United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN JOSE

CR 26-00071-NW (NC)

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.

Clerk

Bail, $ No Bail

Hon. Laurel Beeler, U.S. Magistrate Judge

CRAIG H. MISSAKIAN (CABN 125202)
United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

CR 26-00071-NW (NC)

UNITED STATES OF AMERICA, Plaintiff, v. (1) SAMANEH GHANDALI, (2) MOHAMMADJAVAD KHOSRAVI, a/k/a Mohammad Khosravi, and (3) SOROOR GHANDALI, Defendants.	CASE NO. 5:26-cr-00071 NW VIOLATIONS: 18 U.S.C. § 1832(a)(5) – Conspiracy to Commit Trade Secret Theft; 18 U.S.C. § 1832(a)(1), (2), (3), and (4) – Theft and Attempted Theft of Trade Secrets; 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 SAN JOSE VENUE

INDICTMENT

The Grand Jury charges:

Introductory Allegations

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

The Defendants

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

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

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

3. Defendant **SOROOR GHANDALI** ("**SOROOR**") was an Iranian national present in the United States on a nonimmigrant student visa. After receiving bachelor's and master's degrees from universities in Iran in the area of computer science, **SOROOR** pursued postgraduate studies in the Department of Computer Engineering from Santa Clara University beginning in or around 2020. **SOROOR** was the sister of **SAMANEH** and sister-in-law of **KHOSRAVI**.

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

The Scheme to Commit Trade Secret Theft

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

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

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

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

all with intent to convert trade secrets related to a product or service used in or intended for use in 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

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

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

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

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

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

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

a) Destroying exfiltrated files and other records of the acts from electronic devices;

b) Submitting false, signed affidavits to victim technology company representatives or others about the conduct and the stolen trade secrets; and

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

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

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

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

> a) "During and after my Google employment, I will hold all Google Confidential Information in strict confidence and trust. I will take all reasonable precautions to prevent any unauthorized use or disclosure of Google Confidential Information, and I will not (i) use Google 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."
>
> b) "Upon termination of my Google employment, I will not take with me or retain any documents or materials or copies thereof containing any Google Confidential Information. I 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. "
>
> c) "In the scope of my Google employment, Google may release to me items (including software, technology, systems, equipment, and components) subject to the Export 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. **SAMANEH** and **SOROOR** were required to sign, and did sign, a "Code of Conduct" agreement upon their hiring at Google in or around July 2019 and March 2022, respectively. Among other things, they agreed to "Preserve Confidentiality," including because "company information that leaks prematurely into the press or to competitors can hurt our product launches, eliminate our competitive advantage and prove costly in other ways." Specifically, they agreed to "[P]roperly secure, label, and (when appropriate) dispose of Confidential Google material[.]"; "[T]ake steps to keep our trade secrets and other confidential intellectual property secret."; and "Make sure that confidential company material stays that way; don't disclose it outside of Google without authorization."

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

Google can send or receive its products and/or services." Specifically, they agreed under "What constitutes an . . . 'export'," that "transporting technical data or software on your laptop . . . in your luggage . . . may be an export[.]"

21. **SAMANEH** and **SOROOR** received multiple trainings about Google's policies, including with respect to Google's Code of Conduct and "Privacy and Information Security Training," among others.

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

a) "I have carefully and thoroughly searched all device(s), computer(s), portable drives, hard copy documents, and cloud, email, and other accounts in my custody or control for 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."

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

c) "As a result of the process described above, I no longer have access to or 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 representation on this point was not correct, I will promptly contact Google… to discuss the situation."

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

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

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

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

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

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

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

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

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

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

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

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

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");

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

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

Victim Company 2

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

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

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

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

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

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

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

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

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

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

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

a) "The Company and its employees worldwide have a responsibility to comply with all applicable export laws of the U.S. and countries where the Company conducts business. . . . During my term of employment at the Company, I understand that I am required to use approved [Company 2] information technology systems and processes to engage in exports, reexport, or transfers, and must obtain permission from the [Company 2] Export Compliance group prior to 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**

acknowledged and agreed:

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

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

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

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

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

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

Victim Company 3

40. Company 3 was a technology company headquartered in Santa Clara, California. Company 3 designed and manufactured advanced integrated digital technology platforms consisting of a microprocessor and chipset that may be enhanced by additional hardware, software, and services. Company 3's platforms were used in a wide range of applications, such as personal computers, servers, 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

Company 3.

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

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

Overt Acts

Overt Acts During Google Employment

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

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

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

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

(C-2).

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

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

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

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

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

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

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

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

(A-1, A-3).

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

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

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

59. Between on or about July 21, 2023 and July 25, 2023, **SAMANEH** uploaded and transmitted Google confidential information without authorization from Google to "Samaneh's Project" in Messenger 1.

Overt Acts Following Google's Detection of Theft

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

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

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

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

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

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

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

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

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

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

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

Court-Authorized Search Warrant in March 2024

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

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

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

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

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

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

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

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

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

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

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

SAMANEH GHANDALI,
MOHAMMADJAVAD KHOSRAVI, and
SOROOR GHANDALI,

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

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

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

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

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

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

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

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

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

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

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

SAMANEH GHANDALI,
MOHAMMADJAVAD KHOSRAVI, and/or
SOROOR GHANDALI

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

a) One Apple iPhone 14 Pro, serial number JJ726XH9LY;

b) One Apple iPhone 14 Pro, serial number P2GHQK7GGN;

c) One HP Envy laptop, serial number 8CG94122OZ;

d) One Apple Macbook Pro, serial number M2NY2XF126;

e) One Dell XPS laptop, serial number 6BBRGH2;

f) One Lenovo Slim 7 laptop, serial number PF4GSJLC;

g) One HP laptop, serial number 5CG2287LTW;

h) One Lenovo Thinkpad laptop, serial number PC296RJ2 ;

i) One Apple iPhone, serial number VMDGNWXF22;

j) One ASUS laptop, serial number DAN0CX583711439;

k) One Seagate hard drive, serial number NAD31YBR; and

l) One Apple Macbook laptop, serial number FVFHJ32CQ6LC.

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

SAMANEH GHANDALI,
MOHAMMADJAVAD KHOSRAVI, and
SOROOR GHANDALI

shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), all right, title, and interest in any property constituting and derived from any proceeds defendant obtained, directly or indirectly, as a result of such violations, and including but not limited to the above-referenced property and a forfeiture money judgment.

87. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 981(a)(1)(C), 982(b)(1), and 2323(b), and Title 28, United States Code, Section 2461(c).

All pursuant to Title 18, United States Code, Sections 981, 982, 1834, and 2323, Title 21, United States Code, Section 853, Title 28, United States Code, Section 2461, and Federal Rule of Criminal Procedure 32.2.

DATED: February 18, 2026

A TRUE BILL.

/s/ Foreperson
FOREPERSON
San Francisco, California

CRAIG H. MISSAKIAN
United States Attorney

/s/ Eric Cheng
ERIC CHENG
CASEY BOOME
Assistant United States Attorneys