Gabriel S. Gross (SBN 254672)
WEIL, GOTSHAL & MANGES LLP
201 Redwood Shores Parkway
Redwood Shores, California 94065
Telephone: (650) 802-3000
Facsimile: (650) 802-3100
gabe.gross@weil.com

Christopher W. Henry (*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
1001 Boylston Street, Suite 300
Boston, Massachusetts 02115
Telephone: (617) 772-8300
Facsimile: (617) 772-8333
chris.henry@weil.com

Attorneys for Plaintiff Apple Inc.

[Additional Counsel listed in signature block]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

APPLE INC., Plaintiff, vs. CHANG LIU, TANG YEW TAN, OPENAI FOUNDATION f/k/a OPENAI, INC., OPENAI GROUP PBC, and IO PRODUCTS, LLC f/k/a IO PRODUCTS, INC., Defendants.	Case No. **COMPLAINT FOR TRADE SECRET MISAPPROPRIATION AND BREACH OF CONTRACT** **DEMAND FOR JURY TRIAL**

Apple brings this action against Chang Liu and Tang Yew Tan ("Mr. Liu" and "Mr. Tan," respectively and collectively, the "Individual Defendants"), OpenAI Foundation and OpenAI Group PBC (collectively, "OpenAI"), and io Products, LLC ("io") (OpenAI and io collectively, the "Corporate Defendants"), and alleges as follows:

INTRODUCTION

1. This case is about Apple's former employees stealing Apple's trade secrets for the benefit of OpenAI. Apple brings this suit to put a stop to it.

2. Apple has invested hundreds of billions of dollars and decades of effort in developing groundbreaking consumer hardware products like iPhone, Apple Watch, and MacBook, along with the business acumen and infrastructure to bring them to market at scale. This sustained and focused investment of time, talent, and resources has produced engineering breakthroughs, manufacturing and supply chain innovations, and a global network of strategic partnerships—all built on confidentiality and trust. Apple surprises and delights its customers each year with innovative new hardware products, keeping much of its work secret until the moment its finished products are ready to be revealed.

3. Behind the scenes, Apple keeps its product development, manufacturing, supply chain, technology research, and other innovations confidential. The trade secrets spanning Apple's hardware operations collectively constitute one of the most valuable intellectual assets in all of American business. They enable Apple to bring new products with unique features to consumers at extraordinary speed and scale. Apple takes the confidentiality of its trade secrets seriously. In the rare situation where Apple becomes aware that its confidential information may have been compromised—by a third party, a partner, an employee, or anyone else—it investigates and works to contain and resolve any issues. This case arises from such an investigation. Apple has uncovered a pattern of theft of Apple's trade secrets by OpenAI employees who were formerly at Apple.

4. Chang Liu spent eight years at Apple as a Senior System Electrical Engineer, working on some of Apple's most sensitive product development programs. Apple entrusted him with highly confidential and trade secret information. Mr. Liu left in January 2026 to join OpenAI. When Apple contacted Mr. Liu to sign Apple's confidentiality reminder, schedule an exit interview, and confirm that he had returned his devices and complied with other exit procedures, Mr. Liu did not respond.

5. Mr. Liu has taken steps to hide the full extent of his theft, which Apple is still investigating, but the investigation already has revealed troubling facts:

- After leaving Apple, Mr. Liu failed to return an Apple-issued work laptop that he had previously authenticated to Apple's network. In a message left on a former colleague's Apple-issued work laptop he said, "I still have another computer" on which he planned to access Apple information.
- While employed by OpenAI, he accessed and used his former colleague's Apple-issued work computer that was authenticated to Apple's network, without Apple's authorization.
- While employed by OpenAI, Mr. Liu also exploited a rare, previously unknown authentication bug to access Apple's shared network folders.[1] Upon discovering that he had this unauthorized access to Apple's systems, Mr. Liu did not report it, return his stolen Apple-issued work laptop, or delete the program that allowed the access.
- Instead, he celebrated his improper access, exclaiming in a message left on his colleague's Apple-issued work laptop "LOL" and that it was "so funny." Then, over several weeks, while developing hardware for OpenAI, Mr. Liu surreptitiously accessed and downloaded dozens of Apple's confidential hardware-related files, including voluminous, detailed information about unreleased products, engineering presentations, technical specifications, and proprietary project data.

6. Messages left on an Apple-issued work laptop revealed that Mr. Liu also coached his former Apple colleague (whom he was recruiting to join OpenAI) on ways to "avoid trouble with the security team" when copying confidential Apple files. Knowing that OpenAI interviews would involve discussing Apple technology, Mr. Liu advised her on which confidential Apple material about unannounced Apple products she should study before her interview. To hide his illegal activity, Mr. Liu directed her to communicate with him privately over a separate messaging app.

[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 stolen Apple's confidential information.

7. As Apple continued investigating, a broader pattern emerged. Mr. Liu was not the only one using Apple's proprietary information to OpenAI's advantage. Other former Apple employees who had gone to work for OpenAI emailed themselves Apple's confidential information to personal accounts on their way out the door. And others were improperly using their knowledge of Apple's confidential and trade secret information to assist OpenAI in developing hardware.

8. Tang Yew Tan spent twenty-four years at Apple, most recently as Vice President of Product Design for iPhone and Apple Watch. Today he is OpenAI's Chief Hardware Officer. Apple entrusted Mr. Tan with its most sensitive projects, trusted partner relationships, proprietary manufacturing techniques, and unreleased products. Apple's investigation has revealed that Mr. Tan has been methodically using Apple's confidential information to benefit OpenAI.

9. In the months before he left Apple, Mr. Tan met with OpenAI or its collaborators and discussed meetings with a key Apple supplier. He began emailing himself information about Apple's suppliers and internal summaries of the consumer electronics industry. And today, when interviewing Apple employees for jobs at OpenAI, Mr. Tan uses Apple's confidential information to gain access to even more insider knowledge. He has used an Apple internal project codename to ask, "What's the plan[?]" for an unannounced Apple product. He has directed job candidates still working for Apple to bring "Actual parts" from Apple to their interviews for "show and tell" sessions in which he and his team at OpenAI can elicit still more Apple confidential information. These directions to bring Apple's parts to OpenAI job interviews surprised at least one of the candidates, who commented that he "didn't even know we could take those from the office."

10. This is part of OpenAI's strategy to extract Apple's confidential information. OpenAI has been instructing Apple employees to bring "CAD/design artifacts" and "prototypes" to their interviews and to divulge details about their work such as "subsystem and component selection," the "tools or methodologies you use for system integration, such as CAD software, simulation tools," and "Vendor selection and communication/collaboration with vendors."

11. OpenAI also instructs new hires on how to avoid scrutiny when they leave Apple. For example, Mr. Tan warns them not to tell Apple that they have taken jobs at OpenAI, so they can stay at Apple as long as they can. After his own departure, Mr. Tan improperly retained or obtained an

internal Apple managers' document marked "Need to Know" that describes security procedures for employee departures. Messages left on Apple-issued work devices show that Mr. Tan and his OpenAI colleagues have been sharing this document with new hires before they give notice to Apple of their departures, previewing Apple's security protocols. Unsurprisingly, Apple's investigation has found a pattern by employees who depart for OpenAI of taking steps to evade the security processes intended to protect Apple's confidential information.

12. OpenAI and its cohorts have been engaging in a coordinated pattern of misconduct at an institutional level as well. This includes io (which OpenAI acquired), a venture co-founded by Mr. Tan and other former Apple leaders. The Corporate Defendants, with or through their employees or partners, have been acting in concert and as an enterprise, exploiting Apple's confidential information to advance OpenAI's efforts to enter the consumer hardware market. They have used confidential Apple information in approaching Apple's trusted partners, even having one carry out a specific trade secret metal-finishing technique for OpenAI, misleading the partner to believe they had Apple's permission to do so.

13. This is the tip of the iceberg. Apple lacks visibility into what's been happening behind closed doors at OpenAI, where such misconduct is normalized and exemplified by leadership. This much is clear, however: at every level, from members of its Technical Staff to its Chief Hardware Officer, and in coordination with business partners, OpenAI has been stealing Apple's trade secrets and confidential information. As a natural result, OpenAI's nascent hardware business now rests on the shakiest of foundations, rotten to its core by its illegal reliance on misappropriated trade secrets.

14. In February as its investigation was in its early stages, Apple wrote OpenAI to raise its concerns that Apple's confidential information could be making its way into OpenAI's business improperly. Apple asked OpenAI to discuss what precautions OpenAI was taking to avoid this problem, to investigate it, and to remediate any issues. OpenAI never responded. This necessitated Apple's further investigation, revealing the alarming unlawful conduct discussed above.

15. Apple does not bring this action lightly. Apple operates in the most competitive markets in the world and focuses on creating and shipping the very best products and services that embody its innovations. But it cannot tolerate the theft of its trade secrets. In light of the troubling evidence it

has seen so far, Apple is left with no choice. This lawsuit and the discovery process are needed to expose and begin to remedy the pervasive theft of Apple's trade secrets.

PARTIES

16. Apple is and at all times mentioned herein has been a California corporation, having its principal place of business at One Apple Park Way, Cupertino, California 95014.

17. Defendant Chang Liu, on information and belief, resides in Sunnyvale, California 94087. Mr. Liu has worked at OpenAI since January 2026. Mr. Liu worked at Apple for over eight years, where he served as a Senior System Electrical Engineer for Apple's iPhone product line, and executed Apple's Intellectual Property Agreement (IPA) as a condition of his employment.

18. Defendant Tang Yew Tan, on information and belief, resides in San Francisco, California. Mr. Tan was a co-founder and Chief Hardware Officer of io Products, LLC, which subsequently merged with OpenAI, and now is Chief Hardware Officer at OpenAI. Mr. Tan worked at Apple for over twenty-four years, where he served as Vice President of Product Design for Apple's iPhone and Apple Watch product lines, and executed Apple's IPA as a condition of his employment.

19. OpenAI Foundation is a registered nonprofit organization incorporated under the laws of Delaware, having its principal place of business as 1455 3rd Street, San Francisco, California 94158.

20. OpenAI Group PBC is a registered public benefit corporation registered under the laws of Delaware, having its principal place of business as 1455 3rd Street, San Francisco, California 94158. OpenAI Foundation and OpenAI Group PBC, collectively, are referred to herein as OpenAI.

21. io Products, LLC, formerly known as io Products, Inc., is a Delaware LLC registered to do business in California and having its principal place of business at 1455 3rd Street, San Francisco, California 94158.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises out of the violation of a federal law, the Defend Trade Secrets Act, 18 U.S.C. §§ 1836, et seq.

23. This Court also has supplemental jurisdiction over the asserted state law claims under 28 U.S.C. § 1367(a) because the federal and state law claims derive from a common nucleus of operative facts.

24. This Court has personal jurisdiction over the Individual Defendants because they reside in this District and purposefully directed their activities toward residents of this District. Each Individual Defendant executed an IPA with Apple that provides for personal jurisdiction in and venue in the federal courts within Santa Clara County, California. Apple's claims arise out of and relate to each Individual Defendant's contacts with this forum.

25. This Court has general personal jurisdiction over OpenAI because each OpenAI Defendant lists its principal place of business as 1455 3rd Street, San Francisco, California 94158 in its most recent filings with the California Secretary of State.

26. This Court has specific personal jurisdiction over OpenAI because each OpenAI Defendant has purposefully directed its activities toward residents of this District and the State of California, including by maintaining a place of business in this District, employing individuals in this District, and conducting substantial and continuous business operations in this District. Apple's claims arise out of and relate to each OpenAI Defendant's contacts with this forum, including each OpenAI Defendant's misappropriation of Apple's trade secrets in the forum to further its own development and commercialization efforts within the forum. The exercise of jurisdiction over each OpenAI Defendant comports with traditional notions of fair play and substantial justice, as each OpenAI Defendant is headquartered in this District, has availed itself of the privilege of conducting business here, and should reasonably anticipate litigation in this forum.

27. This Court has general personal jurisdiction over io because io lists its principal place of business as 1455 3rd Street, San Francisco, California 94158 in its most recent filings with the California Secretary of State.

28. This Court has specific personal jurisdiction over io because io has purposefully directed its activities toward residents of this District and the State of California, including by maintaining a place of business in this District, employing individuals in this District, and conducting substantial and continuous business operations in this District. Apple's claims arise out of and relate

to io's contacts with this forum, including io's misappropriation of Apple's trade secrets in the forum to further its own development and commercialization efforts within the forum. The exercise of jurisdiction over io comports with traditional notions of fair play and substantial justice, as io is headquartered in this District, has availed itself of the privilege of conducting business here, and should reasonably anticipate litigation in this forum.

29. This Court also has jurisdiction over io because io is an alter ego of OpenAI. By no later than OpenAI's acquisition of io, io operated as a team in OpenAI to design and develop hardware devices for OpenAI. io and OpenAI collectively do business as OpenAI.

30. Corporate filings for OpenAI and io state the same principal address. Brendan Herron, the CEO, Secretary, and CFO of io, is an employee of OpenAI and has been since 2023.

31. Apple is informed and believes that, at all relevant times, OpenAI directed and controlled the operations and assets of io. Specifically, OpenAI controlled all aspects of io's business decisions and day-to-day operations, including the decisions to hire certain employees, conduct interviews, contact and choose suppliers and vendors, and decide which hardware to design and develop. Apple is informed and believes that there has been such unity of interest and ownership between OpenAI and io that any individuality and separateness between them did not and does not exist.

32. Without individually binding io in this litigation, io will be free to create another corporate shell entity to continue to use Apple's trade secret information and other intellectual property in violation of law. Therefore, adherence to the fiction of the separate existence of io and OpenAI would permit abuse of any applicable privilege and promote an inequitable result.

33. Venue is proper pursuant to 28 U.S.C. § 1391, because Apple, Chang Liu, Tang Yew Tan, each OpenAI Defendant, and io reside in this District, do substantial business in this forum, and the events giving rise to this Complaint occurred in this forum. Venue is also proper for the Individual Defendants, both former Apple employees, because they have signed an Intellectual Property Agreement consenting to the personal jurisdiction of and venue in the state and federal courts within Santa Clara County, California. Individual Defendants, Chang Liu and Tang Yew Tan, also committed the wrongful acts within this District.

DIVISIONAL ASSIGNMENT

34. Pursuant to Civil Local Rule 3-2, this case should be assigned to the San Jose Division. Apple's Intellectual Property Agreement, executed and breached by each of the Individual Defendants, expressly states that "any judicial action between the parties relating to this Agreement will take place in Santa Clara County, California." This is such an action. Additionally, a substantial portion of the events giving rise to the claims has taken place in Santa Clara County.

BACKGROUND

I. OpenAI and Its Consumer Hardware Plans

35. OpenAI was founded in December 2015 as a nonprofit organization with an initial funding commitment of $1 billion.[2] The company's goal was "to advance digital intelligence in the way that is most likely to benefit humanity as a whole, unconstrained by a need to generate financial return."[3] Following the release of its now well-known artificial intelligence chatbot, ChatGPT, OpenAI experienced explosive growth and transformed from a nonprofit to a commercial enterprise.[4] The company's valuation soared from approximately $29 billion in 2023 to $852 billion by April 2026 and has continued growing at a rapid pace.[5] By October 2025, OpenAI had abandoned its "open" nonprofit philosophy in favor of profit maximization and embarked on an aggressive campaign to bring hardware devices to the market.[6] OpenAI now is preparing for its IPO, reportedly having "raised more than $180 billion from investors" and continuing to "burn through cash at a historic pace."[7] OpenAI's CEO, Sam Altman, is "under pressure from investors to show that the numbers work, while facing increasingly stiff competition from rivals."[8]

[2] https://time.com/7328674/openai-chatgpt-sam-altman-elon-musk-timeline/.

[3] *Id.*

[4] https://www.businessinsider.com/sam-altman.

[5] https://www.reuters.com/technology/openai-ouster-microsoft-ai-research-ceo-sam-altmans-tumultuous-weekend-2023-11-20/; https://www.businessinsider.com/sam-altman; https://techcrunch.com/2023/04/28/openai-funding-valuation-chatgpt/.

[6] https://www.businessinsider.com/sam-altman.

[7] https://www.cnbc.com/2026/05/20/openai-ipo-filing.html.

[8] *Id.*

36. In 2024, Tang Tan and other former senior Apple executives co-founded io Products as the dedicated hardware vehicle for OpenAI. In May 2025, OpenAI announced its acquisition of io for approximately $6.5 billion and proceeded to "officially merge[]" the already integrated io team with OpenAI.[9] Meanwhile, Mr. Tan became OpenAI's Chief Hardware Officer, overseeing a hardware division that hired scores of Apple engineers in the months that followed.

37. Also in 2025, OpenAI announced a partnership with Foxconn, Apple's iPhone assembler, for its own production and engaged Luxshare and Goertek, both established Apple suppliers, for components.[10]

38. By November 2025, OpenAI confirmed that it had completed its "first prototypes" of its device.[11] But under mounting pressure to deliver its first commercial hardware product and facing the reality that building a successful consumer device business from scratch is more complex, time-consuming, and difficult than it anticipated, OpenAI has resorted to taking unlawful shortcuts.

II. Apple and Its Trade Secrets

39. Apple receives substantial benefit from its investment and innovation in its interconnected ecosystem of proprietary information spanning hardware engineering, manufacturing design, supply chain, business operations, and institutional expertise across these and other domains. These innovations are critical drivers of Apple's business performance. OpenAI's goals in the consumer market would be immeasurably advanced and accelerated if it were permitted to freely exploit the secret technology, skills, and business acumen that Apple has spent decades developing and optimizing.

40. Apple's trade secrets include those described below. Each category of secrets derives independent economic value from its secrecy and has been the subject of Apple's extensive protective measures.

a. **Hardware Engineering and Product Design**: Apple's hardware engineering trade secrets include confidential hardware engineering information such as circuit and system

[9] https://openai.com/sam-and-jony/; https://techtime.news/2025/07/30/openai/.

[10] *Id*.

[11] https://www.cnbc.com/2025/11/24/openai-hardware-jony-ive-sam-altman-emerson-collective.html.

design specifications, component architecture, and power management innovations; proprietary product designs for current and future unreleased products, maintained under strict confidentiality using internal code names and need-to-know access controls; confidential product roadmaps, milestone schedules, and development timelines; AI and machine learning integration data developed for Apple's hardware products; and proprietary coexistence and electromagnetic interference engineering data, including testing methodologies and design solutions developed to manage signal interference—technical innovations that reflect years of work and investment.

b. **Manufacturing Design, Industrial Design, and Process Engineering**: Apple's engineers design and qualify best-in-class processes and techniques to meet Apple's exacting aesthetic and functional standards. Apple's unique product designs often re-quire custom machinery and processes for manufacturing. Accordingly, unlike competitors who buy off-the-shelf parts, Apple often designs and customizes the specialized, proprietary machinery used in its suppliers' factories, ensuring it can protect the design and development of current and future products along with its cutting-edge manufacturing techniques. Apple's trade secrets in this area include proprietary manufacturing processes, custom machinery, equipment designs and collections and configurations of equipment; proprietary metal alloys, metal-finishing techniques, and material specifications; Design for Manufacturability ("DFM") expertise—confidential optimization of manufacturing processes, part tolerances, and production scalability; and proprietary equipment housed at supplier facilities, subject to strict use restrictions.

c. **Component Technologies**: Apple's trade secrets in this area include proprietary component technologies developed in collaboration with trusted suppliers and sub-suppliers for specific Apple hardware programs—including power management integrated circuits, battery systems, and display, acoustic, and touch subsystems; the identities of the specialized sub-suppliers and vendors who collaborate with Apple on these technologies; the specific technical specifications, performance parameters, and design requirements Ap-

ple imposes on these components; and fully integrated, plug-and-play solutions engineered with specialized third-party vendors unique to Apple and protected by stringent confidentiality terms. These innovations reflect years of research, development, and investment that cannot be readily ascertained through reverse engineering or independent research alone.

d. **Proprietary Testing, Validation, and Development Methodologies:** Apple's trade secrets in this area include confidential testing data, performance evaluations, and trend analyses generated through extensive engineering investment; proprietary fabrication approval workflows and fabrication processes relating to the transition from design to manufacture; lifecycle simulation data and manufacturing process development records; failure analyses and technical evaluations documenting the resolution of engineering challenges; confidential development roadmaps identifying technical challenges, proposed solutions, and supplier collaboration strategies; and proprietary methodologies for evaluating tradeoffs between performance, reliability, cost, and manufacturability. These materials reflect years of accumulated engineering knowledge—including the negative know-how of what approaches have been tested, rejected, or refined—that cannot be replicated through reverse engineering or independent research and that provide a comprehensive window into Apple's hardware development processes.

e. **Global Supply Chain Operations, Supplier Relationships, and Proprietary Business Operations**: Apple's trade secrets in this area include confidential contractual arrangements with suppliers; supplier qualification and allocation strategies; logistics coordination processes that synchronize global component delivery at scale; and proprietary supplier relationships—including the identities and roles of specialized sub-suppliers and vendors who provide Apple with critical components and equipment. Apple has painstakingly developed its supplier network and invested in components and production capacity years in advance to maintain its highly complex operations with exceptional precision. Apple also maintains confidential information regarding its project assignments and aggregated personnel information—information that, if obtained by a competitor,

could be used to strategically identify and recruit employees to acquire their institutional knowledge. Apple also possesses proprietary and secret information regarding how its global supply chain operations, supplier relationships, manufacturing design and process engineering know-how, DFM expertise, and component technologies interconnect and function together as an integrated whole. Apple's systems-level integration knowledge—the confidential coordination and management of its complex network of suppliers, sub-suppliers, vendors, and internal teams—is a trade secret in its own right. The know-how required to make these interconnected elements work together enables Apple to achieve efficiency, quality control, scalability, and speed-to-market that cannot be replicated without the investments in technology and innovation Apple has made over many years.

41. Each category derives independent economic value from its secrecy. Apple has invested hundreds of billions of dollars and decades of effort in developing this information and keeping it confidential. A competitor with access to it could bypass years of independent research and development, skip the capital expenditure required to build genuine expertise, and bring products to market faster and at lower cost—harming the value of Apple's investments. Rather than investing what legitimate development would require, OpenAI has turned to trade secret misappropriation to free-ride off Apple's decades of innovation.

III. Apple Diligently and Reasonably Protects Its Trade Secrets.

42. Apple protects its trade secrets and confidential information through reasonable contractual, technical, and physical measures.

43. As a condition of employment, Apple employees are required to sign an Intellectual Property Agreement ("IPA"), updated from time to time, which details their confidentiality and non-disclosure obligations.

44. Specifically, under an applicable version of the IPA, employees acknowledge that they are prohibited, "during or after employment, from using or disclosing, or permitting any other person or entity to use or disclose, any Proprietary Information without the written consent of Apple, except as necessary to perform [their] duties as an employee of Apple." The prohibition extends beyond the employee's own conduct; the IPA equally bars employees from "permitting any other person or entity

to use or disclose any Proprietary Information" without Apple's consent. Employees further agree to "strictly comply with all of Apple's rules and policies regarding Proprietary Information and use best efforts to safeguard such Proprietary Information and protect it against disclosure, misuse, loss, or theft." And upon departure, the IPA prohibits employees from taking "any documents, materials, or copies thereof, whether on paper or any other medium, containing any Proprietary Information."

45. Apple ensures its employees understand their obligations by providing trainings addressing their confidentiality obligations. For instance, Apple requires all its employees to take a "Business Conduct" course annually, in which Apple reinforces obligations to "protect Apple Confidential Information."[12]

46. Apple reminds departing employees of their ongoing confidentiality obligations under the IPA and reminds them to return any Apple proprietary information before leaving Apple. Apple follows departure procedures to protect its confidential information. Departing employees must return Apple-issued work devices, including laptops and mobile devices, as well as their badges and other Apple-owned equipment. When departing Apple, employees are reminded that their confidentiality obligations remain even after termination.

47. Apple ensures protection of its trade secrets and Apple Confidential Information stored in its secure network file repository, a third-party hosted cloud system that houses confidential engineering files, project documentation, and proprietary technical data, among other types of files. Network storage access at Apple is provisioned through Apple's Access Manager system under Apple's terms of use that limit access to only "for work purposes" and notes that stored files "may contain Apple Confidential Information—including any non-public details regarding our past, present, or future products and services." Apple disables and prohibits access to its network storage upon an employee's departure.

48. Apple engages in other extensive measures protecting its confidential and proprietary technology, including using database exchange and collaboration systems which include permission assignment to ensure access is on a need-to-know basis; requiring non-disclosure and/or confidentiality agreements with Apple's suppliers, vendors, contractors, and other third parties before providing

[12] https://www.apple.com/compliance/pdfs/Business-Conduct-Policy.pdf.

access to Apple's trade secrets, and even then only providing access to confidential information on a need-to-know basis; and maintaining high standards for encryption, password protection, and device authentication, among many other measures.

49. Apple uses locked buildings, security cameras, guards, and other measures to control access to its physical facilities. Apple restricts physical access to its buildings within the company. Badge access for Apple employees may be limited to certain buildings or portions of buildings depending on the employee's specific team and role. Any person who does not have a badge must be escorted by an Apple employee while within Apple's facilities.

50. Apple further protects its trade secrets by restricting access to its file repositories for projects to only those employees who are currently working on and authorized to view them. Apple strictly controls who is disclosed on a project and only permits individuals with a demonstrated business need to be disclosed.

