

MOCK DEPOSITION OUTLINE OF DEFENDANT CHANG LIU

Focusing on the Digital Forensics of Post-Employment Network Intrusions and Coordinated Talent Exfiltration

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION	CASE NO. 5:26-cv-07078-EJD MOCK DEPOSITION ROADMAP
APPLE INC. , a California Corporation, <i>Plaintiff,</i> v. OPENAI FOUNDATION, OPENAI GROUP PBC, io PRODUCTS, TANG TAN, and CHANG LIU, <i>Defendants.</i>	DEPONENT: Chang Liu ROLE: Member of Technical Staff, OpenAI (Former Apple Engineer) DATE: September 2026 LOCATION: San Jose, California

SEC COMMISSION CHAIR STRATEGIC MEMORANDUM

The Wire Fraud Connection & Regulatory Exposure: Under the Defend Trade Secrets Act (DTSA) (18 U.S.C. § 1836), civil liability arises from the misappropriation of proprietary technical data. However, the forensics of Chang Liu's actions suggest a severe crossover into federal criminal liabilities, specifically **Wire Fraud (18 U.S.C. § 1343)**. By retaining his Apple work laptop, exploiting an authentication bug, and transmitting proprietary unannounced product data across state lines to benefit OpenAI's commercial programs, Liu engaged in a scheme to defraud Apple of its high-value physical properties. This exposes the commercial entity (OpenAI Group PBC) to massive compliance and disclosure violations directly under the SEC's purview, especially as it prepares for a Fall 2026 Initial Public Offering (IPO). This deposition outline aims to establish the precise forensic trail of Liu's intrusions to validate these regulatory and civil actions.

I. FORENSIC CHRONOLOGY & DEVIANT post-EMPLOYMENT INTRUSIONS

This phase establishes the timeline and technical specifics of Liu's unauthorized access to Apple's shared network folders, relying directly on Apple's sworn digital forensics expert declarations.

Q: Mr. Liu, you spent eight years as an electrical engineer at Apple before resigning on January 22, 2026, correct?

Goal: Establish his background, technical competence, and complete notice of standard offboarding and laptop return policies.

Q: Is it a fact that you retained your Apple-issued work laptop after your official departure date of January 22, 2026?

Goal: Establish the unauthorized possession of a corporate asset, a physical prerequisite for the downstream exfiltration.

Q: Forensic logs indicate that between February and April 2026, while employed by OpenAI, your credentials were used on at least five separate occasions to log into Apple's internal networks. Did you perform those logins?

Goal: Lock the deponent into admitting active post-employment access or force a perjury risk in the face of verified IP and device logs.

Q: To access those folders, you exploited a previously undocumented authentication vulnerability to bypass Apple's security firewall, did you not?

Goal: Establish deliberate hacking activity (violating the Computer Fraud and Abuse Act) rather than passive, accidental synchronization.

Q: During those five intrusions, you downloaded thousands of pages of Apple's unreleased product designs, manufacturing specifications, and supplier contracts. Who at OpenAI directed you to target those specific files?

Goal: Trace the chain of custody. Establish that the stolen IP went straight into OpenAI's hardware R&D, showing institutional ratification of misappropriation.

II. THE ALYSSA PENG INSIDE-EXFILTRATION PIPELINE

This section exposes the coordinated recruitment pipeline and the use of inside moles to exfiltrate proprietary files before they formally resigned, proving systematic, institutional talent and IP extraction.

Q: While employed at OpenAI, you actively recruited and coached Yu-Ting 'Alyssa' Peng, who was still working inside Apple's CE departments, correct?

Goal: Establish conspiracy and concerted action between OpenAI employees and active Apple personnel.

Q: You instructed Ms. Peng on how to copy confidential R&D; files from Apple workstations onto external hard drives to avoid triggering Apple's internal security alarms, correct?

Goal: Show active instruction and coaching in data exfiltration techniques, directly pointing to criminal intent and active concealment.

Q: Why did you direct Ms. Peng to shift all of your recruiting and technical communications onto the encrypted messaging application LINE?

Goal: Prove a coordinated effort to evade Apple's corporate security and hide the paper trail of the stolen designs from legal discovery.

Q: In your LINE chats, you told Ms. Peng that copying Apple files was necessary 'to avoid trouble with the security team' upon her departure. You knew that what you were directing her to do was highly illegal, didn't you?

Goal: Pin down 'willful and malicious' misappropriation, which opens OpenAI up to treble damages and attorney fees under the DTSA.

III. CROSS-EXAMINING THE IMESSAGE AND 'RESIDUAL ACCESS' DEFENSE

This critical phase dismantles OpenAI's public relations defense—published in their August 3, 2026 blog post—which argued that Apple's loose IT systems and employee communications pro-actively invited Liu's continued access.

Q: In your text messages on your last day, you told a coworker, 'Hey, hope everything is fine for copy pasting. You can keep my iCloud connected if you still need more time.' Why were you encouraging Apple staff to keep your personal account connected to a corporate laptop?

Goal: Reframe the 'cooperation' narrative. Expose that keeping the personal iCloud connected was a Trojan horse to preserve a backdoor tunnel into Apple's systems.

Q: When that same Apple coworker mentioned your iCloud remained connected, you texted: 'LOL, I found out I can access the network storage, so funny.' What is 'funny' about having unauthorized access to a competitor's billion-dollar hardware designs?

Goal: Establish subjective knowledge and a reckless disregard for proprietary boundaries. Highlight the 'LOL' text to demonstrate malice to a jury.

Q: In another text thread with an Apple designer, you wrote: 'I can always give you some fun side projects' at OpenAI. Were those 'side projects' designed to leverage the unreleased display and battery housing secrets you had just downloaded?

Goal: Connect the unauthorized downloads with active, commercial product development at OpenAI, defeating any 'passive sync' defense.

Q: In March 2026, an Apple engineer explicitly messaged you: 'Hi, this is highly irregular, please remove me from this thread.' You knew that Apple employees were pushing back against your unauthorized inquiries, yet you continued to probe, correct?

Goal: Establish that the deponent was explicitly notified of the irregular nature of the communications, destroying the defense of 'consensual, residual cooperation.'

IV. SEC COMPLIANCE & RESTORATION OF INVESTOR TRUST

This section outlines questions to link these digital intrusions directly to OpenAI's impending Fall 2026 IPO and the SEC's mission to prevent fraudulent omissions in investor disclosures.

Q: As of August 2026, OpenAI's corporate executives are actively preparing a confidential IPO registration statement to list the company at a \$1 trillion valuation, correct?

Goal: Establish the deponent's awareness of the immense financial scale and public market implications of the hardware division's valuation.

Q: You are aware that if OpenAI's consumer hardware prototypes are shown to rest on stolen, exfiltrated Apple R&D; blueprints, that \$1 trillion valuation is materially misleading to public investors, correct?

Goal: Link the trade secret theft directly to Securities Fraud and material omissions in IPO disclosures, establishing the SEC's direct enforcement jurisdiction.

Q: In August 2026, OpenAI agreed to three preliminary injunction conditions, including halting future access and ceasing data use, but flatly refused to permit Apple's forensic experts to inspect OpenAI's physical devices. Where are the unreleased Apple designs currently stored on OpenAI's physical servers?

Goal: Expose the 'non-denial denial' and active concealment of the digital evidence, establishing the necessity of the October 1st judicial forensic intervention.