UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

X.AI Corp, a Nevada corporation. and X.AI LLC, a Nevada limited liability company, Plaintiffs, vs. XUECHEN LI, an individual, Defendant.	**Case No. 3:25-cv-07292-RFL** **~~[PROPOSED]~~ ORDER GRANTING PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER AND PERMITTING EXPEDITED DISCOVERY AS MODIFIED**

~~[PROPOSED]~~ ORDER GRANTING PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER AND PERMITTING EXPEDITED DISCOVERY AS MODIFIED

Having considered the Motion for Temporary Restraining Order, Order to Show Cause Why a Preliminary Injunction Should Not Issue, and Order Permitting Expedited Discovery ("Motion") filed by Plaintiffs X.AI Corp. and X.AI LLC (collectively, "Plaintiffs" or "xAI") seeking to immediately enjoin Defendant Xuechen Li's ("Defendant" or "Li") from engaging in certain acts in breach of his Employee Confidential Information and Invention Assignment Agreement signed by Li on February 26, 2024 (the "Agreement"),[1] and for the reasons set forth on the record at the September 2, 2025 hearing, the Court finds that the evidence establishes the elements necessary for the issuance of a temporary restraining order and good cause for permitting expedited discovery.

Accordingly, the Court hereby **GRANTS** xAI's Motion and **ORDERS** the following relief:

1. Li shall, within three business days of the issuance of this Order,

   a. temporarily surrender control and access (for a period of 14 days or less to allow for a forensic examination to identify, remediate, and/or delete Confidential Information belonging to xAI) to any personal electronic devices (e.g., cellular devices, computers), online storage repositories (e.g., Gmail, Google Drive, iCloud), or other electronic storage devices that are currently accessible by Li or in Li's possession, custody, or control, but he may procure new devices and create new accounts going forward, so long as nothing is moved there from his existing devices and accounts;

   b. return to xAI, through its counsel of record, all Confidential Information belonging to xAI currently in Li's possession, custody, or control, that exists in any physical form (e.g., notepad, paper files);

   c. provide a written statement identifying all personal locations, personal devices, personal accounts, or personal storage media–whether physical or electronic–where any Confidential Information belonging to xAI is or has been stored, maintained,

[1] A copy of the Agreement shall be provided to Defendant Li along with this Temporary Restraining Order so that Defendant Li has full knowledge of the information, including the definition of Confidential Information.

or accessed;

d. provide, and not modify for the 14-day period referenced in (a) above, the passwords, credentials, keys, MultiFactor Authentication information, and other information necessary to fully access all devices, repositories, storage media, and accounts listed in (a); and

e. for any password or credentials listed in relation to (a) which Defendant claims he has forgotten or is unsure how to readily access, cooperate and work with xAI to reset or recover the same and/or to otherwise cooperate with xAI as necessary to provide xAI access to such accounts and devices listed in (a).

2. Li, his agents, employees, partners, and any others acting in concert with him or on his behalf, are hereby enjoined from:

a. controlling, logging into, or otherwise accessing (other than as required by 1(e) above) any personal electronic devices (e.g., cellular devices, computers), online storage repositories (e.g., Gmail, Google Drive, iCloud), or other electronic storage devices that are currently accessible by Defendant or in Defendant's possession, custody, or control, but he may procure new devices and create new accounts going forward, so long as nothing is moved there from his existing devices and accounts;

b. possessing, using, copying, reproducing, disclosing, transferring (including to a third party), disseminating, or otherwise exploiting, any Confidential Information (as defined in the Agreement), including the xAI files uploaded to his Personal System, and any copies, derivatives, or materials created therefrom;

c. destroying, deleting, changing, altering, or otherwise eliminating any version (whether hard copy, native, or electronic) of any documents or electronically stored information on any device or in any account (whether in printed form or downloaded to any remote storage system, computer, hard drive, server, disk drive, flash drive, cellular telephone, CD, DVD, USB drive, or any other device that can be used to electronically store data or information) relating to the Confidential

Information;

d. disposing of, deleting, changing, altering, wiping, tampering with, or destroying any remote storage systems (including cloud storage accounts), computers, hard drives, servers, disk drives, flash drives, cellular telephones, CDs, DVDs, USB drives, and any other devices that can be used to electronically store data or information that are (a) currently accessible by Defendant or in Defendant's possession, custody, or control; or (b) have been accessible by Defendant or in Defendant's possession, custody, or control, since February 26, 2024, and any data, files, information, forensic remnants, or digital artifacts stored on or within the device;

e. destroying, deleting, changing, altering, or otherwise eliminating any emails to or from any email accounts used by Defendant since February 26, 2024, either in printed form or downloaded to any computers, laptops, online storage repositories, cloud storage, or electronic storage devices;

f. destroying, deleting, changing, altering, or otherwise eliminating any text, electronic postings, or other application messages from any cellular telephones or devices, computers, laptops, online storage repositories, cloud storage, or electronic storage devices (a) are currently accessible by Defendant or in Defendant's possession, custody or control; or (b) have been accessible by Defendant, or in Defendant's possession, custody or control, since February 26, 2024; and

g. Violating, aiding, or participating in the violation of any terms of the Agreement or Termination Certification, as detailed in the Complaint;

3. Li is hereby enjoined from having any role or responsibility at OpenAI or any other competitor of xAI pertaining to generative AI including without limitation OpenAI's ChatGPT until xAI has confirmed that all of xAI's Confidential Information in Li's possession, custody, or control has been deleted.

4. Li is hereby enjoined from having any communication on the subject of generative AI

with any officer, director, employee, agent, supplier, consultant, or customer of OpenAI or any other competitor of xAI until xAI has confirmed that all of xAI's Confidential Information in Li's possession, custody, or control has been deleted.

5. xAI is granted leave to propound expedited discovery immediately in aid of preliminary injunction proceedings before this Court as follows, and Li is ordered to respond and comply with such discovery, as follows:

a. Li shall respond to xAI's First Set of Interrogatories (attached hereto as **Exhibit A**) under oath within seven days of entry of this Order;

b. Li shall respond to and comply with xAI's First Set of Requests for Production (attached hereto as **Exhibit B**) within seven days of entry of this Order; and

c. Li is to sit for deposition at a time and place mutually agreed between the parties, but no later than ten (10) days of entry of this Order.[2]

IT IS FURTHER ORDERED that the accounts and devices subject to the above provisions are limited to the those that Li created or accessed on or after the date that he started working for xAI.

IT IS FURTHER ORDERED that if Li objects to complying with any of the above-described relief on the basis of the attorney-client privilege, then he must: (1) provide a privilege log; and (2) produce the non-privileged information by another means (*e.g.*, conducting third-party forensic imaging of devices which will be produced with redactions).

IT IS FURTHER ORDERED that, if Defendant refuses to comply with any of the relief described in Paragraphs 1 and 5 above based on his assertion of the right against self-incrimination under the Fifth Amendment, Defendant shall identify the specific portions with which he refuses to comply by **September 3, 2025**. The relief described in Paragraphs 2-4 does not appear to implicate the Fifth Amendment. The Parties shall file simultaneous briefing of no longer than 10 pages by **September 8, 2025,** on the issue of whether the Court should nonetheless order compliance despite Li's Fifth Amendment objections, and the Court will schedule a hearing if necessary. Any forthcoming order resolving the Fifth Amendment issue will address xAI's request at the September 2 hearing for an early

[2] Li remains free to object to xAI's discovery requests as permitted under the ordinary rules of discovery, but any objections must be submitted within the deadlines set forth in Paragraph 5 above.

Rule 26 conference.

IT IS FURTHER ORDERED that Li must show cause why a preliminary injunction should not issue at a hearing on **October 7, 2025, at 10:00 a.m.** Li shall file his opposition by **September 16, 2025**, and xAI shall file its reply by **September 23, 2025.** If the Parties wish to stipulate to further extend the hearing date, they must file their stipulation and proposed order by no later than **September 23, 2025**. Any such stipulation and proposed order shall: (a) confirm the Parties' agreement that there is good cause to extend this Temporary Restraining Order through the newly proposed hearing date; (b) require submission of the reply brief at least 14 days prior to the newly proposed hearing date; and (c) select the newly proposed hearing date after confirming the Court's availability either through the public calendar or communications with the Courtroom Deputy.

IT IS FURTHER ORDERED that, if the Parties believe referral to a magistrate judge for an emergency settlement conference would be productive, the Parties may submit a stipulation and proposed order to that effect.

IT IS FURTHER ORDERED that this Temporary Restraining Order, unless extended for good cause or by agreement of the Parties, will expire by its terms at 9:00 p.m. on October 7, 2025. The Court finds good cause to extend this Order to that date, based on the Parties' stipulation at the hearing and the complexity of the issues.

