

U.S. SECURITIES AND EXCHANGE COMMISSION
FORM TCR (TIP, COMPLAINT, OR REFERRAL) & FORMAL DISCLOSURE

SECTION A: SUBMISSION & WHISTLEBLOWER PROFILE

Submission Date:	August 26, 2026	SEC Whistleblower No:	17684-273-411-436
Submission Device (1):	Google Pixel 8 Pro (Primary)	Device Lock Status:	Unlocked from Enterprise MDM prior to TCR
Submission Device (2):	Google Pixel 8 Pro (Backup)	Device Lock Status:	Unlocked from Enterprise MDM post-TCR
Disclosure Channel:	Privileged Regulatory Counsel	whistleblower Status:	Confidential Insider Filing

SECTION B: SUBJECTS OF COMPLAINT

Primary Entity:	OpenAI Group PBC (Delaware Public Benefit Corp)	Valuation/Target:	\$1.0 Trillion IPO Target (Fall 2026)
Parent/Control Entity:	OpenAI Foundation (f/k/a OpenAI Inc.)	Veto/Control:	Holds 26% Equity & PBC Board Appt. Rights
Acquired Entity:	io Products (co-founded by Jony Ive & Tang Tan)	Purchase Date/Value:	May 21, 2025 // \$6.5 Billion (All-Equity)
Individuals Involved:	Sam Altman (CEO), Tang Tan (CHO, Defendant), Chang Liu (Technical Staff, Defendant)	Legal Venues:	U.S. District Court, N.D. Cal. (Case No. 5:26-cv-07078)

SECTION C: STATEMENT OF VIOLATIONS & MATERIAL OMISSIONS

I. THE MATERIAL OMISSION OF THE 'ROTTEN FOUNDATION' VALUATION

On October 28, 2025, OpenAI restructured its corporate architecture, converting its commercial subsidiary into **OpenAI Group PBC** (a Delaware Public Benefit Corporation) and renaming its non-profit arm to the **OpenAI Foundation**. The foundation retained a **26% paper equity stake**, which immediately valued its charitable assets at **\$130 billion** based on ongoing private investment capital. However, this submission charges that the financial valuations supporting this restructure, as well as the **\$6.5 billion acquisition valuation of Jony Ive's io Products** on May 21, 2025, contain **material omissions of systemic trade secret theft** and corporate espionage that inflate asset values, constituting a direct fraud on investors and regulators.

Specifically, as detailed in the federal DTSA complaint filed by Apple Inc. (*Apple Inc. v. OpenAI Foundation et al.*, Case No. 5:26-cv-07078, N.D. Cal.), the core consumer device assets and the intellectual property backing OpenAI's hardware program rest on a foundation that is **'rotten to its core.'** The \$6.5 billion valuation attributed to the io Products assets was artificially inflated by exfiltrated R&D documentation, component specifications,

and manufacturing blueprints stolen from Apple Inc. through the active orchestration of OpenAI's Chief Hardware Officer Tang Tan and engineer Chang Liu. Because these assets were acquired through unlawful shortcuts and corporate talent siphoning, OpenAI's upcoming Fall 2026 Initial Public Offering (IPO)—seeking a public debut of up to **\$1 trillion**—rests upon a major unhedged litigation risk. The failure to disclose that OpenAI's physical devices program was built upon misappropriated trade secrets represents a material omission under Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5.

II. THE SEC-VALUATION OVERLAP CHRONOLOGY

A forensic timeline of OpenAI's capital raises demonstrates a direct overlap between active database intrusions and commercial valuation spikes. In January 2026, Senior Systems Electrical Engineer Chang Liu joined OpenAI and failed to return his Apple-issued laptop. From February to April 2026, while employed by OpenAI and working in Tang Tan's consumer device division, Liu exploited an authentication bug to bypass Apple's security and exfiltrated thousands of pages of confidential drawings and unreleased specifications on **at least five separate occasions**. Concurrently, Liu coached Alyssa Peng (then still inside Apple) on how to exfiltrate files onto external hard drives and directed communication to the encrypted app LINE.

This active data theft coincided perfectly with OpenAI's massive **Series G capital campaign**. On February 27, 2026, OpenAI announced a **\$110 billion capital raise at a \$730 billion post-money valuation** led by Amazon, SoftBank, and Nvidia. In mid-March, the round was extended by an additional **\$10 billion**. In April 2026, as Liu completed his fifth unauthorized database intrusion, OpenAI closed the round at a final **\$122 billion in committed capital, pricing the PBC at \$852 billion**. This submission asserts that the \$852 billion valuation was materially supported and accelerated by the stolen hardware specifications, displaying a coordinated pattern of using stolen intellectual property to inflate private equity rounds before a planned IPO.

SECTION D: WHISTLEBLOWER RETALIATION & SUPPLEMENTAL DISCLOSURES

I. OREGON STATE TREASURY AUDITOR DIVISION VIOLATIONS

This submission includes severe supplemental disclosures regarding structural retaliation and safety violations occurring within state-level public utility oversight channels. In the course of investigating the non-profit-to-for-profit restructuring of OpenAI's charitable assets, the whistleblower formally filed disclosures with the **Oregon State Treasury Auditor Division**. Under federal and state whistleblower protection frameworks, these disclosures are legally protected, and the confidentiality of the filer is absolute.

However, representatives within the Oregon State Treasury Auditor Division actively violated these whistleblower protections. The Auditor Division engaged in bad-faith obstruction by mocking the whistleblower's forensic timeline. They used **backdated, retroactively altered records** of the whistleblower's real-time activities to discredit the chronological tracking of OpenAI's asset revaluations. This deliberate administrative manipulation was designed to undermine the regulatory credibility of the filings and insulate the target entities from public accountability.

II. ONGOING ONLINE HARASSMENT & LAW ENFORCEMENT ACTION

Following the administrative obstruction and exposure of the whistleblower's timeline by the Oregon State Treasury representatives, the whistleblower became the target of a coordinated campaign of digital intimidation and harassment. Online platforms were leveraged to distribute threat-centric messaging, monitor the whistleblower's real-time actions, and create an environment of active hostility to force the abandonment of these filings.

This campaign of coordinated harassment deteriorated to the point of creating an imminent threat to physical safety and personal security. Consequently, the whistleblower was forced to file an official criminal harassment and intimidation report with the **Washington County Sheriff's Office in Washington County, Oregon**. Copies of the Washington County police report and documented digital footprints of the harassment are appended to this submission as Supplemental Exhibit F. The SEC is formally requested to initiate an expedited investigation into these whistleblower protection violations under Section 21F of the Securities Exchange Act of 1934 and 17 C.F.R. § 240.21F-17.

SECTION E: WHISTLEBLOWER DECLARATION & SIGNATURE

Under penalty of perjury under the laws of the United States, I declare that I have read the foregoing information and that the facts stated in it are true, correct, and complete to the best of my knowledge, information, and belief. I understand that the willful making of false, fictitious, or fraudulent statements or representations in this submission may be punished as a felony under 18 U.S.C. § 1001 and may subject me to criminal prosecution.

Declarant Signature: /s/ Confidential Insider No. 17684-273-411-436 **Date:** August 26, 2026