] U.S. Attorney [] Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) Eric Cheng, Casey Boome

DEFENDANT

IS NOT IN CUSTODY

- Has not been arrested, pending outcome this proceeding.
1) [] If not detained give date any prior summons was served on above charges
2) [] Is a Fugitive
3) [] Is on Bail or Release from (show District)

IS IN CUSTODY

- 4) [] On this charge
5) [] On another conviction } [] Federal [] State
6) [] Awaiting trial on other charges
If answer to (6) is "Yes", show name of institution

Has detainer been filed? [] Yes [] No } If "Yes" give date filed

DATE OF ARREST Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

[] This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

[] SUMMONS [] NO PROCESS* [X] WARRANT

Bail Amount: No Bail

If Summons, complete following:

[] Arraignment [] Initial Appearance

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Defendant Address:

Date/Time: Before Judge:

Comments:

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: [] COMPLAINT [] INFORMATION [X] INDICTMENT [] SUPERSEDING

OFFENSE CHARGED

- 18 U.S.C. § 1832(a)(5) - Conspiracy to Commit Trade Secret Theft (Count 1);
18 U.S.C. § 1832(a)(1), (2), (3), and (4) - Theft and Attempted Theft of Trade Secrets (Counts 7-9, 12-13);
18 U.S.C. § 1512(c)(1) - Obstruction of Official Proceedings (Count 14)
[] Petty
[] Minor
[] Misdemeanor
[X] Felony

PENALTY: Counts 1, 7-9, 12-13 (each): 10 years of imprisonment, \$250,000 fine, 3 years of supervised release; \$100 mandatory special assessment
Count 14: 20 years of imprisonment, \$250,000 fine, 3 years of supervised release; \$100 mandatory special assessment

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DEFENDANT - U.S

Mohammadjavad KHOSRAVI aka Mohammad KHOSRAVI

DISTRICT COURT NUMBER

5:26-cr-00071 NW

CR 26-00071-NW (NC)

DEFENDANT

IS NOT IN CUSTODY

Has not been arrested, pending outcome this proceeding.

- 1) [] If not detained give date any prior summons was served on above charges
2) [] Is a Fugitive
3) [] Is on Bail or Release from (show District)

IS IN CUSTODY

- 4) [] On this charge
5) [] On another conviction } [] Federal [] State
6) [] Awaiting trial on other charges
If answer to (6) is "Yes", show name of institution

Has detainer been filed? [] Yes [] No } If "Yes" give date filed

DATE OF ARREST Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

[] This report amends AO 257 previously submitted

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Federal Bureau of Investigation

[] person is awaiting trial in another Federal or State Court, give name of court

[] this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

this is a reprosecution of charges previously dismissed which were dismissed on motion of: [] U.S. ATTORNEY [] DEFENSE } SHOW DOCKET NO.

this prosecution relates to a pending case involving this same defendant } MAGISTRATE CASE NO.

[] prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under }

Name and Office of Person Furnishing Information on this form Craig Missakian

[X] U.S. Attorney [] Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) Eric Cheng, Casey Boome

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

[] SUMMONS [] NO PROCESS* [X] WARRANT

Bail Amount: No Bail

If Summons, complete following:

[] Arraignment [] Initial Appearance

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Defendant Address:

Date/Time: Before Judge:

Comments:

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: [] COMPLAINT [] INFORMATION [X] INDICTMENT [] SUPERSEDING

OFFENSE CHARGED

- 18 U.S.C. § 1832(a)(5) - Conspiracy to Commit Trade Secret Theft (Count 1);
18 U.S.C. § 1832(a)(1), (2), (3), and (4) - Theft and Attempted Theft of Trade Secrets (Counts 5-6, 10-11);
18 U.S.C. § 1512(c)(1) - Obstruction of Official Proceedings (Count 14)
[] Petty
[] Minor
[] Misdemeanor
[X] Felony

PENALTY: Counts 1, 5-6, 10-11 (each): 10 years of imprisonment, \$250,000 fine, 3 years of supervised release; \$100 mandatory special assessment
Count 14: 20 years of imprisonment, \$250,000 fine, 3 years of supervised release; \$100 mandatory special assessment

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

DEFENDANT - U.S.

Soroor GHANDALI

DISTRICT COURT NUMBER

5:26-cr-00071 NW

CR 26-00071-NW (NC)

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Federal Bureau of Investigation

[] person is awaiting trial in another Federal or State Court, give name of court

[] this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

[] this is a re prosecution of charges previously dismissed which were dismissed on motion of:
[] U.S. ATTORNEY [] DEFENSE } SHOW DOCKET NO.

[] this prosecution relates to a pending case involving this same defendant } MAGISTRATE CASE NO.

[] prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under }

Name and Office of Person Furnishing Information on this form Craig Missakian

[X] U.S. Attorney [] Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) Eric Cheng, Casey Boome

DEFENDANT

IS NOT IN CUSTODY

- Has not been arrested, pending outcome this proceeding.
1) [] If not detained give date any prior summons was served on above charges
2) [] Is a Fugitive
3) [] Is on Bail or Release from (show District)

IS IN CUSTODY

- 4) [] On this charge
5) [] On another conviction } [] Federal [] State
6) [] Awaiting trial on other charges
If answer to (6) is "Yes", show name of institution

Has detainer been filed? [] Yes [] No } If "Yes" give date filed

DATE OF ARREST Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

[] This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

[] SUMMONS [] NO PROCESS* [X] WARRANT

Bail Amount: No Bail

If Summons, complete following:

[] Arraignment [] Initial Appearance

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Defendant Address:

Date/Time: Before Judge:

Comments: