Apple sues OpenAI and two former employees, alleging theft of hardware trade secrets

Source copy kept by wheresthe.ai for the story “Apple sues OpenAI and two former employees, alleging theft of hardware trade secrets” (https://wheresthe.ai/d/us-apple-sues-openai-and-former-employees-over-trade-secrets-2026-07/).

Source: https://storage.courtlistener.com/recap/gov.uscourts.cand.474095/gov.uscourts.cand.474095.1.0.pdf

Text saved 29 Oct 2026 (the source PDF).

SHA-256 of the saved text: b5caf987aa6cd0d70558cc5089c9ee3eebcbb3577681eb3455eb2889f3807fbf

Documents the source offers: https://storage.courtlistener.com/recap/gov.uscourts.cand.474095/gov.uscourts.cand.474095.1.0.pdf

---

1 Gabriel S. Gross (SBN 254672) WEIL, GOTSHAL & MANGES LLP 2 201 Redwood Shores Parkway Redwood Shores, California 94065 3 Telephone: (650) 802-3000 4 Facsimile: (650) 802-3100 gabe.gross@weil.com 5 Christopher W. Henry (pro hac vice forthcoming) 6 WEIL, GOTSHAL & MANGES LLP 7 1001 Boylston Street, Suite 300 Boston, Massachusetts 02115 8 Telephone: (617) 772-8300 Facsimile: (617) 772-8333 9 chris.henry@weil.com 10 Attorneys for Plaintiff Apple Inc. 11 [Additional Counsel listed in signature block] 12

13

14 UNITED STATES DISTRICT COURT

15 NORTHERN DISTRICT OF CALIFORNIA

16 SAN JOSE DIVISION

17

18 APPLE INC., Case No.

19 Plaintiff, COMPLAINT FOR TRADE SECRET MISAPPROPRIATION AND BREACH 20 vs. OF CONTRACT 21 CHANG LIU, TANG YEW TAN, OPENAI DEMAND FOR JURY TRIAL FOUNDATION f/k/a OPENAI, INC., OPENAI 22 GROUP PBC, and IO PRODUCTS, LLC f/k/a IO 23 PRODUCTS, INC.,

24 Defendants.

25

26 27

28

1 Apple brings this action against Chang Liu and Tang Yew Tan (“Mr. Liu” and “Mr. Tan,” 2 respectively and collectively, the “Individual Defendants”), OpenAI Foundation and OpenAI Group 3 PBC (collectively, “OpenAI”), and io Products, LLC (“io”) (OpenAI and io collectively, the “Cor- 4 porate Defendants”), and alleges as follows: 5 INTRODUCTION 6 1. This case is about Apple’s former employees stealing Apple’s trade secrets for the 7 benefit of OpenAI. Apple brings this suit to put a stop to it. 8 2. Apple has invested hundreds of billions of dollars and decades of effort in developing 9 groundbreaking consumer hardware products like iPhone, Apple Watch, and MacBook, along with 10 the business acumen and infrastructure to bring them to market at scale. This sustained and focused 11 investment of time, talent, and resources has produced engineering breakthroughs, manufacturing and 12 supply chain innovations, and a global network of strategic partnerships—all built on confidentiality 13 and trust. Apple surprises and delights its customers each year with innovative new hardware prod- 14 ucts, keeping much of its work secret until the moment its finished products are ready to be revealed. 15 3. Behind the scenes, Apple keeps its product development, manufacturing, supply chain, 16 technology research, and other innovations confidential. The trade secrets spanning Apple’s hardware 17 operations collectively constitute one of the most valuable intellectual assets in all of American busi- 18 ness. They enable Apple to bring new products with unique features to consumers at extraordinary 19 speed and scale. Apple takes the confidentiality of its trade secrets seriously. In the rare situation 20 where Apple becomes aware that its confidential information may have been

compromised—by a 21 third party, a partner, an employee, or anyone else—it investigates and works to contain and resolve 22 any issues. This case arises from such an investigation. Apple has uncovered a pattern of theft of 23 Apple's trade secrets by OpenAI employees who were formerly at Apple. 24 4. Chang Liu spent eight years at Apple as a Senior System Electrical Engineer, working 25 on some of Apple's most sensitive product development programs. Apple entrusted him with highly 26 confidential and trade secret information. Mr. Liu left in January 2026 to join OpenAI. When Apple 27 contacted Mr. Liu to sign Apple's confidentiality reminder, schedule an exit interview, and confirm 28 that he had returned his devices and complied with other exit procedures, Mr. Liu did not respond.

1 5. Mr. Liu has taken steps to hide the full extent of his theft, which Apple is still investi- 2 gating, but the investigation already has revealed troubling facts: 3 • After leaving Apple, Mr. Liu failed to return an Apple-issued work laptop that he had pre- 4 viously authenticated to Apple's network. In a message left on a former colleague's Apple- 5 issued work laptop he said, "I still have another computer" on which he planned to access 6 Apple information. 7 • While employed by OpenAI, he accessed and used his former colleague's Apple-issued 8 work computer that was authenticated to Apple's network, without Apple's authorization. 9 • While employed by OpenAI, Mr. Liu also exploited a rare, previously unknown authenti- 10 cation bug to access Apple's shared network folders.1 Upon discovering that he had this 11 unauthorized access to Apple's systems, Mr. Liu did not report it, return his stolen Apple- 12 issued work laptop, or delete the program that allowed the access. 13 • Instead, he celebrated his improper access, exclaiming in a message left on his colleague's 14 Apple-issued work laptop "LOL" and that it was "so funny." Then, over several weeks, 15 while developing hardware for OpenAI, Mr. Liu surreptitiously accessed and downloaded 16 dozens of Apple's confidential hardware-related files, including voluminous, detailed in- 17 formation about unreleased products, engineering presentations, technical specifications, 18 and proprietary project data. 19 6. Messages left on an Apple-issued work laptop revealed that Mr. Liu also coached his 20 former Apple colleague (whom he was recruiting to join OpenAI) on ways to "avoid trouble with the 21 security team" when copying confidential Apple files. Knowing that OpenAI interviews would in- 22 volve discussing Apple technology, Mr. Liu advised her on which confidential Apple material about 23 unannounced Apple products she should study before her interview. To hide his illegal activity, Mr. 24 Liu directed her to communicate with him privately over a separate messaging app. 25

26 27 1 Upon discovery, Apple quickly fixed this bug. Although Apple is still investigating, server logs show that, unlike Mr. Liu, the few other users affected by this bug do not appear to have accessed or 28 stolen Apple's confidential information.

1 7. As Apple continued investigating, a broader pattern emerged. Mr. Liu was not the 2 only one using Apple's proprietary information to OpenAI's advantage. Other former Apple employ- 3 ees who had gone to work for OpenAI emailed themselves Apple's confidential information to per- 4 sonal accounts on their way out the door. And others were improperly using their knowledge of Ap- 5 ple's confidential and trade secret information to assist OpenAI in developing hardware. 6 8. Tang Yew Tan spent twenty-four years at Apple, most recently as Vice President of 7 Product Design for iPhone and Apple Watch. Today he is OpenAI's Chief Hardware Officer. Apple 8 entrusted Mr. Tan with its most sensitive projects, trusted partner relationships, proprietary manufac- 9 turing techniques, and unreleased products. Apple's investigation has revealed that Mr. Tan has been 10 methodically using Apple's confidential information to benefit OpenAI. 11 9. In the months before he left Apple, Mr. Tan met with OpenAI or its collaborators and 12 discussed meetings with a key Apple supplier. He began emailing himself information about Apple's 13 suppliers and internal summaries of the consumer electronics industry. And today, when interviewing 14 Apple employees for jobs at OpenAI, Mr. Tan uses Apple's confidential information to gain access 15 to even more insider knowledge. He has used an Apple internal project codename to ask, "What's the 16 plan[?]" for an unannounced Apple product. He has directed job candidates still working for Apple 17 to bring "Actual parts" from Apple to their interviews for "show and tell" sessions in which he and 18 his team at OpenAI can elicit still more Apple confidential information. These directions to bring 19 Apple's parts to OpenAI job interviews surprised at least one of the candidates, who commented that 20 he "didn't even know we could take those from the office." 21 10. This is part of OpenAI's strategy to extract Apple's confidential information. OpenAI 22 has been instructing Apple employees to bring "CAD/design artifacts" and "prototypes" to their in- 23 terviews and to divulge details about their work such as "subsystem and component selection," the 24 "tools or methodologies you use for system integration, such as CAD software, simulation tools," 25 and "Vendor selection and communication/collaboration with vendors." 26 11. OpenAI also instructs new hires on how to avoid scrutiny when they leave Apple. For 27 example, Mr. Tan warns them not to tell Apple that they have taken jobs at

OpenAI, so they can stay 28 at Apple as long as they can. After his own departure, Mr. Tan improperly retained or obtained an

COMPLAINT 3 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 5 of 41

1 internal Apple managers' document marked "Need to Know" that describes security procedures for 2 employee departures. Messages left on Apple-issued work devices show that Mr. Tan and his OpenAI 3 colleagues have been sharing this document with new hires before they give notice to Apple of their 4 departures, previewing Apple's security protocols. Unsurprisingly, Apple's investigation has found 5 a pattern by employees who depart for OpenAI of taking steps to evade the security processes in- 6 tended to protect Apple's confidential information. 7 12. OpenAI and its cohorts have been engaging in a coordinated pattern of misconduct at 8 an institutional level as well. This includes io (which OpenAI acquired), a venture co-founded by 9 Mr. Tan and other former Apple leaders. The Corporate Defendants, with or through their employees 10 or partners, have been acting in concert and as an enterprise, exploiting Apple's confidential infor- 11 mation to advance OpenAI's efforts to enter the consumer hardware market. They have used confi- 12 dential Apple information in approaching Apple's trusted partners, even having one carry out a spe- 13 cific trade secret metal-finishing technique for OpenAI, misleading the partner to believe they had 14 Apple's permission to do so. 15 13. This is the tip of the iceberg. Apple lacks visibility into what's been happening behind 16 closed doors at OpenAI, where such misconduct is normalized and exemplified by leadership. This 17 much is clear, however: at every level, from members of its Technical Staff to its Chief Hardware 18 Officer, and in coordination with business partners, OpenAI has been stealing Apple's trade secrets 19 and confidential information. As a natural result, OpenAI's nascent hardware business now rests on 20 the shakiest of foundations, rotten to its core by its illegal reliance on misappropriated trade secrets. 21 14. In February as its investigation was in its early stages, Apple wrote OpenAI to raise its 22 concerns that Apple's confidential information could be making its way into OpenAI's business im- 23 properly. Apple asked OpenAI to discuss what precautions OpenAI was taking to avoid this problem, 24 to investigate it, and to remediate any issues. OpenAI never responded. This necessitated Apple's 25 further investigation, revealing the alarming unlawful conduct discussed above. 26 15. Apple does not bring this action lightly. Apple operates in the most competitive mar- 27 kets in the world and focuses on creating and shipping the very best products and services that embody 28 its innovations. But it cannot tolerate the theft of its trade secrets. In light of the troubling evidence it

COMPLAINT 4 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 6 of 41

1 has seen so far, Apple is left with no choice. This lawsuit and the discovery process are needed to 2 expose and begin to remedy the pervasive theft of Apple's trade secrets. 3 PARTIES 4 16. Apple is and at all times mentioned herein has been a California corporation, having 5 its principal place of business at One Apple Park Way, Cupertino, California 95014. 6 17. Defendant Chang Liu, on information and belief, resides in Sunnyvale, California 7 94087. Mr. Liu has worked at OpenAI since January 2026. Mr. Liu worked at Apple for over eight 8 years, where he served as a Senior System Electrical Engineer for Apple's iPhone product line, and 9 executed Apple's Intellectual Property Agreement (IPA) as a condition of his employment. 10 18. Defendant Tang Yew Tan, on information and belief, resides in San Francisco, Cali- 11 fornia. Mr. Tan was a co-founder and Chief Hardware Officer of io Products, LLC, which subse- 12 quently merged with OpenAI, and now is Chief Hardware Officer at OpenAI. Mr. Tan worked at 13 Apple for over twenty-four years, where he served as Vice President of Product Design for Apple's 14 iPhone and Apple Watch product lines, and executed Apple's IPA as a condition of his employment. 15 19. OpenAI Foundation is a registered nonprofit organization incorporated under the laws 16 of Delaware, having its principal place of business as 1455 3rd Street, San Francisco, California 17 94158. 18 20. OpenAI Group PBC is a registered public benefit corporation registered under the laws 19 of Delaware, having its principal place of business as 1455 3rd Street, San Francisco, California 20 94158. OpenAI Foundation and OpenAI Group PBC, collectively, are referred to herein as OpenAI. 21 21. io Products, LLC, formerly known as io Products, Inc., is a Delaware LLC registered 22 to do business in California and having its principal place of business at 1455 3rd Street, San Fran- 23 cisco, California 94158. 24 JURISDICTION AND VENUE 25 22. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action 26 arises out of the violation of a federal law, the Defend Trade Secrets Act, 18 U.S.C. §§ 1836, et seq. 27

28

COMPLAINT 5 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 7 of 41

1 23. This Court also has supplemental jurisdiction over the asserted state law claims under 2 28 U.S.C. § 1367(a)

because the federal and state law claims derive from a common nucleus of op- 3 erative facts. 4 24. This Court has personal jurisdiction over the Individual Defendants because they reside 5 in this District and purposefully directed their activities toward residents of this District. Each Indi- 6 vidual Defendant executed an IPA with Apple that provides for personal jurisdiction in and venue in 7 the federal courts within Santa Clara County, California. Apple's claims arise out of and relate to 8 each Individual Defendant's contacts with this forum. 9 25. This Court has general personal jurisdiction over OpenAI because each OpenAI De- 10 fendant lists its principal place of business as 1455 3rd Street, San Francisco, California 94158 in its 11 most recent filings with the California Secretary of State. 12 26. This Court has specific personal jurisdiction over OpenAI because each OpenAI De- 13 fendant has purposefully directed its activities toward residents of this District and the State of Cali- 14 fornia, including by maintaining a place of business in this District, employing individuals in this 15 District, and conducting substantial and continuous business operations in this District. Apple's 16 claims arise out of and relate to each OpenAI Defendant's contacts with this forum, including each 17 OpenAI Defendant's misappropriation of Apple's trade secrets in the forum to further its own devel- 18 opment and commercialization efforts within the forum. The exercise of jurisdiction over each 19 OpenAI Defendant comports with traditional notions of fair play and substantial justice, as each 20 OpenAI Defendant is headquartered in this District, has availed itself of the privilege of conducting 21 business here, and should reasonably anticipate litigation in this forum. 22 27. This Court has general personal jurisdiction over io because io lists its principal place 23 of business as 1455 3rd Street, San Francisco, California 94158 in its most recent filings with the 24 California Secretary of State. 25 28. This Court has specific personal jurisdiction over io because io has purposefully di- 26 rected its activities toward residents of this District and the State of California, including by main- 27 taining a place of business in this District, employing individuals in this District, and conducting 28 substantial and continuous business operations in this District. Apple's claims arise out of and relate

1 to io's contacts with this forum, including io's misappropriation of Apple's trade secrets in the forum 2 to further its own development and commercialization efforts within the forum. The exercise of ju- 3 risdiction over io comports with traditional notions of fair play and substantial justice, as io is head- 4 quartered in this District, has availed itself of the privilege of conducting business here, and should 5 reasonably anticipate litigation in this forum. 6 29. This Court also has jurisdiction over io because io is an alter ego of OpenAI. By no 7 later than OpenAI's acquisition of io, io operated as a team in OpenAI to design and develop hardware 8 devices for OpenAI. io and OpenAI collectively do business as OpenAI. 9 30. Corporate filings for OpenAI and io state the same principal address. Brendan Herron, 10 the CEO, Secretary, and CFO of io, is an employee of OpenAI and has been since 2023. 11 31. Apple is informed and believes that, at all relevant times, OpenAI directed and con- 12 trolled the operations and assets of io. Specifically, OpenAI controlled all aspects of io's business 13 decisions and day-to-day operations, including the decisions to hire certain employees, conduct in- 14 terviews, contact and choose suppliers and vendors, and decide which hardware to design and de- 15 velop. Apple is informed and believes that there has been such unity of interest and ownership be- 16 tween OpenAI and io that any individuality and separateness between them did not and does not exist. 17 32. Without individually binding io in this litigation, io will be free to create another cor- 18 porate shell entity to continue to use Apple's trade secret information and other intellectual property 19 in violation of law. Therefore, adherence to the fiction of the separate existence of io and OpenAI 20 would permit abuse of any applicable privilege and promote an inequitable result. 21 33. Venue is proper pursuant to 28 U.S.C. § 1391, because Apple, Chang Liu, Tang Yew 22 Tan, each OpenAI Defendant, and io reside in this District, do substantial business in this forum, and 23 the events giving rise to this Complaint occurred in this forum. Venue is also proper for the Individual 24 Defendants, both former Apple employees, because they have signed an Intellectual Property Agree- 25 ment consenting to the personal jurisdiction of and venue in the state and federal courts within Santa 26 Clara County, California. Individual Defendants, Chang Liu and Tang Yew Tan, also committed the 27 wrongful acts within this District. 28

1 DIVISIONAL ASSIGNMENT 2 34. Pursuant to Civil Local Rule 3-2, this case should be assigned to the San Jose Division. 3 Apple's Intellectual Property Agreement, executed and breached by each of the Individual Defend- 4 ants, expressly states that "any judicial action between the parties relating to this Agreement will take 5 place in Santa Clara County, California." This is such an action. Additionally, a substantial portion 6 of the events giving rise to the claims has taken place in Santa Clara County. 7 BACKGROUND 8 I. OpenAI and Its Consumer Hardware Plans 9 35. OpenAI was founded in December 2015 as a nonprofit organization with an initial 10 funding commitment of $1 billion.2 The company's goal was "to advance digital intelligence in the 11 way that is

most likely to benefit humanity as a whole, unconstrained by a need to generate financial 12 return."3 Following the release of its now well-known artificial intelligence chatbot, ChatGPT, 13 OpenAI experienced explosive growth and transformed from a nonprofit to a commercial enterprise.4 14 The company's valuation soared from approximately $29 billion in 2023 to $852 billion by April 15 2026 and has continued growing at a rapid pace.5 By October 2025, OpenAI had abandoned its "open" 16 nonprofit philosophy in favor of profit maximization and embarked on an aggressive campaign to 17 bring hardware devices to the market.6 OpenAI now is preparing for its IPO, reportedly having "raised 18 more than $180 billion from investors" and continuing to "burn through cash at a historic pace."7 19 OpenAI's CEO, Sam Altman, is "under pressure from investors to show that the numbers work, while 20 facing increasingly stiff competition from rivals."8 21

22 2 23 https://time.com/7328674/openai-chatgpt-sam-altman-elon-musk-timeline/. 3 Id. 24 4 https://www.businessinsider.com/sam-altman. 25 5 https://www.reuters.com/technology/openai-ouster-microsoft-ai-research-ceo-sam-altmans-tumul- tuous-weekend-2023-11-20/; https://www.businessinsider.com/sam-altman; 26 https://techcrunch.com/2023/04/28/openai-funding-valuation-chatgpt/. 6 27 https://www.businessinsider.com/sam-altman. 7 https://www.cnbc.com/2026/05/20/openai-ipo-filing.html. 28 8 Id. COMPLAINT 8 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 10 of 41

1 36. In 2024, Tang Tan and other former senior Apple executives co-founded io Products 2 as the dedicated hardware vehicle for OpenAI. In May 2025, OpenAI announced its acquisition of io 3 for approximately $6.5 billion and proceeded to "officially merge[]" the already integrated io team 4 with OpenAI.9 Meanwhile, Mr. Tan became OpenAI's Chief Hardware Officer, overseeing a hard- 5 ware division that hired scores of Apple engineers in the months that followed. 6 37. Also in 2025, OpenAI announced a partnership with Foxconn, Apple's iPhone assem- 7 bler, for its own production and engaged Luxshare and Goertek, both established Apple suppliers, for 8 components.10 9 38. By November 2025, OpenAI confirmed that it had completed its "first prototypes" of 10 its device.11 But under mounting pressure to deliver its first commercial hardware product and facing 11 the reality that building a successful consumer device business from scratch is more complex, time- 12 consuming, and difficult than it anticipated, OpenAI has resorted to taking unlawful shortcuts. 13 II. Apple and Its Trade Secrets 14 39. Apple receives substantial benefit from its investment and innovation in its intercon- 15 nected ecosystem of proprietary information spanning hardware engineering, manufacturing design, 16 supply chain, business operations, and institutional expertise across these and other domains. These 17 innovations are critical drivers of Apple's business performance. OpenAI's goals in the consumer 18 market would be immeasurably advanced and accelerated if it were permitted to freely exploit the 19 secret technology, skills, and business acumen that Apple has spent decades developing and optimiz- 20 ing. 21 40. Apple's trade secrets include those described below. Each category of secrets derives 22 independent economic value from its secrecy and has been the subject of Apple's extensive protective 23 measures. 24 a. Hardware Engineering and Product Design: Apple's hardware engineering trade se- 25 crets include confidential hardware engineering information such as circuit and system 26 9 https://openai.com/sam-and-jony/; https://techtime.news/2025/07/30/openai/. 27 10 Id. 11 28 https://www.cnbc.com/2025/11/24/openai-hardware-jony-ive-sam-altman-emerson-collective .html. COMPLAINT 9 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 11 of 41

1 design specifications, component architecture, and power management innovations; pro- 2 prietary product designs for current and future unreleased products, maintained under 3 strict confidentiality using internal code names and need-to-know access controls; confi- 4 dential product roadmaps, milestone schedules, and development timelines; AI and ma- 5 chine learning integration data developed for Apple's hardware products; and proprietary 6 coexistence and electromagnetic interference engineering data, including testing meth- 7 odologies and design solutions developed to manage signal interference—technical in- 8 novations that reflect years of work and investment. 9 b. Manufacturing Design, Industrial Design, and Process Engineering: Apple's engi- 10 neers design and qualify best-in-class processes and techniques to meet Apple's exacting 11 aesthetic and functional standards. Apple's unique product designs often re-quire custom 12 machinery and processes for manufacturing. Accordingly, unlike competitors who buy 13 off-the-shelf parts, Apple often designs and customizes the specialized, proprietary ma- 14 chinery used in its suppliers' factories, ensuring it can protect the design and development 15 of current and future products along with its cutting-edge manufacturing techniques. Ap- 16 ple's trade secrets in this area include proprietary manufacturing processes, custom ma- 17 chinery, equipment designs and collections and configurations of equipment; proprietary 18 metal alloys, metal-finishing techniques, and material specifications; Design for Manu- 19 facturability ("DFM") expertise—confidential optimization of manufacturing processes, 20 part tolerances, and production scalability; and proprietary equipment housed at supplier 21 facilities, subject to strict use restrictions. 22 c. Component Technologies: Apple's trade secrets in this area include proprietary compo- 23 nent technologies developed in collaboration with trusted

suppliers and sub-suppliers for 24 specific Apple hardware programs—including power management integrated circuits, 25 battery systems, and display, acoustic, and touch subsystems; the identities of the spe- 26 cialized sub-suppliers and vendors who collaborate with Apple on these technologies; the 27 specific technical specifications, performance parameters, and design requirements Ap- 28

1 ple imposes on these components; and fully integrated, plug-and-play solutions engi- 2 neered with specialized third-party vendors unique to Apple and protected by stringent 3 confidentiality terms. These innovations reflect years of research, development, and in- 4 vestment that cannot be readily ascertained through reverse engineering or independent 5 research alone. 6 d. Proprietary Testing, Validation, and Development Methodologies: Apple's trade se- 7 crets in this area include confidential testing data, performance evaluations, and trend 8 analyses generated through extensive engineering investment; proprietary fabrication ap- 9 proval workflows and fabrication processes relating to the transition from design to man- 10 ufacture; lifecycle simulation data and manufacturing process development records; fail- 11 ure analyses and technical evaluations documenting the resolution of engineering chal- 12 lenges; confidential development roadmaps identifying technical challenges, proposed 13 solutions, and supplier collaboration strategies; and proprietary methodologies for eval- 14 uating tradeoffs between performance, reliability, cost, and manufacturability. These ma- 15 terials reflect years of accumulated engineering knowledge—including the negative 16 know-how of what approaches have been tested, rejected, or refined—that cannot be rep- 17 licated through reverse engineering or independent research and that provide a compre- 18 hensive window into Apple's hardware development processes. 19 e. Global Supply Chain Operations, Supplier Relationships, and Proprietary Business 20 Operations: Apple's trade secrets in this area include confidential contractual arrange- 21 ments with suppliers; supplier qualification and allocation strategies; logistics coordina- 22 tion processes that synchronize global component delivery at scale; and proprietary sup- 23 plier relationships—including the identities and roles of specialized sub-suppliers and 24 vendors who provide Apple with critical components and equipment. Apple has pains- 25 takingly developed its supplier network and invested in components and production ca- 26 pacity years in advance to maintain its highly complex operations with exceptional pre- 27 cision. Apple also maintains confidential information regarding its project assignments 28 and aggregated personnel information—information that, if obtained by a competitor,

1 could be used to strategically identify and recruit employees to acquire their institutional 2 knowledge. Apple also possesses proprietary and secret information regarding how its 3 global supply chain operations, supplier relationships, manufacturing design and process 4 engineering know-how, DFM expertise, and component technologies interconnect and 5 function together as an integrated whole. Apple's systems-level integration knowledge— 6 the confidential coordination and management of its complex network of suppliers, sub- 7 suppliers, vendors, and internal teams—is a trade secret in its own right. The know-how 8 required to make these interconnected elements work together enables Apple to achieve 9 efficiency, quality control, scalability, and speed-to-market that cannot be replicated 10 without the investments in technology and innovation Apple has made over many years. 11 41. Each category derives independent economic value from its secrecy. Apple has in- 12 vested hundreds of billions of dollars and decades of effort in developing this information and keeping 13 it confidential. A competitor with access to it could bypass years of independent research and devel- 14 opment, skip the capital expenditure required to build genuine expertise, and bring products to market 15 faster and at lower cost—harming the value of Apple's investments. Rather than investing what le- 16 gitimate development would require, OpenAI has turned to trade secret misappropriation to free-ride 17 off Apple's decades of innovation. 18 III. Apple Diligently and Reasonably Protects Its Trade Secrets. 19 42. Apple protects its trade secrets and confidential information through reasonable con- 20 tractual, technical, and physical measures. 21 43. As a condition of employment, Apple employees are required to sign an Intellectual 22 Property Agreement ("IPA"), updated from time to time, which details their confidentiality and non- 23 disclosure obligations. 24 44. Specifically, under an applicable version of the IPA, employees acknowledge that they 25 are prohibited, "during or after employment, from using or disclosing, or permitting any other person 26 or entity to use or disclose, any Proprietary Information without the written consent of Apple, except 27 as necessary to perform [their] duties as an employee of Apple." The prohibition extends beyond the 28 employee's own conduct; the IPA equally bars employees from "permitting any other person or entity

1 to use or disclose any Proprietary Information" without Apple's consent. Employees further agree to 2 "strictly

comply with all of Apple's rules and policies regarding Proprietary Information and use best 3 efforts to safeguard such Proprietary Information and protect it against disclosure, misuse, loss, or 4 theft." And upon departure, the IPA prohibits employees from taking "any documents, materials, or 5 copies thereof, whether on paper or any other medium, containing any Proprietary Information." 6 45. Apple ensures its employees understand their obligations by providing trainings ad- 7 dressing their confidentiality obligations. For instance, Apple requires all its employees to take a 8 "Business Conduct" course annually, in which Apple reinforces obligations to "protect Apple Confi- 9 dential Information."12 10 46. Apple reminds departing employees of their ongoing confidentiality obligations under 11 the IPA and reminds them to return any Apple proprietary information before leaving Apple. Apple 12 follows departure procedures to protect its confidential information. Departing employees must return 13 Apple-issued work devices, including laptops and mobile devices, as well as their badges and other 14 Apple-owned equipment. When departing Apple, employees are reminded that their confidentiality 15 obligations remain even after termination. 16 47. Apple ensures protection of its trade secrets and Apple Confidential Information stored 17 in its secure network file repository, a third-party hosted cloud system that houses confidential engi- 18 neering files, project documentation, and proprietary technical data, among other types of files. Net- 19 work storage access at Apple is provisioned through Apple's Access Manager system under Apple's 20 terms of use that limit access to only "for work purposes" and notes that stored files "may contain 21 Apple Confidential Information—including any non-public details regarding our past, present, or fu- 22 ture products and services." Apple disables and prohibits access to its network storage upon an em- 23 ployee's departure. 24 48. Apple engages in other extensive measures protecting its confidential and proprietary 25 technology, including using database exchange and collaboration systems which include permission 26 assignment to ensure access is on a need-to-know basis; requiring non-disclosure and/or confidenti- 27 ality agreements with Apple's suppliers, vendors, contractors, and other third parties before providing 28 12 https://www.apple.com/compliance/pdfs/Business-Conduct-Policy.pdf. COMPLAINT 13 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 15 of 41

1 access to Apple's trade secrets, and even then only providing access to confidential information on a 2 need-to-know basis; and maintaining high standards for encryption, password protection, and device 3 authentication, among many other measures. 4 49. Apple uses locked buildings, security cameras, guards, and other measures to control 5 access to its physical facilities. Apple restricts physical access to its buildings within the company. 6 Badge access for Apple employees may be limited to certain buildings or portions of buildings de- 7 pending on the employee's specific team and role. Any person who does not have a badge must be 8 escorted by an Apple employee while within Apple's facilities. 9 50. Apple further protects its trade secrets by restricting access to its file repositories for 10 projects to only those employees who are currently working on and authorized to view them. Apple 11 strictly controls who is disclosed on a project and only permits individuals with a demonstrated busi- 12 ness need to be disclosed. 13 51. Apple goes to great lengths to ensure that its trusted business partners, including ven- 14 dors, laboratories, and other companies in its supply chain, commit to stringent confidentiality obli- 15 gations. Suppliers working with Apple must sign restrictive confidentiality agreements to protect Ap- 16 ple's innovations. Suppliers are required to implement physical security measures, such as using qual- 17 ified security teams, security cameras, sensors, personnel identification credential screening, and ve- 18 hicle markings. Apple uses code names for projects to prevent leaks and requires suppliers to track 19 all confidential materials, including by using proprietary chain-of-custody protocols for sensitive 20 components to ensure secure disposal of scrap materials. Apple also maintains a proprietary shipping 21 process to transport confidential prototypes between facilities. 22

23

24

25

26 27

28

COMPLAINT 14 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 16 of 41

1 52. These measures are mere examples of Apple's substantial investment in maintaining 2 the secrecy of its global supply chain and manufacturing trade secrets. Apple continually strives to 3 implement effective and stringent security measures to protect its trade secrets. If and when Apple 4 learns of a bug or vulnerability in its security measures, it investigates and takes steps to fix the issue 5 and improve its security measures. Due to Apple's rigorous security measures and practices, Apple's 6 trade secrets are not available to the public or to

Apple’s competitors through any legitimate means. 7 IV. Defendants’ Misappropriation of Apple’s Trade Secrets and Confidential Information 8 53. Despite Apple’s rigorous security measures and practices, Apple’s trade secrets have 9 been compromised through the deliberate misconduct by those previously entrusted with them. Ap- 10 ple’s former engineers and executives—recruited, directed and rewarded by OpenAI—along with 11 OpenAI itself and its business cohorts, have been stealing Apple’s most sensitive information for a 12 would-be competitor. With over four hundred former Apple employees now working at OpenAI, it 13 is not surprising that certain OpenAI personnel have knowledge of Apple’s confidential and proprie- 14 tary information, which they are obligated to keep confidential. But OpenAI has resorted to exploiting 15 this confidential information, using it to extract still more from Apple’s current employees and trusted 16 partners, and to structure its interview processes to try to solicit additional confidential Apple infor- 17 mation—all while taking steps to conceal its actions. That OpenAI now employs people who were 18 once entrusted with Apple’s trade secrets does not entitle OpenAI to use that information to jumpstart 19 its hardware efforts.13 20 A. Former Apple employees have taken Apple’s trade secrets and confidential information to OpenAI. 21 54. Apple’s investigation has uncovered misconduct reaching across seniority levels, tech- 22 nical disciplines, and departments at OpenAI. The following examples, drawn from Apple’s ongoing 23 internal investigation of information gleaned from Apple’s company-owned devices and systems, 24 begin to illuminate the scope and nature of the Defendants’ unlawful conduct. While Apple’s ongoing 25 investigation has provided insights obtained from its own systems, Apple has virtually no visibility 26 13 Apple and OpenAI have a commercial relationship involving the integration of OpenAI’s ChatGPT 27 into Apple Intelligence. The companies have entered into a written agreement governing that integra- tion. That agreement is not at issue here. OpenAI’s acts of trade secret misappropriation alleged herein 28 do not arise from and have no connection to that agreement. COMPLAINT 15 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 17 of 41

1 into what has been happening behind closed doors at OpenAI and io. Discovery will expose that the 2 misappropriation has been occurring on a scale many times greater than the several instances de- 3 scribed below. 4 1. Chang Liu, Member of Technical Staff at OpenAI

5 55. Chang Liu departed Apple on January 22, 2026 to join OpenAI. Like other Apple em-

6 ployees, Mr. Liu signed and is bound by an IPA obligating him to protect Apple’s confidential infor-

7 mation. Around the time of his departure, however, Mr. Liu was unresponsive to Apple’s outreach

8 trying to confirm whether he had returned his devices and complied with other exit procedures, sched-

9 uling an exit interview, and instructing him to sign Apple’s confidentiality reminder. And, at the time

10 of his departure, Mr. Liu failed to return at least one Apple-owned computer.

11 56. After leaving Apple, Mr. Liu maintained a close relationship with an employee who

12 was still working at Apple, Yu-Ting “Alyssa” Peng, and he communicated with her frequently prior

13 to her own departure for OpenAI on April 16, 2026. Within hours of leaving Apple, Mr. Liu shared

14 with Ms. Peng, “I still have another computer” he was planning to use to access Apple’s confidential

15 information so he could discuss it with Ms. Peng that evening. Within weeks of departing Apple,

16 Mr. Liu also used Ms. Peng’s Apple-issued work computer that was authenticated to Apple’s net-

17 work—accessing it while she was still employed at Apple and he was not.

18 57. On or around February 9, 2026, weeks after he had left Apple and knowing he had no

19 right to do so, Mr. Liu tried to access Apple’s network storage—a cloud-based file repository con-

20 taining Apple’s confidential engineering files, project documentation, and other proprietary infor-

21 mation. Mr. Liu discovered that, surprisingly, he still could access the Apple’s network repository

22 after leaving Apple, the result of a then-unknown authentication vulnerability. Rather than bringing

23 this to Apple’s attention or protecting Apple’s confidential information as required by his IPA, Mr.

24 Liu celebrated his find with Ms. Peng and set about exploiting it: “LOL, I found out I can access the

25 [network storage], so funny." Ms. Peng's response was immediate: "I'm ready." Mr. Liu knew ac-

26 cessing Apple's network storage after he had left the company was unauthorized and prohibited, as

27 he had agreed to the confidentiality restrictions of his IPA.

28

1 58. While employed by OpenAI, Mr. Liu then proceeded to select, access, and download 2 dozens of confidential files from Apple's network repository. He downloaded confidential technical 3 presentations, spreadsheets, PDFs, and written work product—including a compilation of technical 4 files with over a thousand pages reflecting details of confidential work he and others did at Apple— 5 many expressly labeled as confidential. He shared his findings with Ms. Peng, who was still employed 6 by Apple, sending her links to Apple's proprietary materials—and directing her attention to specific 7 project folders, engineering documentation, and technical data. 8 59. Among the files Mr. Liu downloaded is a presentation concerning the manufacture and 9 testing of MLBs (multi-layer or main logic boards)—complex circuit boards in Apple's hardware. 10 The presentation details the manufacturing process, testing workflows, data captured during testing 11 and how to interpret it, and more, with photographs and accompanying analyses. It identifies specific 12 equipment to perform these analyses and issues each piece of equipment is capable of diagnosing— 13 proprietary operational knowledge that reflects years of accumulated testing experience and would 14 be invaluable to anyone developing hardware. 15 60. Mr. Liu continued illicitly accessing and downloading Apple's confidential and pro- 16 prietary information while he was developing products for OpenAI. Apple discovered Mr. Liu's mis- 17 conduct through its own investigation. Once it learned of this security breach, Apple immediately 18 took steps to ensure Mr. Liu's access was terminated. 19 61. At no point did Mr. Liu notify Apple or take steps to stop it. Only OpenAI and Mr. Liu 20 know all the ways they have been exploiting the trove of Apple confidential information he stole, and 21 to the extent they have not concealed or destroyed the evidence of these misappropriations, it will be 22 investigated thoroughly in discovery. 23 62. Mr. Liu's theft of dozens of confidential files and trade secrets from Apple's network 24 storage is not his only offense. For months while he was working for OpenAI, and while Ms. Peng 25 was still working at Apple, Mr. Liu received from her frequent updates on Apple's active confidential 26 projects, vendor decisions, and engineering details. Ms. Peng and Mr. Liu would engage in depth 27 about those confidential projects, while Mr. Liu was working on developing OpenAI's competing 28

1 hardware. Mr. Liu's work for OpenAI was informed by a steadily flowing stream of Apple's trade 2 secret information from Ms. Peng. 3 63. Before Ms. Peng left Apple for OpenAI in April, Mr. Liu also coached her on how to 4 access and copy files from Apple workstations "to avoid trouble with the security team," and directed 5 Ms. Peng to specific Apple project folders and proprietary engineering data. 6 64. Mr. Liu also equipped and prepared Ms. Peng with proprietary Apple information to 7 use at her interview with OpenAI. Knowing OpenAI's interviewing practices and what technical ex- 8 pertise at Apple would be valuable to OpenAI, Mr. Liu instructed Ms. Peng on which of Apple's 9 confidential information she should study in preparation for her OpenAI interviews. 10 65. Messages left on Apple-issued work devices show that Mr. Liu told Ms. Peng how 11 another former Apple employee who had interviewed at OpenAI had "fumbled" his answers to ques- 12 tions that OpenAI's Chief Hardware Officer Tang Tan asked him about a top-secret project for an 13 unreleased new Apple product. Hoping to help Ms. Peng prepare and better handle such questions, 14 messages and other evidence shows that Mr. Liu helped Ms. Peng study, using, on information and 15 belief, his illicit access to Apple's network storage to "download[] some info" for Ms. Peng's review. 16 Ms. Peng was subsequently offered a position at OpenAI and departed Apple in April 2026. 17 66. Mr. Liu knew what he was doing was wrong, wanted to hide it from Apple, and took 18 steps to keep it from being discovered. Although he and Ms. Peng sometimes communicated using 19 Apple-owned devices, Mr. Liu recognized this could risk exposing his misdeeds and so told her they 20 should communicate privately over an alternative platform, the LINE Messenger app, to try to avoid 21 detection. To the extent they have not destroyed or concealed this evidence, it will be revealed through 22 discovery. 23 67. While working for OpenAI, Mr. Liu acquired Apple's trade secrets by improper 24 means—by his own unauthorized access and through his ongoing contact with Ms. Peng—knowing 25 it was unauthorized. He used and disclosed those trade secrets for OpenAI's benefit. Expressing 26 amusement upon discovering he could surreptitiously access troves of Apple trade secrets while 27 working for OpenAI, downloading them repeatedly and deliberately, and using private channels to 28

1 hide his communications about his conduct lay bare his willful and malicious intent. Mr. Liu's mate- 2 rial breaches of his contract are equally clear and deliberate: he accessed, copied, and directed the 3 disclosure of Apple Confidential Information after his employment ended, in direct violation of his 4 post-termination obligations. 5 2. Tang Tan, Chief Hardware Officer at OpenAI 6 68. Tang Tan is OpenAI's Chief Hardware Officer and has been centrally involved in 7 OpenAI's extraction and improper use of proprietary Apple information. 8 69. Mr. Tan has unlawfully exploited Apple's trade secrets and other confidential infor- 9 mation in recruiting Apple employees for OpenAI. For example, Mr. Tan has used Apple's internal 10 project code names during OpenAI interviews to inquire about the status of Apple's confidential 11 projects for developing unreleased products—reinforcing that Mr. Tan is using Apple's internal in- 12 formation to solicit its trade secrets from job candidates. For instance, in the hours before his OpenAI 13 interview with Mr. Tan, a then-Apple employee began screenshotting and downloading files relating 14 to a highly confidential Apple project. Then, in the interview, Mr. Tan solicited more information 15 about that same Apple project. This has become an established pattern. 16 70. Mr. Tan has directed candidates to bring physical hardware components, "parts," and 17 product samples from their Apple work to their OpenAI interviews for "show and tell" sessions that 18 would disclose Apple's proprietary technologies. For example, messages left on an Apple-issued 19 work device show that Mr. Tan instructed an Apple employee to "bring some parts [she] worked on" 20 such as "Batteries," "SIP" (Systems-in-Package), "mlb" (multi-layer or main logic boards), and 21 "shields" and that it may "be good to show" other interviewers these Apple components. 22 71. Apple has seen no evidence to date suggesting that OpenAI or Mr. Tan meaningfully 23 tried to prevent or avoid the improper disclosure of Apple's confidential information during these 24 "show and tell" sessions. To the contrary, this seems their very purpose. 25 72. This is emblematic of how OpenAI has been unlawfully extracting confidential Apple 26 information through its recruiting processes more generally. First, to prepare for an interview with 27 leaders at OpenAI, a candidate is encouraged to access and get ready to discuss some of Apple's most 28 sensitive information. Then, in the interview, OpenAI leaders, who are former Apple insiders like

1 Mr. Tan, use Apple's internal project codes to ask about and receive more of Apple's trade secret 2 information. Before the interview is over, OpenAI has used and acquired more confidential Apple 3 information and "primed the pump" to keep it coming once the new hire arrives from Apple. 4 73. While employed at OpenAI, Mr. Tan also improperly retained or obtained an internal 5 Apple document bearing a "Need to Know" designation that describes offboarding procedures for 6 Apple's managers. The document details security processes Apple uses to protect the company's 7 confidential information when one of its employees is leaving. OpenAI's personnel refer to this as "a 8 checklist that Tang put together," though it is clearly an internal Apple document. Mr. Tan and 9 OpenAI have disclosed it to recruited Apple employees before they notify Apple that they are leaving, 10 providing them with advance notice of Apple's forensic and security checks. 11 74. These tactics appear to be having their desired effect. Apple has observed a recent trend 12 of employees who are leaving Apple for OpenAI and taking steps to evade security measures. This 13 includes ignoring outreach by security personnel to schedule exit processes and security reviews. 14 B. OpenAI has been stealing Apple's trade secrets and confidential information through current and former Apple employees. 15 75. OpenAI and its cohorts, led at least in part by former Apple employees, have recruited 16 candidates from Apple, extracted their knowledge of Apple's sensitive and confidential information, 17 and then continued to exploit that knowledge once they arrived. As a result, OpenAI has misappro- 18 priated Apple's trade secrets and confidential information in a variety of ways. For example, mes- 19 sages left on Apple-issued work laptops have revealed that: 20 a. OpenAI coaches candidates to prepare for their interviews by studying Apple's 21 confidential engineering documentation, internal presentations, and proprietary 22 technical materials. OpenAI then uses its insider Apple information to ask de- 23 tailed questions to extract more: about Apple's proprietary tools, vendor man- 24 agement processes, engineering methodologies, manufacturing workflows, and 25 supplier relationships, for example. 26 b. OpenAI asks candidates to prepare "Technical Deep Dive" presentations, com- 27 plete with "slides (required)," about their work at Apple at such a level of detail 28 that requires revealing Apple's confidential information. For example, OpenAI COMPLAINT 20 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 22 of 41

1 instructs candidates to bring "CAD/design artifacts" and "prototypes" from 2 their recent work at Apple. It asks Apple's employees to divulge their "subsys- 3 tem and component selection" and information about Apple's "tools or meth- 4 odologies you use for system integration, such as CAD software, simulation 5 tools." It asks candidates to explain "Vendor selection and communication/col- 6 laboration with vendors" in Apple's prized network of

partners. 7 c. OpenAI interviewers also request that Apple candidates bring “Actual parts” 8 as “props” from Apple for “show and tell.” For example, OpenAI has instructed 9 Apple employees to bring “Batteries,” “SIP” (systems-in-package), “mlb” 10 (multi-layer or main logic boards), “shields,” “piece parts,” and “housings and 11 BGs [back glass] in different colours,” along with other hardware components 12 and product samples from their Apple work. One candidate expressed concern 13 over OpenAI’s tactics, noting he was “surprised people have brought” Apple 14 parts to interviews because he “didn’t know we could take those from the of- 15 fice.” 16 d. Panels of OpenAI interviewers use Apple’s internal project code names, pro- 17 prietary terminology, and knowledge to probe for secret information about Ap- 18 ple’s projects and operations. OpenAI interviewers include former Apple em- 19 ployees such as Tang Tan who possess Apple’s confidential information and 20 know which questions will unlock more. No evidence that Apple has seen to 21 date suggests that Defendants have taken steps to avoid the improper disclosure 22 of Apple’s confidential information during these interviews. 23 e. At OpenAI’s instruction or for its benefit, departing Apple employees, around 24 the time they are leaving Apple, send Apple’s confidential information to their 25 personal email accounts for future use in their work at OpenAI—including pro- 26 prietary engineering data, manufacturing design documentation, and AI-related 27 materials. 28

1 76. OpenAI is the beneficiary of every act described above. OpenAI’s recruiting practices 2 suggest it hires these individuals at least in part because of the confidential Apple-specific knowledge 3 and expertise they have and could improperly obtain; OpenAI assesses and extracts that expertise and 4 information; and OpenAI has been deploying it in its hardware development, supply chain and partner 5 operations and communications, and hiring decisions. 6 77. OpenAI’s conduct is knowing and deliberate, as demonstrated, for example, by its sen- 7 ior executives using Apple’s internal project code names in interviews, asking candidates about con- 8 fidential Apple projects, directing them to bring Apple parts and prototypes, distributing Apple’s 9 internal departure procedures to Apple employees before they announce their departures, which helps 10 them avoid scrutiny, by OpenAI employees celebrating, using, and doing nothing to stop prohibited 11 access to confidential Apple data and repositories, and by OpenAI employees communicating over 12 private platforms to avoid detection. 13 78. This is a systematic effort to acquire, retain, and use Apple’s trade secrets to help 14 OpenAI try to replicate the secret technologies, business processes, and supply chain innovations that 15 took Apple decades to build in its consumer hardware business. 16 C. OpenAI has been stealing Apple’s trade secrets and confidential information through Apple’s trusted partners. 17 79. OpenAI has not stopped at extracting Apple’s trade secrets and confidential infor- 18 mation through Apple’s current and former employees. OpenAI also has been targeting Apple’s 19 prized partner network and supply chain directly. It has been using misappropriated knowledge of 20 Apple’s confidential relationships, manufacturing and design processes, and proprietary terminology 21 to extract from trusted third parties additional trade secret information and processes. 22 80. As one example, OpenAI, including through io, has accessed, exploited, and used Ap- 23 ple’s secret, proprietary industrial design techniques, processes, and know-how related to metal-fin- 24 ishing, at least by having a trusted Apple partner perform Apple’s proprietary, trade secret processes 25 for OpenAI’s benefit. This is a third-party partner with whom Apple works on industrial design ser- 26 vices and experimentation, including metal-finishing techniques, among others. The partner is bound 27 by agreements with Apple that include use restrictions and confidentiality obligations prohibiting it 28

1 from doing for other companies the confidential work it does for Apple and from using certain facil- 2 ities for anyone but Apple. Apple developed its proprietary, multi-step metal-finishing techniques 3 over many years to ultimately produce the finishes that define the look and feel of Apple products. 4 81. Former Apple executives at OpenAI including Mr. Tan have confidential knowledge 5 of Apple’s use restrictions and confidentiality arrangement with this partner. Despite this, OpenAI, 6 on its own or with or through its partner io, used, without authorization, Apple’s proprietary and 7 confidential metal-finishing processes, having the partner perform them for OpenAI’s benefit, and in 8 so doing, obtained products produced by exploiting misappropriated trade secrets. OpenAI and its 9 cohorts misled the partner to believe they had Apple’s permission to have the partner carry out the 10 confidential metal-finishing technique for OpenAI’s benefit. 11 82. Apple has not given OpenAI or io permission to use or a license to any of Apple’s trade 12 secrets or confidential information, including those it has entrusted with this partner. 13 83. OpenAI also has approached at least another trusted Apple supplier who works with 14 Apple on manufacturing and manufacturing design, including with respect to power and batteries, 15 among other things. OpenAI has been using Apple’s confidential information and internal terminol- 16 ogy about manufacturing design and specific component technologies to approach this trusted sup- 17 plier and ask targeted

questions (that only Apple-insiders would know to ask) about specific confi- 18 dential Apple components that would be useful in furthering OpenAI's hardware ambitions. 19 20

21

22

23

24

25

26 27

28

1 D. OpenAI has been attempting to conceal its trade secret misappropriation. 2 84. OpenAI has actively coached Apple employees on how to manage their exits from 3 Apple in ways that avoid scrutiny. This helps OpenAI's new hires evade Apple's security procedures 4 and reduce the chance that their confidentiality violations and trade secret theft would be detected. 5 OpenAI has been circulating to their new hires an internal Apple document bearing a "Need to Know" 6 designation before they give notice to Apple of their departures. OpenAI has counseled departing 7 employees not to disclose their next employer and given advice on how to avoid the "dreaded walk 8 out" that would promptly remove them from the company rather than giving them a standard two 9 weeks in which they could continue to access Apple's confidential information and trade secrets. 10 And, review of Apple-issued work laptops has revealed that OpenAI has been advising Apple's de- 11 parting employees that they "won't sign anything at the exit interview" and is instructing them that if 12 Apple personnel "do ask you to sign anything" to let OpenAI know "asap." 13 85. Unsurprisingly, Apple has uncovered a concerning recent pattern among employees 14 who depart and then go work for OpenAI. Departing employees have been taking actions to evade 15 security measures, such as failing to provide two-weeks' notice, and ignoring outreach by security 16 personnel to schedule exit processes and security reviews, all of which may help to conceal the misuse 17 and misappropriation of confidential information. 18 FIRST CLAIM FOR RELIEF 19 Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 20 18 U.S.C. §§ 1832(a), 1836-37, 1839 et seq. 21 (Against Chang Liu) 22 86. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as 23 though fully set forth herein. 24 87. Apple is the owner of certain valuable trade secrets and confidential information relat- 25 ing to each category identified above. This information constitutes "trade secrets" within the meaning 26 of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory 27 definition of trade secret, it nonetheless constitutes Apple Confidential Information protected under 28 Apple's IPA and other applicable contracts and laws.

1 88. Apple's trade secrets and confidential information derive independent economic value, 2 both actual and potential, from not being generally known to, and not being readily ascertainable 3 through proper means by, other persons or entities who might obtain economic value from their dis- 4 closure or use. Apple has invested hundreds of billions of dollars and decades of research and devel- 5 opment to develop its trade secrets and confidential information, establishing operational excellence 6 that cannot be readily replicated without the same investments Apple has made. If these trade secrets 7 and confidential information were publicly known, competitors could quickly exploit Apple's inno- 8 vations without incurring the substantial costs and years of experimentation that Apple undertook, 9 harming the value of Apple's innovations and eroding the competitive advantage those investments 10 have created. 11 89. Mr. Liu's own conduct demonstrates the economic value of Apple's trade secrets and 12 confidential information. Rather than invest the time and resources necessary to further OpenAI's 13 hardware aspirations, Mr. Liu seeks to misappropriate Apple's innovations to accelerate efforts to 14 bring consumer hardware products to market. 15 90. Apple's trade secrets and confidential information relate to products used, sold, pur- 16 chased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign com- 17 merce—including Apple's iPhone, Apple Watch, and MacBook product lines, which are designed, 18 manufactured through global supply chains, and sold to consumers worldwide. Mr. Liu acquired Ap- 19 ple's trade secrets and confidential information through improper means and used them while em- 20 ployed by OpenAI, a company developing and manufacturing hardware products for sale in interstate 21 and foreign

commerce. 22 91. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy 23 of its trade secrets and confidential information. 24 92. Mr. Liu has misappropriated Apple's trade secrets and confidential information by ac- 25 quiring and using them by improper means, including by at least: obtaining and/ or maintaining unau- 26 thorized access to Apple's confidential systems and illicitly communicating about Apple's confiden- 27 tial information and trade secrets through Apple personnel without authorization, including about 28 ongoing confidential Apple engineering and product development projects after his departure from

1 Apple; exfiltrating Apple's trade secrets and confidential information after his departure from Apple 2 and for use outside of Apple; and deploying Apple's institutional knowledge in hardware develop- 3 ment for OpenAI. 4 93. At no time has Apple consented to Mr. Liu's improper acquisition, disclosure, or use 5 of Apple's trade secrets or confidential information. 6 94. Mr. Liu knew, or had reason to know, that the trade secrets and confidential infor- 7 mation he was acquiring were maintained confidentially by Apple, were not generally available to 8 the public or competitors, and were developed at great expense and effort. Mr. Liu's own employment 9 and execution of an IPA with Apple foreclose any defense of ignorance. 10 95. To the extent that Mr. Liu's acts of misappropriation have occurred outside the United 11 States, including any attempts to extract Apple's trade secrets from Apple's trusted overseas suppli- 12 ers, such conduct is unlawful under the Defend Trade Secrets Act as Mr. Liu has acted domestically 13 in furtherance of the misappropriation. For example, Mr. Liu resides in Sunnyvale and intends to use 14 and is using Apple's misappropriated trade secrets in the United States to develop, manufacture, and 15 commercialize products that will be marketed and sold to American consumers. Mr. Liu in the United 16 States has directed, coordinated, supported, or benefited from, his misappropriation of Apple's trade 17 secrets, and any products or services incorporating or resulting from Apple's trade secrets will be 18 developed and offered in the United States. 19 96. Mr. Liu's misappropriation was willful and malicious. 20 97. Mr. Liu's misappropriation has caused and continues to cause damage to Apple, in- 21 cluding loss of competitive advantage, diminishment of the economic value of its trade secrets and 22 confidential information, and ongoing threat of further harm. Mr. Liu has been unjustly enriched by 23 avoiding the substantial investment Apple has made. 24 98. Apple has no adequate remedy at law. Unless enjoined, Mr. Liu will continue to use 25 and benefit from Apple's misappropriated information. Apple is entitled to preliminary injunctive 26 relief, including: an order (i) requiring Mr. Liu to immediately preserve and not delete or destroy 27 evidence in any format relevant to Apple's claims in this action; (ii) enjoining Mr. Liu from further 28 acquiring, possessing, using, or disclosing Apple's trade secrets and confidential information; (iii)

1 enjoining Mr. Liu from altering or destroying any evidence related to his conduct; and (iv) requiring 2 Mr. Liu to return all copies of Apple's trade secrets and confidential information in his possession.14 3 SECOND CLAIM FOR RELIEF 4 Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 5 18 U.S.C. §§ 1832(a), 1836-37, 1839 et seq. 6 (Against Tang Tan) 7 99. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as 8 though fully set forth herein. 9 100. Apple is the owner of certain valuable trade secrets and confidential information relat- 10 ing to each category identified above. This information constitutes "trade secrets" within the meaning 11 of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory 12 definition of trade secret, it nonetheless constitutes Apple Confidential Information protected under 13 Apple's IPA and other applicable contracts and laws. 14 101. Apple's trade secrets and confidential information derive independent economic value, 15 both actual and potential, from not being generally known to, and not being readily ascertainable 16 through proper means by, other persons or entities who might obtain economic value from their dis- 17 closure or use. Apple has invested hundreds of billions of dollars and decades of research and devel- 18 opment to develop its trade secrets and confidential information, establishing operational excellence 19 that cannot be readily replicated without the same investments Apple has made. If these trade secrets 20 and confidential information were publicly known, competitors could quickly exploit Apple's inno- 21 vations without incurring the substantial costs and years of experimentation that Apple undertook, 22 harming the value of Apple's innovations and eroding the competitive advantage those investments 23 have created. 24 102. Mr. Tan's own conduct demonstrates the economic value of Apple's trade secrets and 25 confidential information. Rather than invest the time and resources necessary to further its hardware 26 14 Mr. Liu's employment contract with Apple includes an arbitration clause with a clear exception for 27 seeking preliminary injunctive relief in court. This suit is necessary so Apple may move for prelimi- nary injunctive relief against Mr. Liu and other defendants collectively, which Apple will do 28 promptly. COMPLAINT 27 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 29 of 41

1 aspirations, Mr. Tan seeks to misappropriate Apple's innovations to accelerate efforts to bring con- 2 sumer hardware products to market. 3 103. Apple's trade secrets and confidential information relate to products used, sold, pur- 4 chased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign com- 5 merce—including Apple's iPhone and Apple Watch product lines that Mr. Tan oversaw as VP of 6 Product Design, which are manufactured through global supply chains spanning multiple countries 7 and sold internationally. Mr. Tan has used and disclosed Apple's trade secrets and confidential infor- 8 mation to benefit OpenAI, a company developing and manufacturing hardware products for sale in 9 interstate and foreign commerce. 10 104. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy 11 of its trade secrets and confidential information. 12 105. Mr. Tan has misappropriated Apple's trade secrets and confidential information by 13 acquiring and using them by improper means, including by at least: directing exfiltration and disclo- 14 sure of Apple's trade secrets through the interview process; exfiltrating Apple's trade secrets and 15 confidential information for use outside of Apple; using Apple's internal project codes and technical 16 terminology to probe for and extract Apple's trade secrets; and deploying Apple's institutional 17 knowledge in hardware development, supply chain and partner operations and communications, and 18 hiring decisions. 19 106. At no time has Apple consented to Mr. Tan's improper acquisition, disclosure, or use 20 of Apple's trade secrets or confidential information. 21 107. Mr. Tan knew, or had reason to know, that the trade secrets and confidential infor- 22 mation he was acquiring were maintained confidentially by Apple, were not generally available to 23 the public or competitors, and were developed at great expense and effort. Mr. Tan's own possession 24 and distribution of Apple's internal departure procedures—which expressly reference Apple's IPA 25 obligations—foreclose any defense of ignorance. Mr. Tan also executed his own IPA and served in a 26 senior role with access to Apple's most sensitive information for over twenty-four years. 27

28

1 108. To the extent that Mr. Tan's acts of misappropriation have occurred outside the United 2 States, including any attempts to extract Apple's trade secrets from Apple's trusted overseas suppli- 3 ers, such conduct is unlawful under the Defend Trade Secrets Act, as Mr. Tan has acted domestically 4 in furtherance of the misappropriation. For example, Mr. Tan resides in San Francisco and intends to 5 use and is using Apple's misappropriated trade secrets in the United States to develop, manufacture, 6 and commercialize products that will be marketed and sold to American consumers. Mr. Tan in the 7 United States has directed, coordinated, supported, or benefited from, his misappropriation of Apple's 8 trade secrets, and any products or services incorporating or resulting from Apple's trade secrets will 9 be developed and offered in the United States. 10 109. Mr. Tan's misappropriation was willful, entitling Apple to exemplary damages under 11 18 U.S.C. § 1836(b)(3)(C). 12 110. Mr. Tan's misappropriation has caused and continues to cause damage to Apple, in- 13 cluding loss of competitive advantage, diminishment of the economic value of its trade secrets and 14 confidential information, and ongoing threat of further harm. Mr. Tan has been unjustly enriched by 15 avoiding the substantial investment Apple has made, for which Apple will seek damages in an amount 16 to be determined at trial. 17 111. Apple has no adequate remedy at law. Unless enjoined, Mr. Tan will continue to use 18 and benefit from Apple's misappropriated trade secrets and confidential information. Apple is entitled 19 to preliminary and permanent injunctive relief, including: an order (i) requiring Mr. Tan to immedi- 20 ately preserve and not delete or destroy evidence in any format relevant to Apple's claims in this 21 action; (ii) enjoining Mr. Tan from further acquiring, possessing, using, or disclosing Apple's trade 22 secrets and confidential information; (iii) enjoining Mr. Tan from altering or destroying any evidence 23 related to his conduct; and (iv) requiring Mr. Tan to return all copies of Apple's trade secrets and 24 confidential information in his possession. 25

26 27

28

1 THIRD CLAIM FOR RELIEF 2 Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 3 18 U.S.C. §§ 1832(a), 1836-37, 1839 et seq. 4 (Against OpenAI) 5 112. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as 6 though fully set forth herein. 7 113. Apple is the owner of certain valuable trade secrets and confidential information relat- 8 ing to each category identified above. This information constitutes "trade secrets" within the meaning 9 of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory 10 definition of trade secret, it nonetheless constitutes Apple Confidential

Information protected under 11 Apple's IPA and other applicable contracts and laws. 12 114. Apple's trade secrets and confidential information derive independent economic value, 13 both actual and potential, from not being generally known to, and not being readily ascertainable 14 through proper means by, other persons or entities who might obtain economic value from their dis- 15 closure or use. Apple has invested hundreds of billions of dollars and decades of research and devel- 16 opment to develop its trade secrets and confidential information, establishing operational excellence 17 that cannot be readily replicated without the same investments Apple has made. If these trade secrets 18 and confidential information were publicly known, competitors could quickly exploit Apple's inno- 19 vations without incurring the substantial costs and years of experimentation that Apple undertook, 20 harming the value of Apple's innovations and eroding the competitive advantage those investments 21 have created. 22 115. OpenAI's own conduct demonstrates the economic value of Apple's trade secrets and 23 confidential information. Rather than invest the time and resources necessary to further its hardware 24 aspirations, OpenAI seeks to misappropriate Apple's innovations to accelerate its efforts to bring 25 consumer hardware products to market. 26 116. Apple's trade secrets and confidential information relate to products used, sold, pur- 27 chased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign com- 28 merce—including Apple's iPhone, Apple Watch, and MacBook product lines, which are designed,

1 manufactured through global supply chains, and sold to consumers worldwide. OpenAI has acquired 2 and is deploying Apple's trade secrets and confidential information to develop and commercialize its 3 own hardware devices, which it intends to sell to consumers in interstate and foreign commerce. 4 117. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy 5 of its trade secrets and confidential information. 6 118. OpenAI has misappropriated Apple's trade secrets and confidential information by ac- 7 quiring and using them by improper means, including by at least: approaching Apple's suppliers and 8 partners using misappropriated trade secrets to extract still more of Apple's confidential and propri- 9 etary technology; inducing breach of partners' confidentiality obligations and use restrictions; direct- 10 ing exfiltration and disclosure of Apple's trade secrets through its interview process; obtaining and/or 11 maintaining unauthorized access to Apple's confidential systems and illicitly communicating about 12 Apple's confidential information and trade secrets through Apple personnel without authorization, 13 including about ongoing confidential Apple engineering and product development projects; exfiltrat- 14 ing Apple's trade secrets and confidential information for use outside of Apple; using Apple's internal 15 project codes and technical terminology to probe for and extract Apple's trade secrets; and deploying 16 Apple's institutional knowledge in hardware development, supply chain and partner operations and 17 communications, and hiring decisions. 18 119. At no time has Apple consented to OpenAI's improper acquisition, disclosure, or use 19 of Apple's trade secrets or confidential information. 20 120. OpenAI knew, or had reason to know, that the trade secrets and confidential infor- 21 mation it was acquiring were maintained confidentially by Apple, were not generally available to the 22 public or competitors, and were developed at great expense and effort. OpenAI's possession and 23 distribution of Apple's internal departure procedures (which expressly reference Apple's IPA obliga- 24 tions), its recently hired former Apple employees' various efforts to avoid scrutiny and detection by 25 Apple, and its senior leadership's knowledge of Apple's confidentiality and exclusivity arrangements 26 with trusted partners foreclose any defense of ignorance. 27 121. To the extent that OpenAI's acts of misappropriation have occurred outside the United 28 States, including OpenAI's attempts to extract Apple's trade secrets from Apple's trusted overseas

1 suppliers, such conduct is unlawful under the Defend Trade Secrets Act, as OpenAI has acted domes- 2 tically in furtherance of the misappropriation. For example, OpenAI is headquartered in San Fran- 3 cisco and organized under the laws of the United States (Delaware), and intends to use and is using 4 Apple's misappropriated trade secrets in the United States to develop, manufacture, and commercial- 5 ize products that will be marketed, and sold to American consumers. OpenAI in the United States has 6 directed, coordinated, supported, or benefited from, its misappropriation of Apple's trade secrets, and 7 any products or services incorporating or resulting from Apple's trade secrets will be developed and 8 offered in the United States. 9 122. OpenAI's misappropriation was willful and malicious, entitling Apple to exemplary 10 damages under 18 U.S.C. § 1836(b)(3)(C). 11 123. OpenAI's misappropriation has caused and continues to cause damage to Apple, in- 12 cluding loss of competitive advantage, diminishment of the economic value of its trade secrets and 13 confidential information, and ongoing threat of further harm. OpenAI has been unjustly enriched by 14 avoiding the substantial investment Apple has made, for which Apple will seek damages in an amount 15 to be determined at trial. 16 124. Apple has no adequate remedy at law. Unless enjoined, OpenAI will continue to use 17 and benefit from Apple's

misappropriated information. Apple is entitled to preliminary and perma- 18 nent injunctive relief, including: an order (i) requiring OpenAI, its officers, agents, servants, employ- 19 ees, and attorneys, and all persons and entities acting in active concert or participation with them to 20 immediately preserve and not delete or destroy evidence in any format relevant to Apple's claims in 21 this action; (ii) enjoining OpenAI from further acquiring, possessing, using, or disclosing Apple's 22 trade secrets and confidential information; (iii) enjoining OpenAI from altering or destroying any 23 evidence related to its conduct; and (iv) requiring OpenAI to return all copies of Apple's trade secrets 24 and confidential information in its possession. 25

26 27

28

1 FOURTH CLAIM FOR RELIEF 2 Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 3 18 U.S.C. §§ 1832(a), 1836-37, 1839 et seq. 4 (Against io Products) 5 125. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as 6 though fully set forth herein. 7 126. Apple is the owner of certain valuable trade secrets and confidential information relat- 8 ing to each category identified above. This information constitutes "trade secrets" within the meaning 9 of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory 10 definition of trade secret, it nonetheless constitutes Apple Confidential Information protected under 11 Apple's IPA and other applicable contracts and laws. 12 127. Apple's trade secrets and confidential information derive independent economic value, 13 both actual and potential, from not being generally known to, and not being readily ascertainable 14 through proper means by, other persons or entities who might obtain economic value from their dis- 15 closure or use. Apple has invested hundreds of billions of dollars and decades of research and devel- 16 opment to develop its trade secrets and confidential information, establishing operational excellence 17 that cannot be readily replicated without the same investments Apple has made. If these trade secrets 18 and confidential information were publicly known, competitors could quickly exploit Apple's inno- 19 vations without incurring the substantial costs and years of experimentation that Apple undertook, 20 harming the value of Apple's innovations and eroding the competitive advantage those investments 21 have created. 22 128. io's own conduct demonstrates the economic value of Apple's trade secrets and confi- 23 dential information. Rather than invest the time and resources necessary to further its hardware aspi- 24 rations, io seeks to misappropriate Apple's innovations to accelerate efforts to bring consumer hard- 25 ware products to market. 26 129. Apple's trade secrets and confidential information relate to products used, sold, pur- 27 chased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign com- 28 merce—including Apple's iPhone, Apple Watch, and MacBook product lines, which are designed,

1 manufactured through global supply chains, and sold to consumers worldwide. io was incorporated 2 and operated as a hardware development company to develop devices for commercial sale in inter- 3 state and foreign commerce. io has acquired and is deploying Apple's trade secrets and confidential 4 information to develop and commercialize hardware devices for OpenAI, which it intends to sell to 5 consumers in interstate and foreign commerce. 6 130. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy 7 of its trade secrets and confidential information. 8 131. io has misappropriated Apple's trade secrets and confidential information by acquiring 9 and using them by improper means, including by at least: approaching Apple's suppliers and partners 10 using misappropriated trade secrets to extract still more of Apple's confidential and proprietary tech- 11 nology; inducing breach of partners' confidentiality obligations and use restrictions; directing exfil- 12 tration and disclosure of Apple's trade secrets through its interview process; obtaining and/or main- 13 taining unauthorized access to Apple's confidential systems and illicitly communicating about Ap- 14 ple's confidential information and trade secrets through Apple personnel without authorization, in- 15 cluding about ongoing confidential Apple engineering and product development projects; exfiltrating 16 Apple's trade secrets and confidential information for use outside of Apple; using Apple's internal 17 project codes and technical terminology to probe for and extract Apple's trade secrets; and deploying 18 Apple's institutional knowledge in hardware development, supply chain and partner operations and 19 communications, and hiring decisions. 20 132. At no time has Apple consented to io's improper acquisition, disclosure, or use of Ap- 21 ple's trade secrets or confidential information. 22 133. io knew, or had reason to know, that the trade secrets and confidential information it 23 was acquiring were maintained confidentially by Apple, were not generally available to the public or 24 competitors, and were developed at great expense and effort. io's recently hired former Apple em- 25

ployees' various efforts to avoid scrutiny and detection by Apple, and its senior leadership's 26 knowledge of Apple's confidentiality and exclusivity arrangements with trusted partners foreclose 27 any defense of ignorance. 28

1 134. To the extent that io's acts of misappropriation have occurred outside the United States, 2 including io's attempts to extract Apple's trade secrets from Apple's trusted overseas suppliers, such 3 conduct is unlawful under the Defend Trade Secrets Act as io has acted domestically in furtherance 4 of the misappropriation. For example, io is headquartered in San Francisco and organized under the 5 laws of the United States (Delaware), and intends to use and is using Apple's misappropriated trade 6 secrets in the United States to develop, manufacture, and commercialize products that will be mar- 7 keted, and sold to American consumers. io in the United States has directed, coordinated, supported, 8 or benefited from, its misappropriation of Apple's trade secrets, and any products or services incor- 9 porating or resulting from Apple's trade secrets will be developed and offered in the United States. 10 135. io's misappropriation was willful and malicious, entitling Apple to exemplary damages 11 under 18 U.S.C. § 1836(b)(3)(C). 12 136. io's misappropriation has caused and continues to cause damage to Apple, including 13 loss of competitive advantage, diminishment of the economic value of its trade secrets and confiden- 14 tial information, and ongoing threat of further harm. io has been unjustly enriched by avoiding the 15 substantial investment Apple has made, for which Apple will seek damages in an amount to be de- 16 termined at trial. 17 137. Apple has no adequate remedy at law. Unless enjoined, io will continue to use and 18 benefit from Apple's misappropriated information. Apple is entitled to preliminary and permanent 19 injunctive relief, including: an order (i) requiring io, its officers, agents, servants, employees, and 20 attorneys, and all persons and entities acting in active concert or participation with them to immedi- 21 ately preserve and not delete or destroy evidence in any format relevant to Apple's claims in this 22 action; (ii) enjoining io from further acquiring, possessing, using, or disclosing Apple's trade secrets 23 and confidential information; (iii) enjoining io from altering or destroying any evidence related to its 24 conduct; and (iv) requiring io to return all copies of Apple's trade secrets and confidential information 25 in its possession. 26 27

28

1 FIFTH CLAIM FOR RELIEF 2 Breach of Intellectual Property Agreement 3 (Against Chang Liu) 4 138. Apple re-alleges and incorporates by reference Paragraphs 1-98 of this Complaint as 5 though fully set forth herein. 6 139. Mr. Liu voluntarily entered into a valid, binding, and enforceable IPA with Apple as a 7 condition of his employment. 8 140. The IPA imposes obligations that survive termination of employment, including pro- 9 hibitions on the use and disclosure of Proprietary Information and an obligation to promptly return 10 all Apple property, documents, and materials containing Proprietary Information upon termination. 11 141. Apple has fully performed all of its obligations under the IPA. 12 142. Under the terms of the IPA, Mr. Liu agreed to "promptly deliver to Apple all docu- 13 ments and materials of any kind pertaining to your work at Apple" and to "not take with you any 14 documents, materials, or copies thereof, whether on paper or any other medium, containing any Pro- 15 prietary Information." 16 143. Under the terms of the IPA, Mr. Liu agreed that his "employment by Apple prohibits 17 you, during or after employment, from using or disclosing, or permitting any other person or entity 18 to use or disclose, any Proprietary Information without the written consent of Apple, except as nec- 19 essary to perform your duties as an employee of Apple." 20 144. Under the terms of the IPA, Mr. Liu agreed to "strictly comply with all of Apple's rules 21 and policies regarding Proprietary Information and use best efforts to safeguard such Proprietary In- 22 formation and protect it against disclosure, misuse, loss, or theft." 23 145. Mr. Liu materially breached the IPA at least by: failing to return an Apple-issued work 24 device upon his departure from Apple; soliciting and receiving Proprietary Information, including 25 about confidential ongoing Apple projects, after his departure from Apple and while working for 26 OpenAI; directing a still-employed Apple colleague to access and copy files including Proprietary 27 Information and coaching her to evade Apple's security; receiving, accessing, and directing the cop- 28 ying of Proprietary Information without authorization; failing to return Proprietary Information upon

1 his departure from Apple; accessing and downloading Proprietary Information without authorization 2 following his departure from Apple; and failing to comply with Apple's rules and policies regarding 3 Proprietary Information and use best efforts to safeguard and protect such Proprietary Information. 4 146. As a direct and proximate result

of Mr. Liu's breach, Apple has been damaged. 5 147. Apple has suffered and will continue to suffer irreparable harm for which there is no 6 adequate remedy at law, and Apple is entitled to preliminary injunctive relief against further breaches 7 of the IPA. 8 SIXTH CLAIM FOR RELIEF 9 Breach of Intellectual Property Agreement 10 (Against Tang Tan) 11 148. Apple re-alleges and incorporates by reference Paragraphs 1-85 and 99-111 of this 12 Complaint as though fully set forth herein. 13 149. Mr. Tan voluntarily entered into a valid, binding, and enforceable IPA with Apple as 14 a condition of his employment. 15 150. The IPA imposes obligations that survive termination of employment, including pro- 16 hibitions on the use and disclosure of Proprietary Information and an obligation to promptly return 17 all Apple property, documents, and materials containing Proprietary Information upon termination. 18 151. Apple has fully performed all of its obligations under the IPA. 19 152. Under the terms of the IPA, Mr. Tan agreed to "not take with you any documents, 20 materials, or copies thereof, whether on paper, magnetic or optical media or any other medium, con- 21 taining any Proprietary Information." 22 153. Under the terms of the IPA, Mr. Tan agreed that his "employment by Apple requires 23 you to keep all Proprietary Information in confidence and trust for the tenure of your employment 24 and thereafter, and that you will not use or disclose Proprietary Information without the written con- 25 sent of Apple except as necessary to perform your duties as an employee of Apple." 26 154. Mr. Tan materially breached the IPA at least by: using Proprietary Information in job 27 interviews of Apple employees, including to extract additional Proprietary Information; directing 28

1 candidates to bring and discuss Apple work product, including Proprietary Information, to OpenAI 2 interviews; retaining and using Proprietary Information for the benefit of a competitor. 3 155. As a direct and proximate result of Mr. Tan's breach, Apple has been damaged and is 4 entitled to damages in an amount to be proven at trial. 5 156. Apple has suffered and will continue to suffer irreparable harm for which there is no 6 adequate remedy at law, and Apple is entitled to preliminary and/or permanent injunctive relief 7 against further breaches of the IPA. 8 DEMAND FOR JURY TRIAL 9 157. Plaintiff Apple demands a trial by jury on all issues so triable. 10 PRAYER FOR RELIEF 11 Wherefore, Plaintiff prays for relief and judgment from this Court as follows: 12 1. Judgment in Apple's favor against all Defendants on the claims for relief alleged 13 herein. 14 2. For the entry of a Preliminary and Permanent Injunction against Defendants, their of- 15 ficers, agents, servants, employees, and attorneys and all others who are in active concert or participation with them, to prevent the actual or threatened misappropria- 16 tion of Apple's trade secrets. 17 3. For a Preliminary and Permanent Injunction prohibiting Defendants, and all those acting on their behalf or in active concert or participation with them, from possessing, 18 using, or disclosing Apple's trade secrets and confidential information. 19 4. For a Preliminary Injunction restraining and enjoining Defendants, their officers, 20 agents, servants, employees, and attorneys and all others who are in active concert or participation with them, from altering, destroying, or disposing of any evidence, in 21 any form, relating to this action, including without limitation emails, electronic docu- ments, metadata, and directories. 22 5. For an Order directing Defendants, their officers, agents, servants, employees, and 23 attorneys and all others who are in active concert or participation with them, to return 24 all of Apple's property in their possession, custody, or control and cease any access to or use of Apple's trade secrets. 25 6. For a declaration that Defendants have no rights or privileges to use Apple's confi- 26 dential information or trade secrets. 27 7. Damages sufficient to compensate for the actual loss caused by Defendants' trade se- 28 cret misappropriation and breach of contract.

1 8. A further award of monetary recovery for any unjust enrichment caused by Defend- ants' trade secret misappropriation. 2 9. In lieu of damages measured by any other methods, a reasonable royalty for Defend- 3 ants' misappropriation of trade secrets. 4 10. Exemplary damages, based on Defendants' willful and malicious appropriation of 5 trade secrets.

6 11. For prejudgment and post-judgment interest at the maximum legal rate as applicable, as an element of damages that Apple has suffered as a result of Defendants' wrongful 7 and unlawful acts. 8 12. For reasonable attorneys' fees and costs incurred herein as allowed under the Defend 9 Trade Secrets Act.

10 13. For such other and further relief as the Court deems just and proper.

11

12 Dated: July 10, 2026 Respectfully submitted, 13 WEIL, GOTSHAL & MANGES LLP 14 /s/ Gabriel S. Gross 15 Gabriel S. Gross (SBN 254672) Gaby LaHatte (SBN 321844) 16 Vanessa K. Sim (SBN 341107) WEIL, GOTSHAL & MANGES LLP 17 201 Redwood Shores Parkway Redwood Shores, California 94065 18 Telephone: (650)

802-3000 Facsimile: (650) 802-3100 19 gabe.gross@weil.com vanessa.sim@weil.com 20 gaby.lahatte@weil.com 21 Christopher W. Henry (pro hac vice forthcoming) 22 WEIL, GOTSHAL & MANGES LLP 1001 Boylston Street, Suite 300 23 Boston, Massachusetts 02115 Telephone: (617) 772-8300 24 Facsimile: (617) 772-8333 chris.henry@weil.com 25 Rachel L. Weiner Cohen 26 (pro hac vice forthcoming) Nicole Elena Bruner 27 (pro hac vice forthcoming) WEIL, GOTSHAL & MANGES LLP 28 2001 M Street NW, Suite 600 Washington, DC 20036 COMPLAINT 39 Case 5:26-cv-07078 Document 1 Filed 07/10/26 Page 41 of 41

1 Telephone: (202) 682-7000 Facsimile: (202) 857-0940 2 rachel.cohen@weil.com nicole.bruner@weil.com 3 Heather Blacklaws 4 (pro hac vice forthcoming) WEIL, GOTSHAL & MANGES LLP 5 600 Congress Avenue, Suite 2170 Austin, Texas 78701 6 Telephone: (512) 487-1480 Facsimile: (512) 487-1520 7 heather.blacklaws@weil.com 8 Nina Shapiro (pro hac vice forthcoming) 9 WEIL, GOTSHAL & MANGES LLP 767 5th Avenue 10 New York, New York 10153 Telephone: (212) 310-8000 11 Facsimile: (212) 310-8007 nina.shapiro@weil.com 12 Attorneys for Plaintiff Apple Inc. 13

14

15

16

17

18

19 20

21

22

23

24

25

26 27

28

COMPLAINT 40