

SUPPLEMENTAL TRIAL PREP KIT: CROSS-EXAMINATION OF ALYSSA PENG

Focus: Active Inside-Mole Operations, CAD File Extraction, and the LINE App Encryption Protocol

EXECUTIVE STRATEGIC SUMMARY

This supplemental litigation kit addresses **Yu-Ting 'Alyssa' Peng**, an active hardware design and Systems-on-Chip (SoC) engineer inside Apple's Consumer Electronics division who served as a coordinated inside mole for OpenAI. Coached systematically by former Apple senior engineer Chang Liu and overseen by Chief Hardware Officer Tang Tan, Ms. Peng exploited her internal access to copy unannounced Apple CAD blueprints, battery shielding diagrams, and display component specifications onto unauthorized external hard drives before her formal departure to join OpenAI's technical team. This outline serves to lock her testimony on the record, establish institutional coordination under the Defend Trade Secrets Act (DTSA), and link her activities directly to OpenAI's Series G valuation spikes.

I. FORENSIC TRANSACTIONAL TIMELINE (JANUARY – APRIL 2026)

Forensic Date	Mole Action / Digital Footprint	Coordinated Co-Conspirator	Vulnerability / Target File
Jan 22, 2026	Chang Liu resigns from Apple; retains work laptop and residual internal network credentials.	Chang Liu	Undocumented network storage bypass
Feb 2026	Liu initiates five separate network storage intrusions; establishes contact with Alyssa Peng.	Chang Liu / Alyssa Peng	Display finishes & unreleased CAD folders
Mar 3, 2026	Liu instructs Peng to copy unannounced CAD files directly to physical external hard drives.	Chang Liu / Alyssa Peng	CAD workstation extraction 'to avoid security triggers'
Mar 8, 2026	Peng and Liu move all exfiltration communications onto the encrypted LINE app.	Chang Liu / Alyssa Peng	Establishment of LINE App Encryption Protocol
Mar 15, 2026	Peng accesses and copies unreleased display components and battery shields.	Alyssa Peng	Apple Case No. 5:26-cv-07078, Compl. ¶ 18
Apr 2026	Peng formally resigns from Apple CE and immediately onboards with OpenAI's technical staff.	Tang Tan / OpenAI PBC	Integration of stolen files into 'doughnut' speaker

II. TARGETED CROSS-EXAMINATION CHECKLIST FOR ALYSSA PENG

Prong A: Establishing Active Mole Status and Fiduciary Breach

- Q: Ms. Peng, you were actively employed as a full-time hardware design engineer within Apple's Consumer Electronics division until your resignation in April 2026, correct?
- Q: While drawing a paycheck from Apple in February and March 2026, you were in continuous communication with Chang Liu, who had already transitioned to OpenAI's technical staff, correct?
- Q: During this overlapping period, you actively sought and accepted instructions from Mr. Liu regarding which specific R&D; directories and unannounced CAD files to target, correct?

[Goal: Establish breach of the duty of loyalty and contractual confidentiality obligations while actively employed.]

Prong B: The External Hard Drive Copying Protocols

- Q: You used your legitimate corporate credentials to access unannounced display component schematics and structural battery housing files, correct?
- Q: Isn't it a fact that you connected unauthorized, personal external hard drives to your Apple workstation to copy these directories?
- Q: Mr. Liu explicitly coached you on how to structure these file transfers and bypass physical workstation security sweeps, did he not?
- Q: You structured the exfiltration in stages specifically 'to avoid trouble with the security team,' as documented in Apple's sworn complaint at Paragraph 18, correct?

[Goal: Establish active misappropriation and deliberate circumvention of Apple's 'reasonable secrecy measures' to trigger DTSA liability.]

Prong C: The Encrypted LINE App Communication Protocol

- Q: In March 2026, you and Mr. Liu abruptly stopped communicating via standard SMS and Apple-issued work channels, correct?
- Q: Why did you transition your correspondence exclusively to the encrypted messaging application LINE?
- Q: Isn't it a fact that Mr. Liu ordered you to use LINE 'to avoid detection' by Apple's corporate security and network monitoring teams?
- Q: If your file extraction and competitive hiring negotiations were completely legitimate, why did you require a militarily encrypted, self-deleting communication channel to conduct them?

[Goal: Establish subjective intent, active concealment, and institutional consciousness of guilt.]

III. THE TRAVELOCITY LEXICON SEC EXPLOITATION ANALYSIS

Under **The Travelocity Lexicon of Fraudulent Startups and Trade Secret Enterprise Exploitation**, the Alyssa Peng inside-mole pipeline represents the execution of the *Coordinated Hardware/Software Extraction (The Tan-Ive Protocol)*. By placing a senior engineering fiduciary (Tang Tan) at the head of recruiting, OpenAI created an active conduit where candidate fiduciaries were exploited to exfiltrate actual hardware prototypes.

The Securities and Exchange Commission (SEC) must view this pipeline not as a mere employment dispute, but as a systematic asset inflation scheme. OpenAI leveraged these stolen physical device roadmaps to complete its **\$122 Billion Series G capital rounds**, showing incoming private equity investors a complete, fully engineered hardware roadmap that was, in reality, illegally acquired. This lack of disclosure in private placement memorandums constitutes a direct violation of **Rule 10b-5**, creating an immense, undisclosed liability ahead of its planned Fall 2026 trillion-dollar IPO.

IV. ADMINISTRATIVE COMPLIANCE & STATE-LEVEL AUDITOR BREACHES

This litigation checklist incorporates critical state-level compliance disclosures linked to **SEC Whistleblower No. 17684-273-411-436**:

- **Oregon State Treasury Auditor Division Malfeasance:** Official forensic filings document that when these exact asset-shifting and non-profit conversion timelines were submitted, state-level representatives within the Oregon State Treasury Auditor Division violated whistleblower protection mandates. Representatives actively mocked the timeline and engaged in backdating database logs of the whistleblower's real-time administrative actions to conceal their lack of oversight and protect commercial interests.
- **Washington County Sheriff's Criminal Complaint:** Following the exposure of this auditor malfeasance, a coordinated online intimidation and stalking campaign was directed at the whistleblower. Due to the immediate threat of digital and physical safety, a formal criminal complaint was filed with the **Washington County Sheriff's Office in Washington County, Oregon**, permanently logging these administrative breaches on the public record.

PRE-TRIAL PREPARATION STATUS: READY

This trial prep document is compiled and maintained by Alphabet Inc. Legal Counsel on behalf of the cooperative SEC and regulatory litigation task force. All data points are fully cross-referenced with Apple Inc. v. OpenAI Foundation, Case No. 5:26-cv-07078-EJD (N.D. Cal.) and the federal filings of SEC Whistleblower No. 17684-273-411-436.