

IP Litigator, Apple's Trade Secret Claims Could Disrupt OpenAI's Hardware Plans, (Sept. 1, 2026)

IP Litigator

Apple's Trade Secret Claims Could Disrupt OpenAI's Hardware Plans

Bryan Sterba, Mark P. Kessler, and Chloe Rippe

Bryan Sterba is a partner in the Artificial Intelligence and IP & Tech Transactions practices at Lowenstein Sandler LLP.

Mark P. Kessler chairs the Intellectual Property group and is a partner in the IP & Tech Transactions and Artificial Intelligence practices at Lowenstein Sandler LLP.

Chloe Rippe is an associate in the Intellectual Property group at Lowenstein Sandler LLP.

Overview

On July 10, Apple filed a complaint in the U.S. District Court for the Northern District of California asserting claims under the federal Defend Trade Secrets Act of 2016 (DTSA) against OpenAI, its hardware affiliate io Products, and two former Apple employees, as well as breach-of-contract claims against the former employees. [\[1\]](#) Apple alleges that the defendants misappropriated its trade secrets to accelerate OpenAI's entry into consumer hardware and accordingly seeks damages, exemplary damages, attorneys' fees, and broad preliminary and permanent injunctive relief.

Although the dispute does not center on the development of artificial intelligence (AI) models and other software infrastructure most associated with today's advancements in generative AI, it is particularly notable because it could significantly hinder OpenAI's ability to monetize its consumer base in a new and highly anticipated consumer hardware vertical in the near term. Although the allegations remain unproven, the complaint provides a high-profile example of the trade secret risks that can arise when a company enters an adjacent market by recruiting from an established competitor and working with overlapping suppliers and vendors without imposing stringent controls and restrictions to avoid trade secret cross-contamination.

Summary of the Allegations

Apple alleges that OpenAI and its subsidiary io Products (an entity founded in 2024 by former Apple executives, including famed iPhone designer Jony Ive, and purchased by OpenAI in 2025 for an estimated \$6.5 billion) obtained and used confidential information concerning Apple's hardware design, engineering, manufacturing, testing, and supply chain through a brazen pattern of conduct. The complaint focuses on the two former Apple employees named as individual defendants, Chang Liu and Tang Yew Tan. Among other allegations, Apple asserts that Liu retained and accessed Apple information after his departure and assisted another Apple employee in transferring confidential materials, and that Tan used internal Apple project knowledge in OpenAI's recruiting activities and circulated information concerning Apple's offboarding procedures to help departing employees anticipate and potentially evade Apple's security reviews.

Further, Apple alleges that OpenAI's recruiting practices actively encouraged candidates to provide detailed presentations, design artifacts, prototypes, and supplier information concerning their Apple work, while OpenAI and io Products used Apple-specific knowledge and supplier relationships to obtain the benefit of proprietary manufacturing

techniques. Apple characterizes the alleged conduct as coordinated, and claims that OpenAI personnel took steps to conceal it or help departing employees evade Apple's security controls. Some of the most egregious allegations in the complaint regarding OpenAI's conduct include:

- Instructing Apple-employed candidates to bring actual materials from their recent Apple work, including "CAD/design artifacts" and prototypes, in connection with required "Technical Deep Dive" presentations during the OpenAI interview process
- Circulating to recruited Apple employees an internal Apple document marked "Need to Know" that described Apple's offboarding procedures and gave them advance notice of Apple's forensic and security checks prior to such employees' notification of their departure plans to Apple
- Counseling departing Apple employees not to disclose their next employer and advising them how to avoid being immediately removed from Apple during the standard notice period (allowing for continued access to Apple's confidential information and trade secrets)
- Soliciting a known Apple partner to perform Apple's proprietary multistep metal-finishing processes by misleading the partner into believing that Apple had authorized the same

Although its specific claims are unproven, Apple claims that they are backed up by forensic evidence of Liu's obtaining improper access to Apple's internal network folders post-termination and his unauthorized retention of Apple devices post-termination. Further, Apple claims that it possesses messages on devices from former Apple employees recruited by OpenAI during such employees' tenure at Apple that confirm much about the allegations.

Trade Secret Analysis

To prevail under the DTSA, Apple must establish that 1) it possessed information qualifying as a trade secret, 2) the defendants misappropriated that information, and 3) the misappropriation caused or threatened harm.^[2] Information qualifies as a trade secret only if the owner took reasonable measures to keep it secret and the information derives independent economic value from not being generally known or readily ascertainable through proper means.^[3] The DTSA defines "misappropriation" to include acquisition by improper means, as well as unauthorized disclosure or use under the circumstances specified in the statute.^[4] Misappropriation therefore does not require proof that the defendant made actual use of the trade secret information in order to obtain recourse under the DTSA, as such acquisition by improper means alone is sufficient.