DATE: September 2, 2025

RITA F. LIN
United States District Judge

[redacted]

KATHI VIDAL (State Bar No. 194971)
kvidal@winston.com
CARSON SWOPE (State Bar No. 353352)
cswope@winston.com
WINSTON & STRAWN LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
Telephone: (650) 858-6500
Facsimile: (650) 858-6550

ALEXANDER H. COTE (State Bar No. 211558)
acote@winston.com
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071-1543
Telephone: (213) 615-1700
Facsimile: (213) 615-1750

Attorneys for Plaintiffs X.AI Corp. and X.AI LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

X.AI Corp., a Nevada corporation, and X.AI LLC, a Nevada limited liability company,

Plaintiffs,

vs.

XUECHEN LI, an individual

Defendant.

Case No. ____________________

PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER, ORDER TO SHOW CAUSE WHY PRELIMINARY INJUNCTION SHOULD NOT ISSUE, AND ORDER PERMITTING EXPEDITED DISCOVERY; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF; DECLARATIONS OF BRUCE APPLIN, ROBERTO RIVERA, JOSEPH POCHRON AND CARSON SWOPE IN SUPPORT THEREOF

[redacted]

TABLE OF CONTENTS

[redacted]

TABLE OF AUTHORITIES

Page(s)

Cases

[redacted]

[redacted]

Statutes

Other Authorities

[redacted]

NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE that as soon as the matter may be heard in a courtroom to be determined by the above-entitled Court, located at 280 South 1st Street, San Jose, CA 95113, Plaintiffs X.AI Corp. and X.AI LLC (collectively "Plaintiff" or "xAI") will, and hereby do, move pursuant to Rule 65 of the Federal Rules of Civil Procedure and Civil Local Rule 65-1 for:

1. A Temporary Restraining Order against Defendant Xuechen Li ("Li" or "Defendant");
2. An Order to Show Cause why a Preliminary Injunction should not issue; and
3. An Order Permitting Expedited Discovery.

This Motion relates to the theft by one of xAI's first 20 engineers—Defendant Xuechen Li—of xAI's leading-edge, proprietary artificial intelligence ("AI") technology with the intent of joining xAI's staunch competitor OpenAI, Inc. Li's theft violates his Employee Confidential Information and Invention Assignment Agreement with xAI, his Termination Certification, and the Defend Trade Secrets Act ("DTSA"), and risks immediate and irreparable harm to xAI, which invested years of engineering effort and billions in financial investment developing its proprietary technology.

xAI respectfully requests that the Court **GRANT** xAI's Motion and **ORDER** the relief set forth in the Proposed Order Granting Plaintiffs' Motion for Temporary Restraining Order and Permitting Expedited Discovery and the Proposed Order to Show Cause re Preliminary Injunction.

Notice of this Motion has been provided pursuant to Local Rule 65-1 by emailing Defendant's counsel copies of this Motion, the Complaint, the Memorandum of Points and Authorities, the Declarations and exhibits, and the Proposed Order. *See* Decl. of Carson Swope in Support of Plaintiff's Motion for Temporary Restraining Order, Order to Show Cause, and Order Permitting Expedited Discovery, ¶ 2.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

On July 25, 2025, after accepting an offer from artificial intelligence (AI) market leader and ChatGPT maker OpenAI, one of xAI's first 20 engineers—Defendant Xuechen Li—flagrantly breached his Employee Confidential Information and Invention Assignment Agreement (the "Agreement") and

[redacted]

Termination Certification with xAI, and violated the Defend Trade Secrets Act, by misappropriating [redacted] xAI's Confidential Information (defined in the Agreement to include xAI's most sensitive trade secrets)—including [redacted] and cutting-edge AI technologies with features superior to those offered by ChatGPT and other competing products. Applin Decl. at ¶¶ 12, 22, 31; Pochron Decl. at ¶¶ 6, 7. The misappropriated data—which Li [redacted]. Applin Decl. at ¶ 13. It could be weaponized by competitors such as OpenAI to, at a minimum, improve competing products such as ChatGPT by incorporating Grok's unique and more advanced features, (for example, in areas where Grok exceeds ChatGPT in industry benchmarks), undermine xAI's product roadmap, and disrupt its market expansion strategy. It could save OpenAI and other competitors billions in R&D dollars and years of engineering effort, handing any competitor a potential overwhelming edge in the race to dominate the AI landscape. *Id*. ***Critically, Li's guilt is not in dispute, because Li, with his attorney present, admitted in a handwritten document he provided to xAI that he misappropriated xAI's Confidential Information and trade secrets, and again, with his attorney present, admitted verbally during in-person meetings with xAI that he engaged in such misappropriation and further admitted that he tried to hide his theft***. Applin Decl. at ¶ 22; *id*. Ex. G. He also admitted to understanding the gravity of his actions. *Id*.