51. Apple goes to great lengths to ensure that its trusted business partners, including vendors, laboratories, and other companies in its supply chain, commit to stringent confidentiality obligations. Suppliers working with Apple must sign restrictive confidentiality agreements to protect Apple's innovations. Suppliers are required to implement physical security measures, such as using qualified security teams, security cameras, sensors, personnel identification credential screening, and vehicle markings. Apple uses code names for projects to prevent leaks and requires suppliers to track all confidential materials, including by using proprietary chain-of-custody protocols for sensitive components to ensure secure disposal of scrap materials. Apple also maintains a proprietary shipping process to transport confidential prototypes between facilities.

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

IV. Defendants' Misappropriation of Apple's Trade Secrets and Confidential Information

53. Despite Apple's rigorous security measures and practices, Apple's trade secrets have been compromised through the deliberate misconduct by those previously entrusted with them. Apple's former engineers and executives—recruited, directed and rewarded by OpenAI—along with OpenAI itself and its business cohorts, have been stealing Apple's most sensitive information for a would-be competitor. With over four hundred former Apple employees now working at OpenAI, it is not surprising that certain OpenAI personnel have knowledge of Apple's confidential and proprietary information, which they are obligated to keep confidential. But OpenAI has resorted to exploiting this confidential information, using it to extract still more from Apple's current employees and trusted partners, and to structure its interview processes to try to solicit additional confidential Apple information—all while taking steps to conceal its actions. That OpenAI now employs people who were once entrusted with Apple's trade secrets does not entitle OpenAI to use that information to jumpstart its hardware efforts.[13]

A. Former Apple employees have taken Apple's trade secrets and confidential information to OpenAI.

54. Apple's investigation has uncovered misconduct reaching across seniority levels, technical disciplines, and departments at OpenAI. The following examples, drawn from Apple's ongoing internal investigation of information gleaned from Apple's company-owned devices and systems, begin to illuminate the scope and nature of the Defendants' unlawful conduct. While Apple's ongoing investigation has provided insights obtained from its own systems, Apple has virtually no visibility

[13] Apple and OpenAI have a commercial relationship involving the integration of OpenAI's ChatGPT into Apple Intelligence. The companies have entered into a written agreement governing that integration. That agreement is not at issue here. OpenAI's acts of trade secret misappropriation alleged herein do not arise from and have no connection to that agreement.

into what has been happening behind closed doors at OpenAI and io. Discovery will expose that the misappropriation has been occurring on a scale many times greater than the several instances described below.

1. Chang Liu, Member of Technical Staff at OpenAI

55. Chang Liu departed Apple on January 22, 2026 to join OpenAI. Like other Apple employees, Mr. Liu signed and is bound by an IPA obligating him to protect Apple's confidential information. Around the time of his departure, however, Mr. Liu was unresponsive to Apple's outreach trying to confirm whether he had returned his devices and complied with other exit procedures, scheduling an exit interview, and instructing him to sign Apple's confidentiality reminder. And, at the time of his departure, Mr. Liu failed to return at least one Apple-owned computer.

56. After leaving Apple, Mr. Liu maintained a close relationship with an employee who was still working at Apple, Yu-Ting "Alyssa" Peng, and he communicated with her frequently prior to her own departure for OpenAI on April 16, 2026. Within hours of leaving Apple, Mr. Liu shared with Ms. Peng, "I still have another computer" he was planning to use to access Apple's confidential information so he could discuss it with Ms. Peng that evening. Within weeks of departing Apple, Mr. Liu also used Ms. Peng's Apple-issued work computer that was authenticated to Apple's network—accessing it while she was still employed at Apple and he was not.

57. On or around February 9, 2026, weeks after he had left Apple and knowing he had no right to do so, Mr. Liu tried to access Apple's network storage—a cloud-based file repository containing Apple's confidential engineering files, project documentation, and other proprietary information. Mr. Liu discovered that, surprisingly, he still could access the Apple's network repository after leaving Apple, the result of a then-unknown authentication vulnerability. Rather than bringing this to Apple's attention or protecting Apple's confidential information as required by his IPA, Mr. Liu celebrated his find with Ms. Peng and set about exploiting it: "LOL, I found out I can access the [network storage], so funny." Ms. Peng's response was immediate: "I'm ready." Mr. Liu knew accessing Apple's network storage after he had left the company was unauthorized and prohibited, as he had agreed to the confidentiality restrictions of his IPA.

58. While employed by OpenAI, Mr. Liu then proceeded to select, access, and download dozens of confidential files from Apple's network repository. He downloaded confidential technical presentations, spreadsheets, PDFs, and written work product—including a compilation of technical files with over a thousand pages reflecting details of confidential work he and others did at Apple—many expressly labeled as confidential. He shared his findings with Ms. Peng, who was still employed by Apple, sending her links to Apple's proprietary materials—and directing her attention to specific project folders, engineering documentation, and technical data.

59. Among the files Mr. Liu downloaded is a presentation concerning the manufacture and testing of MLBs (multi-layer or main logic boards)—complex circuit boards in Apple's hardware. The presentation details the manufacturing process, testing workflows, data captured during testing and how to interpret it, and more, with photographs and accompanying analyses. It identifies specific equipment to perform these analyses and issues each piece of equipment is capable of diagnosing—proprietary operational knowledge that reflects years of accumulated testing experience and would be invaluable to anyone developing hardware.

60. Mr. Liu continued illicitly accessing and downloading Apple's confidential and proprietary information while he was developing products for OpenAI. Apple discovered Mr. Liu's misconduct through its own investigation. Once it learned of this security breach, Apple immediately took steps to ensure Mr. Liu's access was terminated.

61. At no point did Mr. Liu notify Apple or take steps to stop it. Only OpenAI and Mr. Liu know all the ways they have been exploiting the trove of Apple confidential information he stole, and to the extent they have not concealed or destroyed the evidence of these misappropriations, it will be investigated thoroughly in discovery.

62. Mr. Liu's theft of dozens of confidential files and trade secrets from Apple's network storage is not his only offense. For months while he was working for OpenAI, and while Ms. Peng was still working at Apple, Mr. Liu received from her frequent updates on Apple's active confidential projects, vendor decisions, and engineering details. Ms. Peng and Mr. Liu would engage in depth about those confidential projects, while Mr. Liu was working on developing OpenAI's competing

hardware. Mr. Liu's work for OpenAI was informed by a steadily flowing stream of Apple's trade secret information from Ms. Peng.

63. Before Ms. Peng left Apple for OpenAI in April, Mr. Liu also coached her on how to access and copy files from Apple workstations "to avoid trouble with the security team," and directed Ms. Peng to specific Apple project folders and proprietary engineering data.

64. Mr. Liu also equipped and prepared Ms. Peng with proprietary Apple information to use at her interview with OpenAI. Knowing OpenAI's interviewing practices and what technical expertise at Apple would be valuable to OpenAI, Mr. Liu instructed Ms. Peng on which of Apple's confidential information she should study in preparation for her OpenAI interviews.

65. Messages left on Apple-issued work devices show that Mr. Liu told Ms. Peng how another former Apple employee who had interviewed at OpenAI had "fumbled" his answers to questions that OpenAI's Chief Hardware Officer Tang Tan asked him about a top-secret project for an unreleased new Apple product. Hoping to help Ms. Peng prepare and better handle such questions, messages and other evidence shows that Mr. Liu helped Ms. Peng study, using, on information and belief, his illicit access to Apple's network storage to "download[] some info" for Ms. Peng's review. Ms. Peng was subsequently offered a position at OpenAI and departed Apple in April 2026.

66. Mr. Liu knew what he was doing was wrong, wanted to hide it from Apple, and took steps to keep it from being discovered. Although he and Ms. Peng sometimes communicated using Apple-owned devices, Mr. Liu recognized this could risk exposing his misdeeds and so told her they should communicate privately over an alternative platform, the LINE Messenger app, to try to avoid detection. To the extent they have not destroyed or concealed this evidence, it will be revealed through discovery.

67. While working for OpenAI, Mr. Liu acquired Apple's trade secrets by improper means—by his own unauthorized access and through his ongoing contact with Ms. Peng—knowing it was unauthorized. He used and disclosed those trade secrets for OpenAI's benefit. Expressing amusement upon discovering he could surreptitiously access troves of Apple trade secrets while working for OpenAI, downloading them repeatedly and deliberately, and using private channels to

hide his communications about his conduct lay bare his willful and malicious intent. Mr. Liu's material breaches of his contract are equally clear and deliberate: he accessed, copied, and directed the disclosure of Apple Confidential Information after his employment ended, in direct violation of his post-termination obligations.

2. **Tang Tan, Chief Hardware Officer at OpenAI**

68. Tang Tan is OpenAI's Chief Hardware Officer and has been centrally involved in OpenAI's extraction and improper use of proprietary Apple information.