Apple defines its asserted trade secrets broadly but in considerable detail, identifying methodologies, logistics strategies, and confidential supplier relationships that form the outlines of such trade secrets. Its theory also extends beyond discrete documents to the systems-level know-how involved in coordinating product design, manufacturing, testing, and supply chain operations at scale.^[5]

Apple will also need to show that the identified information derives independent economic value from not being generally known or readily ascertainable through proper means to warrant protection under the DTSA. Apple emphasizes the years of investment required to develop the information and the alleged ability of OpenAI to accelerate its hardware program by obtaining that information without making comparable investments. On the other hand, OpenAI may argue that some of the alleged information reflects the general expertise of former employees or the independent capabilities of suppliers rather than confidential Apple information that provides a competitive advantage because of its secrecy.

The complaint also provides details on the lengths to which Apple goes to keep the information secret through use of confidentiality and intellectual property agreements, use restrictions, access controls, physical security, confidentiality training, and offboarding procedures. And Apple may rely on the alleged efforts to retain unauthorized access, transfer materials outside Apple, solicit Apple-specific information during recruiting, obtain physical components, and evade security controls. Those allegations may serve both as evidence of improper means and as circumstantial support that the information was understood to be confidential and commercially valuable.

Potential Implications

Apple has requested preliminary injunctive relief that, if granted, could materially delay or disrupt OpenAI's consumer-hardware program. Depending on the scope of such an order, OpenAI could be restricted from using particular information, manufacturing processes, supplier relationships, or work performed by former Apple employees and could be required to pause, rework, or abandon portions of the program while the litigation proceeds. This could have cascading effects across the AI ecosystem for any partners of OpenAI anticipating economic and commercial activity tied to the program's launch and success.

Discovery may significantly affect the scope of that risk. Apple characterizes the conduct described in the complaint as potentially only the "tip of the iceberg" and is likely to seek recruiting records, interview materials, employee communications, product-development documents, and evidence from suppliers implicated in the allegations. That discovery could clarify whether OpenAI's hardware program relies on identifiable Apple trade secrets and could lead Apple to seek broader relief than can presently be supported by the information available to it.

The potential impact of the litigation will be relevant to companies engaged in or considering partnerships, supply arrangements, or other commercial relationships tied to OpenAI's consumer hardware vertical, as well as to investors evaluating OpenAI more broadly. In assessing those opportunities, parties may wish to take into account the extent to which the anticipated value of the relationship depends on the timing and continued development of the consumer hardware program, particularly given the possibility of delays, redesigns, increased costs, or other operational disruption as the litigation proceeds.

Best Practices

The allegations also highlight several practices companies can use to reduce trade secret risk when hiring from competitors, engaging suppliers, and managing employee departures:

- New employees hired from competitors should confirm that they have returned former-employer property and will not use or disclose former-employer confidential information in their new roles.
- Companies hiring multiple employees from a single competitor should be mindful during recruitment to avoid ingestion of protected information and should consider enhanced onboarding, training, certifications, and measures to segregate potentially sensitive information for new hires.
- Supplier agreements must clearly address ownership and permitted use of customer-specific processes, tooling, and facilities as well as jointly developed know-how.
- Offboarding procedures should promptly terminate access, recover devices, preserve relevant records, and investigate unusual downloads or transfers.
- Trade secret owners should identify the information they regard as confidential and maintain records of the contractual, technical, and operational measures used to protect it.

Although the merits of Apple's claims have yet to be tested, the allegations illustrate how otherwise lawful hiring and supplier relationships can create trade secret exposure when accompanied by transfers of confidential materials, requests for proprietary information, or the use of customer-specific processes subject to confidentiality or use restrictions. And for companies that have lost employees to a competitor, it illustrates the importance of ensuring all devices, access credentials, and other means of interacting with company client information are returned by employees as part of offboarding, both by the departing employee and using any operational security controls to effect the same promptly following departure.

For more information regarding this article, its potential implications, or best practices for protecting trade secrets in connection with employee hiring and departures, supplier relationships, or other business activities, please contact the authors.

Footnotes

- ¹ Complaint, *Apple Inc. v. Liu*, No. 5:26-cv-07078 (N.D. Cal. July 10, 2026), ECF No. 1.
- ² *InteliClear, LLC v. ETC Global Holdings, Inc.*, 978 F.3d 653, 657–58 (9th Cir. 2020).
- ³ 18 U.S.C. § 1839(3)(A) –(B).
- ⁴ 18 U.S.C. § 1839(5).
- ⁵ See, e.g., Complaint ¶ 40(e), *Apple Inc. v. Liu*, No. 5:26-cv-07078 (N.D. Cal. filed July 10, 2026), ECF No. 1 (“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.”).

[https://prod.resource.cch.com/resource/scion/document/default/\(%40%40PZG01%20WK-JSTORY20260901-5\)229d35987c9945f8a0e96af8068b8c39?cfu=Legal&cpid=WKUS-Legal-Cheetah&uAppCtx=cheetah](https://prod.resource.cch.com/resource/scion/document/default/(%40%40PZG01%20WK-JSTORY20260901-5)229d35987c9945f8a0e96af8068b8c39?cfu=Legal&cpid=WKUS-Legal-Cheetah&uAppCtx=cheetah)