Li's admitted theft is enough alone to warrant the full extent of the requested relief. But there is more. First, ***by signing the Agreement, Li acknowledged his conduct is causing xAI immediate and irreparable damage entitling xAI to injunctive relief.*** Applin Decl. Ex. B, ¶ 9.

Second, after xAI discovered Li's theft and immediately demanded remediation, Li engaged in efforts to obstruct xAI's access to the accounts. To forestall legal action, ***Li agreed in writing to the very relief xAI now seeks,*** most importantly agreeing to allow xAI to conduct a forensic analysis of Li's [redacted] and other accounts and devices to find and destroy xAI's Confidential Information. Applin Decl. Ex. E. But Li then violated that agreement by failing to give xAI access to the accounts, conveniently "forgetting" the password to a key online account xAI identified as containing its Confidential Information (which password Li had changed only seven days earlier) and failing to disclose the existence of other accounts

[redacted]

entirely. Applin Decl. at ¶ 28. To date, Li has yet to give xAI the access it needs to protect its interests.

Third, ***Li is a flight risk and any delay in justice could effectively amount to a denial***. Li has both a Chinese passport and permanent residency in Canada, and could easily travel beyond this Court's reach. Applin Decl. at ¶¶ 8, 24. And this is no idle speculation—an investigator hired by xAI observed Li leaving his residence with luggage, driving alone with that luggage to the airport, not picking anyone up, and sitting in the parking lot for approximately 45 minutes. Rivera Decl. at ¶ 2. The investigator also observed Li staying in a hotel close to the airport and traveling with luggage. *Id*. at ¶¶ 3-8. And, after selling nearly $7 million of his xAI company stock, Li also has the financial means to flee. Applin Decl. at ¶ 11.

xAI seeks immediate Court action enforcing the Agreement, finding a violation of the DTSA and granting xAI the relief to which xAI is entitled under the Agreement and the DTSA (i.e., forensic imaging, and deletion of stolen information) and in equity (i.e., forbidding Li from working on his new employer's generative AI, including ChatGPT). Immediate Court action is necessary to protect xAI's confidential and proprietary information from further improper use and/or dissemination, as the Agreement, the DTSA, and equity demand. Pochron Decl. at ¶ 27.

II. <u>FACTUAL BACKGROUND</u>

A. xAI Is a Leading AI Company in a Fiercely Competitive Market

xAI is a leading artificial intelligence company founded in 2023 to advance human comprehension and capabilities through its Grok large language models (LLMs) and other advanced AI. Compl., at ¶ 8; Applin Decl. at ¶ 3. xAI's Grok is a preeminent frontier model, representing the cutting edge of AI research and development and pushing the boundaries of what AI can do across multiple domains. Applin Decl. at ¶ 3. Competing alongside OpenAI's ChatGPT, Google's Gemini and China's DeepSeek, Grok's newest release—Grok 4—is one of the most, if not the most, advanced and powerful generative AI systems in the world, leading industry benchmarks in reasoning and pretraining capabilities. *Id*.

B. xAI's Confidential Information Drives Its Competitive Advantage

xAI entered the AI market a year after OpenAI launched ChatGPT in November 2022. *Id*. Because of xAI's extraordinary investment in its innovation, it has been able to deliver the world's most advanced AI model in just two years, leading industry benchmarks in reasoning and pretraining capabilities. xAI

[redacted]

has been able to offer more innovative and imaginative features than ChatGPT. While traditional technologies that shaped Silicon Valley, such as semiconductors and mobile devices, are best safeguarded through patents, the most valuable and sensitive components of modern AI demand broader and more adaptable trade secret protection. Trade secrets protect xAI's innovation and intellectual property, including its model weights, training data, tuning methods, system prompts, know-how, and more. *Id.*

C. xAI Takes Reasonable Measures to Protect Its Trade Secrets

Because xAI's protection of its Confidential Information is paramount to maintaining its competitive edge in the hyper-competitive AI industry, xAI has implemented a variety of industry-leading practices to maintain secrecy, such as: routinely conducting security awareness training for all employees; conducting background checks on employees and contractors who may access xAI data; conducting secure development and data handling training for employees with access to sensitive data, after which such employees must complete an assessment to demonstrate understanding; employing a team dedicated to information security; adopting the NIST 800-171 Rev.3 framework as a baseline for internal security standards; achieving SOC 2, Type II compliance; securing endpoints, including employee devices, with ongoing patch maintenance and full disk encryption; and maintaining a formal written information security policy, among other practices. Applin Decl. at ¶ 4.