69. Mr. Tan has unlawfully exploited Apple's trade secrets and other confidential information in recruiting Apple employees for OpenAI. For example, Mr. Tan has used Apple's internal project code names during OpenAI interviews to inquire about the status of Apple's confidential projects for developing unreleased products—reinforcing that Mr. Tan is using Apple's internal information to solicit its trade secrets from job candidates. For instance, in the hours before his OpenAI interview with Mr. Tan, a then-Apple employee began screenshotting and downloading files relating to a highly confidential Apple project. Then, in the interview, Mr. Tan solicited more information about that same Apple project. This has become an established pattern.

70. Mr. Tan has directed candidates to bring physical hardware components, "parts," and product samples from their Apple work to their OpenAI interviews for "show and tell" sessions that would disclose Apple's proprietary technologies. For example, messages left on an Apple-issued work device show that Mr. Tan instructed an Apple employee to "bring some parts [she] worked on" such as "Batteries," "SIP" (Systems-in-Package), "mlb" (multi-layer or main logic boards), and "shields" and that it may "be good to show" other interviewers these Apple components.

71. Apple has seen no evidence to date suggesting that OpenAI or Mr. Tan meaningfully tried to prevent or avoid the improper disclosure of Apple's confidential information during these "show and tell" sessions. To the contrary, this seems their very purpose.

72. This is emblematic of how OpenAI has been unlawfully extracting confidential Apple information through its recruiting processes more generally. First, to prepare for an interview with leaders at OpenAI, a candidate is encouraged to access and get ready to discuss some of Apple's most sensitive information. Then, in the interview, OpenAI leaders, who are former Apple insiders like

Mr. Tan, use Apple's internal project codes to ask about and receive more of Apple's trade secret information. Before the interview is over, OpenAI has used and acquired more confidential Apple information and "primed the pump" to keep it coming once the new hire arrives from Apple.

73. While employed at OpenAI, Mr. Tan also improperly retained or obtained an internal Apple document bearing a "Need to Know" designation that describes offboarding procedures for Apple's managers. The document details security processes Apple uses to protect the company's confidential information when one of its employees is leaving. OpenAI's personnel refer to this as "a checklist that Tang put together," though it is clearly an internal Apple document. Mr. Tan and OpenAI have disclosed it to recruited Apple employees before they notify Apple that they are leaving, providing them with advance notice of Apple's forensic and security checks.

74. These tactics appear to be having their desired effect. Apple has observed a recent trend of employees who are leaving Apple for OpenAI and taking steps to evade security measures. This includes ignoring outreach by security personnel to schedule exit processes and security reviews.

B. OpenAI has been stealing Apple's trade secrets and confidential information through current and former Apple employees.

75. OpenAI and its cohorts, led at least in part by former Apple employees, have recruited candidates from Apple, extracted their knowledge of Apple's sensitive and confidential information, and then continued to exploit that knowledge once they arrived. As a result, OpenAI has misappropriated Apple's trade secrets and confidential information in a variety of ways. For example, messages left on Apple-issued work laptops have revealed that:

a. OpenAI coaches candidates to prepare for their interviews by studying Apple's confidential engineering documentation, internal presentations, and proprietary technical materials. OpenAI then uses its insider Apple information to ask detailed questions to extract more: about Apple's proprietary tools, vendor management processes, engineering methodologies, manufacturing workflows, and supplier relationships, for example.

b. OpenAI asks candidates to prepare "Technical Deep Dive" presentations, complete with "slides (required)," about their work at Apple at such a level of detail that requires revealing Apple's confidential information. For example, OpenAI

instructs candidates to bring "CAD/design artifacts" and "prototypes" from their recent work at Apple. It asks Apple's employees to divulge their "subsystem and component selection" and information about Apple's "tools or methodologies you use for system integration, such as CAD software, simulation tools." It asks candidates to explain "Vendor selection and communication/collaboration with vendors" in Apple's prized network of partners.

c. OpenAI interviewers also request that Apple candidates bring "Actual parts" as "props" from Apple for "show and tell." For example, OpenAI has instructed Apple employees to bring "Batteries," "SIP" (systems-in-package), "mlb" (multi-layer or main logic boards), "shields," "piece parts," and "housings and BGs [back glass] in different colours," along with other hardware components and product samples from their Apple work. One candidate expressed concern over OpenAI's tactics, noting he was "surprised people have brought" Apple parts to interviews because he "didn't know we could take those from the office."

d. Panels of OpenAI interviewers use Apple's internal project code names, proprietary terminology, and knowledge to probe for secret information about Apple's projects and operations. OpenAI interviewers include former Apple employees such as Tang Tan who possess Apple's confidential information and know which questions will unlock more. No evidence that Apple has seen to date suggests that Defendants have taken steps to avoid the improper disclosure of Apple's confidential information during these interviews.

e. At OpenAI's instruction or for its benefit, departing Apple employees, around the time they are leaving Apple, send Apple's confidential information to their personal email accounts for future use in their work at OpenAI—including proprietary engineering data, manufacturing design documentation, and AI-related materials.

76. OpenAI is the beneficiary of every act described above. OpenAI's recruiting practices suggest it hires these individuals at least in part because of the confidential Apple-specific knowledge and expertise they have and could improperly obtain; OpenAI assesses and extracts that expertise and information; and OpenAI has been deploying it in its hardware development, supply chain and partner operations and communications, and hiring decisions.

77. OpenAI's conduct is knowing and deliberate, as demonstrated, for example, by its senior executives using Apple's internal project code names in interviews, asking candidates about confidential Apple projects, directing them to bring Apple parts and prototypes, distributing Apple's internal departure procedures to Apple employees before they announce their departures, which helps them avoid scrutiny, by OpenAI employees celebrating, using, and doing nothing to stop prohibited access to confidential Apple data and repositories, and by OpenAI employees communicating over private platforms to avoid detection.

78. This is a systematic effort to acquire, retain, and use Apple's trade secrets to help OpenAI try to replicate the secret technologies, business processes, and supply chain innovations that took Apple decades to build in its consumer hardware business.

C. OpenAI has been stealing Apple's trade secrets and confidential information through Apple's trusted partners.

79. OpenAI has not stopped at extracting Apple's trade secrets and confidential information through Apple's current and former employees. OpenAI also has been targeting Apple's prized partner network and supply chain directly. It has been using misappropriated knowledge of Apple's confidential relationships, manufacturing and design processes, and proprietary terminology to extract from trusted third parties additional trade secret information and processes.

80. As one example, OpenAI, including through io, has accessed, exploited, and used Apple's secret, proprietary industrial design techniques, processes, and know-how related to metal-finishing, at least by having a trusted Apple partner perform Apple's proprietary, trade secret processes for OpenAI's benefit. This is a third-party partner with whom Apple works on industrial design services and experimentation, including metal-finishing techniques, among others. The partner is bound by agreements with Apple that include use restrictions and confidentiality obligations prohibiting it

from doing for other companies the confidential work it does for Apple and from using certain facilities for anyone but Apple. Apple developed its proprietary, multi-step metal-finishing techniques over many years to ultimately produce the finishes that define the look and feel of Apple products.

81. Former Apple executives at OpenAI including Mr. Tan have confidential knowledge of Apple's use restrictions and confidentiality arrangement with this partner. Despite this, OpenAI, on its own or with or through its partner io, used, without authorization, Apple's proprietary and confidential metal-finishing processes, having the partner perform them for OpenAI's benefit, and in so doing, obtained products produced by exploiting misappropriated trade secrets. OpenAI and its cohorts misled the partner to believe they had Apple's permission to have the partner carry out the confidential metal-finishing technique for OpenAI's benefit.

82. Apple has not given OpenAI or io permission to use or a license to any of Apple's trade secrets or confidential information, including those it has entrusted with this partner.

83. OpenAI also has approached at least another trusted Apple supplier who works with Apple on manufacturing and manufacturing design, including with respect to power and batteries, among other things. OpenAI has been using Apple's confidential information and internal terminology about manufacturing design and specific component technologies to approach this trusted supplier and ask targeted questions (that only Apple-insiders would know to ask) about specific confidential Apple components that would be useful in furthering OpenAI's hardware ambitions.

D. OpenAI has been attempting to conceal its trade secret misappropriation.

84. OpenAI has actively coached Apple employees on how to manage their exits from Apple in ways that avoid scrutiny. This helps OpenAI's new hires evade Apple's security procedures and reduce the chance that their confidentiality violations and trade secret theft would be detected. OpenAI has been circulating to their new hires an internal Apple document bearing a "Need to Know" designation before they give notice to Apple of their departures. OpenAI has counseled departing employees not to disclose their next employer and given advice on how to avoid the "dreaded walk out" that would promptly remove them from the company rather than giving them a standard two weeks in which they could continue to access Apple's confidential information and trade secrets. And, review of Apple-issued work laptops has revealed that OpenAI has been advising Apple's departing employees that they "won't sign anything at the exit interview" and is instructing them that if Apple personnel "do ask you to sign anything" to let OpenAI know "asap."