In addition, xAI requires employees to enter into the Agreement, which imposes clear obligations to protect xAI's Confidential Information[1] (*id.* at ¶ 5), including that each employee:

- Acknowledges that their employment "creates a relationship of confidence and trust" with respect to xAI's Confidential Information, which xAI "has a protectable interest therein" (Applin Decl. Ex. B ¶ 1.1);

[1] The Agreement defines "Confidential Information" to mean "any and all confidential knowledge, data or information" belonging to xAI, including as relevant here: (a) trade secrets, proprietary technology, inventions, mask works, ideas, processes, formulas, software in source or object code, data, programs, other works of authorship, know-how, improvements, discoveries, developments, designs and techniques, and any other work product of any nature and all Intellectual Property Rights (as defined below) therein (collectively, "Inventions"), including all Company Inventions (as defined below); [and] (g) any other non-public information that a competitor of Company could use to Company's competitive disadvantage. Applin Decl. Ex. B ¶ 1.2.

[redacted]

- Is required to maintain confidentiality "during and after [the employee's] employment," and prohibits disclosure, use, or publication of Confidential Information unless required for the employee's work or expressly authorized by an officer of xAI (*id.*);
- Is required, upon termination, to return "any and all" materials containing or disclosing Confidential Information, including documents, notes, and devices, along with all copies, and "any other material containing or disclosing . . . Confidential Information" (*id.*, ¶ 8);
- Is required to provide xAI with a computer-usable copy of any Confidential Information stored on personal devices or systems and to "permanently delete and expunge" such information (*id.*);
- Is required to "agree to provide [xAI] access to [the employee's] system as reasonably requested to verify that the necessary copying and/or deletion is completed" (*id.*); and
- Is required to "agree to: (a) provide [xAI] any and all information needed to access any [xAI] property or information returned or required to be returned . . . , including without limitation any login, password, and account information." *Id.*

Each employee agrees that "any threatened or actual violation" of the Agreement would "constitute immediate and irreparable injury" to xAI. *Id.* ¶ 9. Each employee also agrees that xAI may remedy those violations with injunctive, specific performance or equitable relief without bond. *Id.*

When an employee resigns, as Li did, xAI requires that the employee sign a Termination Certification verifying that they have complied with the Agreement. Applin Decl. at ¶ 6, Ex. B at 1. The Certification also requires departing employees to certify that they have undertaken a diligent search for all xAI documents and returned them to the company. Applin Decl. Ex. B at 1. It provides that "if [the employee has] used any personal computer, server, or e-mail system to receive, store, review, prepare or transmit any … Confidential Information, [the employee] agree[s] to provide Company with a computer-useable copy of all such Confidential Information and then permanently delete and expunge such Confidential Information from those systems." *Id.* To ensure compliance, the Certification requires the employee to "agree to provide [xAI] access to [the employee's] system as reasonably requested to verify that the necessary copying and/or deletion is completed." *Id.*

[redacted]

D. Defendant Li Breached His Agreement and Certification with xAI by Stealing xAI's Confidential Information and Trade Secrets

Li began working for xAI as a Member of the Technical Staff on or about February 26, 2024 and, as a condition of employment, signed the Agreement on February 26, 2024. *Id.* at ¶ 9. As one of the company's initial group of approximately 20 engineers, Li was responsible for developing and training Grok, xAI's advanced AI model. *Id.* at ¶ 10. In this role, Defendant had access to and responsibility for components across the entirety of xAI's technology stack. *Id.* To support his job responsibilities, xAI entrusted Li with restricted and controlled access to confidential documents and proprietary information, including [redacted]. *Id.*

xAI awarded stock options and shares to Li as part of his compensation. *Id.* at ¶ 11. In the days leading up to his misappropriation of xAI's confidential and trade secret information, Li began liquidating his equity, selling approximately $4.7 million of xAI stock on July 23, 2025, and $2.2 million two days later. All told, Li sold almost $7 million in xAI stock through July 25, 2025. *Id.*