85. Unsurprisingly, Apple has uncovered a concerning recent pattern among employees who depart and then go work for OpenAI. Departing employees have been taking actions to evade security measures, such as failing to provide two-weeks' notice, and ignoring outreach by security personnel to schedule exit processes and security reviews, all of which may help to conceal the misuse and misappropriation of confidential information.

FIRST CLAIM FOR RELIEF

Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1832(a), 1836-37, 1839 *et seq.*

(Against Chang Liu)

86. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as though fully set forth herein.

87. Apple is the owner of certain valuable trade secrets and confidential information relating to each category identified above. This information constitutes "trade secrets" within the meaning of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory definition of trade secret, it nonetheless constitutes Apple Confidential Information protected under Apple's IPA and other applicable contracts and laws.

88. Apple's trade secrets and confidential information derive independent economic value, both actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, other persons or entities who might obtain economic value from their disclosure or use. Apple has invested hundreds of billions of dollars and decades of research and development to develop its trade secrets and confidential information, establishing operational excellence that cannot be readily replicated without the same investments Apple has made. If these trade secrets and confidential information were publicly known, competitors could quickly exploit Apple's innovations without incurring the substantial costs and years of experimentation that Apple undertook, harming the value of Apple's innovations and eroding the competitive advantage those investments have created.

89. Mr. Liu's own conduct demonstrates the economic value of Apple's trade secrets and confidential information. Rather than invest the time and resources necessary to further OpenAI's hardware aspirations, Mr. Liu seeks to misappropriate Apple's innovations to accelerate efforts to bring consumer hardware products to market.

90. Apple's trade secrets and confidential information relate to products used, sold, purchased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign commerce—including Apple's iPhone, Apple Watch, and MacBook product lines, which are designed, manufactured through global supply chains, and sold to consumers worldwide. Mr. Liu acquired Apple's trade secrets and confidential information through improper means and used them while employed by OpenAI, a company developing and manufacturing hardware products for sale in interstate and foreign commerce.

91. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy of its trade secrets and confidential information.

92. Mr. Liu has misappropriated Apple's trade secrets and confidential information by acquiring and using them by improper means, including by at least: obtaining and/or maintaining unauthorized access to Apple's confidential systems and illicitly communicating about Apple's confidential information and trade secrets through Apple personnel without authorization, including about ongoing confidential Apple engineering and product development projects after his departure from

Apple; exfiltrating Apple's trade secrets and confidential information after his departure from Apple and for use outside of Apple; and deploying Apple's institutional knowledge in hardware development for OpenAI.

93. At no time has Apple consented to Mr. Liu's improper acquisition, disclosure, or use of Apple's trade secrets or confidential information.

94. Mr. Liu knew, or had reason to know, that the trade secrets and confidential information he was acquiring were maintained confidentially by Apple, were not generally available to the public or competitors, and were developed at great expense and effort. Mr. Liu's own employment and execution of an IPA with Apple foreclose any defense of ignorance.

95. To the extent that Mr. Liu's acts of misappropriation have occurred outside the United States, including any attempts to extract Apple's trade secrets from Apple's trusted overseas suppliers, such conduct is unlawful under the Defend Trade Secrets Act as Mr. Liu has acted domestically in furtherance of the misappropriation. For example, Mr. Liu resides in Sunnyvale and intends to use and is using Apple's misappropriated trade secrets in the United States to develop, manufacture, and commercialize products that will be marketed and sold to American consumers. Mr. Liu in the United States has directed, coordinated, supported, or benefited from, his misappropriation of Apple's trade secrets, and any products or services incorporating or resulting from Apple's trade secrets will be developed and offered in the United States.

96. Mr. Liu's misappropriation was willful and malicious.

97. Mr. Liu's misappropriation has caused and continues to cause damage to Apple, including loss of competitive advantage, diminishment of the economic value of its trade secrets and confidential information, and ongoing threat of further harm. Mr. Liu has been unjustly enriched by avoiding the substantial investment Apple has made.

98. Apple has no adequate remedy at law. Unless enjoined, Mr. Liu will continue to use and benefit from Apple's misappropriated information. Apple is entitled to preliminary injunctive relief, including: an order (i) requiring Mr. Liu to immediately preserve and not delete or destroy evidence in any format relevant to Apple's claims in this action; (ii) enjoining Mr. Liu from further acquiring, possessing, using, or disclosing Apple's trade secrets and confidential information; (iii)

enjoining Mr. Liu from altering or destroying any evidence related to his conduct; and (iv) requiring Mr. Liu to return all copies of Apple's trade secrets and confidential information in his possession.[14]

SECOND CLAIM FOR RELIEF

Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1832(a), 1836-37, 1839 *et seq.*

(Against Tang Tan)

99. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as though fully set forth herein.

100. Apple is the owner of certain valuable trade secrets and confidential information relating to each category identified above. This information constitutes "trade secrets" within the meaning of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory definition of trade secret, it nonetheless constitutes Apple Confidential Information protected under Apple's IPA and other applicable contracts and laws.

101. Apple's trade secrets and confidential information derive independent economic value, both actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, other persons or entities who might obtain economic value from their disclosure or use. Apple has invested hundreds of billions of dollars and decades of research and development to develop its trade secrets and confidential information, establishing operational excellence that cannot be readily replicated without the same investments Apple has made. If these trade secrets and confidential information were publicly known, competitors could quickly exploit Apple's innovations without incurring the substantial costs and years of experimentation that Apple undertook, harming the value of Apple's innovations and eroding the competitive advantage those investments have created.

102. Mr. Tan's own conduct demonstrates the economic value of Apple's trade secrets and confidential information. Rather than invest the time and resources necessary to further its hardware

[14] Mr. Liu's employment contract with Apple includes an arbitration clause with a clear exception for seeking preliminary injunctive relief in court. This suit is necessary so Apple may move for preliminary injunctive relief against Mr. Liu and other defendants collectively, which Apple will do promptly.

aspirations, Mr. Tan seeks to misappropriate Apple's innovations to accelerate efforts to bring consumer hardware products to market.

103. Apple's trade secrets and confidential information relate to products used, sold, purchased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign commerce—including Apple's iPhone and Apple Watch product lines that Mr. Tan oversaw as VP of Product Design, which are manufactured through global supply chains spanning multiple countries and sold internationally. Mr. Tan has used and disclosed Apple's trade secrets and confidential information to benefit OpenAI, a company developing and manufacturing hardware products for sale in interstate and foreign commerce.

104. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy of its trade secrets and confidential information.

105. Mr. Tan has misappropriated Apple's trade secrets and confidential information by acquiring and using them by improper means, including by at least: directing exfiltration and disclosure of Apple's trade secrets through the interview process; exfiltrating Apple's trade secrets and confidential information for use outside of Apple; using Apple's internal project codes and technical terminology to probe for and extract Apple's trade secrets; and deploying Apple's institutional knowledge in hardware development, supply chain and partner operations and communications, and hiring decisions.

106. At no time has Apple consented to Mr. Tan's improper acquisition, disclosure, or use of Apple's trade secrets or confidential information.

107. Mr. Tan knew, or had reason to know, that the trade secrets and confidential information he was acquiring were maintained confidentially by Apple, were not generally available to the public or competitors, and were developed at great expense and effort. Mr. Tan's own possession and distribution of Apple's internal departure procedures—which expressly reference Apple's IPA obligations—foreclose any defense of ignorance. Mr. Tan also executed his own IPA and served in a senior role with access to Apple's most sensitive information for over twenty-four years.

108. To the extent that Mr. Tan's acts of misappropriation have occurred outside the United States, including any attempts to extract Apple's trade secrets from Apple's trusted overseas suppliers, such conduct is unlawful under the Defend Trade Secrets Act, as Mr. Tan has acted domestically in furtherance of the misappropriation. For example, Mr. Tan resides in San Francisco and intends to use and is using Apple's misappropriated trade secrets in the United States to develop, manufacture, and commercialize products that will be marketed and sold to American consumers. Mr. Tan in the United States has directed, coordinated, supported, or benefited from, his misappropriation of Apple's trade secrets, and any products or services incorporating or resulting from Apple's trade secrets will be developed and offered in the United States.

109. Mr. Tan's misappropriation was willful, entitling Apple to exemplary damages under 18 U.S.C. § 1836(b)(3)(C).

110. Mr. Tan's misappropriation has caused and continues to cause damage to Apple, including loss of competitive advantage, diminishment of the economic value of its trade secrets and confidential information, and ongoing threat of further harm. Mr. Tan has been unjustly enriched by avoiding the substantial investment Apple has made, for which Apple will seek damages in an amount to be determined at trial.

111. Apple has no adequate remedy at law. Unless enjoined, Mr. Tan will continue to use and benefit from Apple's misappropriated trade secrets and confidential information. Apple is entitled to preliminary and permanent injunctive relief, including: an order (i) requiring Mr. Tan to immediately preserve and not delete or destroy evidence in any format relevant to Apple's claims in this action; (ii) enjoining Mr. Tan from further acquiring, possessing, using, or disclosing Apple's trade secrets and confidential information; (iii) enjoining Mr. Tan from altering or destroying any evidence related to his conduct; and (iv) requiring Mr. Tan to return all copies of Apple's trade secrets and confidential information in his possession.

THIRD CLAIM FOR RELIEF

Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1832(a), 1836-37, 1839 *et seq.*

(Against OpenAI)

112. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as though fully set forth herein.

113. Apple is the owner of certain valuable trade secrets and confidential information relating to each category identified above. This information constitutes "trade secrets" within the meaning of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory definition of trade secret, it nonetheless constitutes Apple Confidential Information protected under Apple's IPA and other applicable contracts and laws.

114. Apple's trade secrets and confidential information derive independent economic value, both actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, other persons or entities who might obtain economic value from their disclosure or use. Apple has invested hundreds of billions of dollars and decades of research and development to develop its trade secrets and confidential information, establishing operational excellence that cannot be readily replicated without the same investments Apple has made. If these trade secrets and confidential information were publicly known, competitors could quickly exploit Apple's innovations without incurring the substantial costs and years of experimentation that Apple undertook, harming the value of Apple's innovations and eroding the competitive advantage those investments have created.

115. OpenAI's own conduct demonstrates the economic value of Apple's trade secrets and confidential information. Rather than invest the time and resources necessary to further its hardware aspirations, OpenAI seeks to misappropriate Apple's innovations to accelerate its efforts to bring consumer hardware products to market.

116. Apple's trade secrets and confidential information relate to products used, sold, purchased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign commerce—including Apple's iPhone, Apple Watch, and MacBook product lines, which are designed,

manufactured through global supply chains, and sold to consumers worldwide. OpenAI has acquired and is deploying Apple's trade secrets and confidential information to develop and commercialize its own hardware devices, which it intends to sell to consumers in interstate and foreign commerce.

117. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy of its trade secrets and confidential information.

118. OpenAI has misappropriated Apple's trade secrets and confidential information by acquiring and using them by improper means, including by at least: approaching Apple's suppliers and partners using misappropriated trade secrets to extract still more of Apple's confidential and proprietary technology; inducing breach of partners' confidentiality obligations and use restrictions; directing exfiltration and disclosure of Apple's trade secrets through its interview process; obtaining and/or maintaining unauthorized access to Apple's confidential systems and illicitly communicating about Apple's confidential information and trade secrets through Apple personnel without authorization, including about ongoing confidential Apple engineering and product development projects; exfiltrating Apple's trade secrets and confidential information for use outside of Apple; using Apple's internal project codes and technical terminology to probe for and extract Apple's trade secrets; and deploying Apple's institutional knowledge in hardware development, supply chain and partner operations and communications, and hiring decisions.

119. At no time has Apple consented to OpenAI's improper acquisition, disclosure, or use of Apple's trade secrets or confidential information.

120. OpenAI knew, or had reason to know, that the trade secrets and confidential information it was acquiring were maintained confidentially by Apple, were not generally available to the public or competitors, and were developed at great expense and effort. OpenAI's possession and distribution of Apple's internal departure procedures (which expressly reference Apple's IPA obligations), its recently hired former Apple employees' various efforts to avoid scrutiny and detection by Apple, and its senior leadership's knowledge of Apple's confidentiality and exclusivity arrangements with trusted partners foreclose any defense of ignorance.

121. To the extent that OpenAI's acts of misappropriation have occurred outside the United States, including OpenAI's attempts to extract Apple's trade secrets from Apple's trusted overseas

suppliers, such conduct is unlawful under the Defend Trade Secrets Act, as OpenAI has acted domestically in furtherance of the misappropriation. For example, OpenAI is headquartered in San Francisco and organized under the laws of the United States (Delaware), and intends to use and is using Apple's misappropriated trade secrets in the United States to develop, manufacture, and commercialize products that will be marketed, and sold to American consumers. OpenAI in the United States has directed, coordinated, supported, or benefited from, its misappropriation of Apple's trade secrets, and any products or services incorporating or resulting from Apple's trade secrets will be developed and offered in the United States.

122. OpenAI's misappropriation was willful and malicious, entitling Apple to exemplary damages under 18 U.S.C. § 1836(b)(3)(C).

123. OpenAI's misappropriation has caused and continues to cause damage to Apple, including loss of competitive advantage, diminishment of the economic value of its trade secrets and confidential information, and ongoing threat of further harm. OpenAI has been unjustly enriched by avoiding the substantial investment Apple has made, for which Apple will seek damages in an amount to be determined at trial.

124. Apple has no adequate remedy at law. Unless enjoined, OpenAI will continue to use and benefit from Apple's misappropriated information. Apple is entitled to preliminary and permanent injunctive relief, including: an order (i) requiring OpenAI, its officers, agents, servants, employees, and attorneys, and all persons and entities acting in active concert or participation with them to immediately preserve and not delete or destroy evidence in any format relevant to Apple's claims in this action; (ii) enjoining OpenAI from further acquiring, possessing, using, or disclosing Apple's trade secrets and confidential information; (iii) enjoining OpenAI from altering or destroying any evidence related to its conduct; and (iv) requiring OpenAI to return all copies of Apple's trade secrets and confidential information in its possession.

FOURTH CLAIM FOR RELIEF

Misappropriation of Trade Secrets in Violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1832(a), 1836-37, 1839 *et seq.*

(Against io Products)

125. Apple re-alleges and incorporates by reference Paragraphs 1-85 of this Complaint as though fully set forth herein.

126. Apple is the owner of certain valuable trade secrets and confidential information relating to each category identified above. This information constitutes "trade secrets" within the meaning of 18 U.S.C. § 1839(3). To the extent any particular item is determined not to meet the statutory definition of trade secret, it nonetheless constitutes Apple Confidential Information protected under Apple's IPA and other applicable contracts and laws.

127. Apple's trade secrets and confidential information derive independent economic value, both actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, other persons or entities who might obtain economic value from their disclosure or use. Apple has invested hundreds of billions of dollars and decades of research and development to develop its trade secrets and confidential information, establishing operational excellence that cannot be readily replicated without the same investments Apple has made. If these trade secrets and confidential information were publicly known, competitors could quickly exploit Apple's innovations without incurring the substantial costs and years of experimentation that Apple undertook, harming the value of Apple's innovations and eroding the competitive advantage those investments have created.

128. io's own conduct demonstrates the economic value of Apple's trade secrets and confidential information. Rather than invest the time and resources necessary to further its hardware aspirations, io seeks to misappropriate Apple's innovations to accelerate efforts to bring consumer hardware products to market.

129. Apple's trade secrets and confidential information relate to products used, sold, purchased, or transported, or intended for use, sale, purchase, or transport, in interstate and foreign commerce—including Apple's iPhone, Apple Watch, and MacBook product lines, which are designed,

manufactured through global supply chains, and sold to consumers worldwide. io was incorporated and operated as a hardware development company to develop devices for commercial sale in interstate and foreign commerce. io has acquired and is deploying Apple's trade secrets and confidential information to develop and commercialize hardware devices for OpenAI, which it intends to sell to consumers in interstate and foreign commerce.

130. At all times relevant herein, Apple has taken reasonable measures to protect the secrecy of its trade secrets and confidential information.

131. io has misappropriated Apple's trade secrets and confidential information by acquiring and using them by improper means, including by at least: approaching Apple's suppliers and partners using misappropriated trade secrets to extract still more of Apple's confidential and proprietary technology; inducing breach of partners' confidentiality obligations and use restrictions; directing exfiltration and disclosure of Apple's trade secrets through its interview process; obtaining and/or maintaining unauthorized access to Apple's confidential systems and illicitly communicating about Apple's confidential information and trade secrets through Apple personnel without authorization, including about ongoing confidential Apple engineering and product development projects; exfiltrating Apple's trade secrets and confidential information for use outside of Apple; using Apple's internal project codes and technical terminology to probe for and extract Apple's trade secrets; and deploying Apple's institutional knowledge in hardware development, supply chain and partner operations and communications, and hiring decisions.

132. At no time has Apple consented to io's improper acquisition, disclosure, or use of Apple's trade secrets or confidential information.

133. io knew, or had reason to know, that the trade secrets and confidential information it was acquiring were maintained confidentially by Apple, were not generally available to the public or competitors, and were developed at great expense and effort. io's recently hired former Apple employees' various efforts to avoid scrutiny and detection by Apple, and its senior leadership's knowledge of Apple's confidentiality and exclusivity arrangements with trusted partners foreclose any defense of ignorance.

134. To the extent that io's acts of misappropriation have occurred outside the United States, including io's attempts to extract Apple's trade secrets from Apple's trusted overseas suppliers, such conduct is unlawful under the Defend Trade Secrets Act as io has acted domestically in furtherance of the misappropriation. For example, io is headquartered in San Francisco and organized under the laws of the United States (Delaware), and intends to use and is using Apple's misappropriated trade secrets in the United States to develop, manufacture, and commercialize products that will be marketed, and sold to American consumers. io in the United States has directed, coordinated, supported, or benefited from, its misappropriation of Apple's trade secrets, and any products or services incorporating or resulting from Apple's trade secrets will be developed and offered in the United States.

135. io's misappropriation was willful and malicious, entitling Apple to exemplary damages under 18 U.S.C. § 1836(b)(3)(C).

136. io's misappropriation has caused and continues to cause damage to Apple, including loss of competitive advantage, diminishment of the economic value of its trade secrets and confidential information, and ongoing threat of further harm. io has been unjustly enriched by avoiding the substantial investment Apple has made, for which Apple will seek damages in an amount to be determined at trial.

137. Apple has no adequate remedy at law. Unless enjoined, io will continue to use and benefit from Apple's misappropriated information. Apple is entitled to preliminary and permanent injunctive relief, including: an order (i) requiring io, its officers, agents, servants, employees, and attorneys, and all persons and entities acting in active concert or participation with them to immediately preserve and not delete or destroy evidence in any format relevant to Apple's claims in this action; (ii) enjoining io from further acquiring, possessing, using, or disclosing Apple's trade secrets and confidential information; (iii) enjoining io from altering or destroying any evidence related to its conduct; and (iv) requiring io to return all copies of Apple's trade secrets and confidential information in its possession.

FIFTH CLAIM FOR RELIEF

Breach of Intellectual Property Agreement

(Against Chang Liu)

138. Apple re-alleges and incorporates by reference Paragraphs 1-98 of this Complaint as though fully set forth herein.

139. Mr. Liu voluntarily entered into a valid, binding, and enforceable IPA with Apple as a condition of his employment.

140. The IPA imposes obligations that survive termination of employment, including prohibitions on the use and disclosure of Proprietary Information and an obligation to promptly return all Apple property, documents, and materials containing Proprietary Information upon termination.

141. Apple has fully performed all of its obligations under the IPA.

142. Under the terms of the IPA, Mr. Liu agreed to "promptly deliver to Apple all documents and materials of any kind pertaining to your work at Apple" and to "not take with you any documents, materials, or copies thereof, whether on paper or any other medium, containing any Proprietary Information."

143. Under the terms of the IPA, Mr. Liu agreed that his "employment by Apple prohibits you, during or after employment, from using or disclosing, or permitting any other person or entity to use or disclose, any Proprietary Information without the written consent of Apple, except as necessary to perform your duties as an employee of Apple."

144. Under the terms of the IPA, Mr. Liu agreed to "strictly comply with all of Apple's rules and policies regarding Proprietary Information and use best efforts to safeguard such Proprietary Information and protect it against disclosure, misuse, loss, or theft."

145. Mr. Liu materially breached the IPA at least by: failing to return an Apple-issued work device upon his departure from Apple; soliciting and receiving Proprietary Information, including about confidential ongoing Apple projects, after his departure from Apple and while working for OpenAI; directing a still-employed Apple colleague to access and copy files including Proprietary Information and coaching her to evade Apple's security; receiving, accessing, and directing the copying of Proprietary Information without authorization; failing to return Proprietary Information upon

his departure from Apple; accessing and downloading Proprietary Information without authorization following his departure from Apple; and failing to comply with Apple's rules and policies regarding Proprietary Information and use best efforts to safeguard and protect such Proprietary Information.

146. As a direct and proximate result of Mr. Liu's breach, Apple has been damaged.

147. Apple has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law, and Apple is entitled to preliminary injunctive relief against further breaches of the IPA.

SIXTH CLAIM FOR RELIEF

Breach of Intellectual Property Agreement

(Against Tang Tan)

148. Apple re-alleges and incorporates by reference Paragraphs 1-85 and 99-111 of this Complaint as though fully set forth herein.

149. Mr. Tan voluntarily entered into a valid, binding, and enforceable IPA with Apple as a condition of his employment.

150. The IPA imposes obligations that survive termination of employment, including prohibitions on the use and disclosure of Proprietary Information and an obligation to promptly return all Apple property, documents, and materials containing Proprietary Information upon termination.

151. Apple has fully performed all of its obligations under the IPA.

152. Under the terms of the IPA, Mr. Tan agreed to "not take with you any documents, materials, or copies thereof, whether on paper, magnetic or optical media or any other medium, containing any Proprietary Information."

153. Under the terms of the IPA, Mr. Tan agreed that his "employment by Apple requires you to keep all Proprietary Information in confidence and trust for the tenure of your employment and thereafter, and that you will not use or disclose Proprietary Information without the written consent of Apple except as necessary to perform your duties as an employee of Apple."

154. Mr. Tan materially breached the IPA at least by: using Proprietary Information in job interviews of Apple employees, including to extract additional Proprietary Information; directing

candidates to bring and discuss Apple work product, including Proprietary Information, to OpenAI interviews; retaining and using Proprietary Information for the benefit of a competitor.

155. As a direct and proximate result of Mr. Tan's breach, Apple has been damaged and is entitled to damages in an amount to be proven at trial.

156. Apple has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law, and Apple is entitled to preliminary and/or permanent injunctive relief against further breaches of the IPA.

DEMAND FOR JURY TRIAL

157. Plaintiff Apple demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

Wherefore, Plaintiff prays for relief and judgment from this Court as follows:

1. Judgment in Apple's favor against all Defendants on the claims for relief alleged herein.

2. For the entry of a Preliminary and Permanent Injunction against Defendants, their officers, agents, servants, employees, and attorneys and all others who are in active concert or participation with them, to prevent the actual or threatened misappropriation of Apple's trade secrets.

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, using, or disclosing Apple's trade secrets and confidential information.

4. For a Preliminary Injunction restraining and enjoining Defendants, their officers, 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 any form, relating to this action, including without limitation emails, electronic documents, metadata, and directories.

5. For an Order directing Defendants, their officers, agents, servants, employees, and attorneys and all others who are in active concert or participation with them, to return all of Apple's property in their possession, custody, or control and cease any access to or use of Apple's trade secrets.

6. For a declaration that Defendants have no rights or privileges to use Apple's confidential information or trade secrets.

7. Damages sufficient to compensate for the actual loss caused by Defendants' trade secret misappropriation and breach of contract.

8. A further award of monetary recovery for any unjust enrichment caused by Defendants' trade secret misappropriation.

9. In lieu of damages measured by any other methods, a reasonable royalty for Defendants' misappropriation of trade secrets.

10. Exemplary damages, based on Defendants' willful and malicious appropriation of trade secrets.

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 and unlawful acts.

12. For reasonable attorneys' fees and costs incurred herein as allowed under the Defend Trade Secrets Act.

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

Dated: July 10, 2026

Respectfully submitted,

WEIL, GOTSHAL & MANGES LLP

/s/ Gabriel S. Gross
Gabriel S. Gross (SBN 254672)
Gaby LaHatte (SBN 321844)
Vanessa K. Sim (SBN 341107)
WEIL, GOTSHAL & MANGES LLP
201 Redwood Shores Parkway
Redwood Shores, California 94065
Telephone: (650) 802-3000
Facsimile: (650) 802-3100
gabe.gross@weil.com
vanessa.sim@weil.com
gaby.lahatte@weil.com

Christopher W. Henry
(*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
1001 Boylston Street, Suite 300
Boston, Massachusetts 02115
Telephone: (617) 772-8300
Facsimile: (617) 772-8333
chris.henry@weil.com

Rachel L. Weiner Cohen
(*pro hac vice* forthcoming)
Nicole Elena Bruner
(*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
2001 M Street NW, Suite 600
Washington, DC 20036

Telephone: (202) 682-7000
Facsimile: (202) 857-0940
rachel.cohen@weil.com
nicole.bruner@weil.com

Heather Blacklaws
(*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
600 Congress Avenue, Suite 2170
Austin, Texas 78701
Telephone: (512) 487-1480
Facsimile: (512) 487-1520
heather.blacklaws@weil.com

Nina Shapiro
(*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
767 5th Avenue
New York, New York 10153
Telephone: (212) 310-8000
Facsimile: (212) 310-8007
nina.shapiro@weil.com

Attorneys for Plaintiff Apple Inc.