That same day—and three days before he announced his resignation—Li exploited xAI's trust by surreptitiously copying [redacted], from his company-issued laptop to a [redacted] account. *Id.* at ¶ 12. This misappropriated data included Confidential Information and trade secrets with independent economic value in the AI market. *Id.* at ¶ 13. The stolen data is [redacted]. *Id.* The misappropriated data could be used by competitors to preempt xAI's product offerings and market expansion efforts. *Id.* It is sufficient to give any competitor a competitive advantage in the AI race, potentially saving them billions of dollars and years of development time. *Id.*

E. Li Agreed to the Relief xAI Now Seeks but Then Engaged in Subterfuge

Li took extensive measures to conceal his misconduct. He deleted his browser history and system logs, renamed files, compressed them, and appended files together, prior to uploading xAI's Confidential Information to his personal, non-work [redacted]. *Id.* at ¶16; Pochron Decl. at ¶ 25. xAI discovered

[redacted]

Li's theft on August 11, 2025 during a routine review of logs from security software designed to detect and prevent data exfiltration. Applin Decl. at ¶ 16. On that date, xAI sent a demand letter to Li, requiring him to return and delete the stolen data by August 13. *Id*. at 17, Ex. D. The letter also requested a detailed accounting of any disclosures or unauthorized use. *Id*. Ex. D at 1.

Since xAI discovered his theft, Li has been stringing xAI along. He sent his lawyer to talk to xAI while simultaneously changing his passwords and going to the San Jose airport with his luggage. Applin Decl. at ¶ 20 (attorney contact on August 13); Rivera Decl. at ¶ 2 (travel to airport on August 13), Pochron Decl. ¶¶ 10, 11 (password changed August 11/12). Li retained criminal defense counsel and engaged in subterfuge. Li also moved to a hotel near the airport with his luggage. *Id.* at ¶¶ 2-7.

After xAI sent a demand letter to Li, Li and his attorney met with xAI twice. Applin Decl. at ¶ 21. During the meetings, Li left three devices as a supposed "showing of good faith," but did not provide the passwords necessary to access the devices. Applin Decl. at ¶ 25; Pochron Decl. at ¶¶ 8, 9. Also during the meetings, Li admitted, in his own handwriting and verbally, to intentionally taking xAI's files and covering his tracks. Applin Decl. at ¶22; *id*. Ex. G. Li also admitted to signing a job offer with another employer prior to his resignation from xAI, but Li refused to identify the employer. *Id*. at ¶ 23. Subsequently, xAI discovered Li had accepted an offer with OpenAI, one of xAI's main competitors. *See* Pochron Decl. at ¶¶ 18-23.[2]

After four days of negotiations, Li entered into a contract with xAI entitled Authorization for Access to Accounts and Personal Devices ("Authorization"), authorizing, and supposedly granting, access to his [redacted] account and other devices and accounts. Applin Decl. at ¶ 26; *Id*. Ex. E. Li authorized this access to allow xAI to (among other things): search the devices and accounts for the misappropriated Confidential Information and delete any Confidential Information that it found. Applin Decl. Ex. E ¶¶ 2.b, 2.e.

Li promised in the Authorization to provide the passwords necessary to access Li's accounts and devices and handwrote into the Authorization *some* passwords, but he omitted some critical ones,

[2] Li's counsel has represented that he has postponed his start date at OpenAI. Applin Decl. at ¶ 23.

[redacted]

including in particular the password for the [redacted] account to which Li had uploaded xAI's [redacted] [redacted]. Applin Decl. Ex. E ¶2.d; Pochron Decl. at ¶¶ 8, 9. Li later represented through his lawyer that he did not remember the password for that [redacted] account, but that xAI could access the account through one of two laptops Li surrendered to xAI. Applin Decl. Ex. F; Pochron Decl. at ¶¶ 13, 24. xAI's forensic expert was unable to determine any such method of access. Pochron Decl. at ¶¶ 13, 14, 24. xAI's forensic expert did find on the password manager on Li's phone a password—last updated as of August 12, 2025—to access the [redacted] account, but when he tried it, it did not work. Pochron Decl. at ¶¶ 11, 12. What's more, digital artifacts discovered by the forensic expert indicated that the password for the [redacted] account had been changed on ***August 11, 2025***, the *same day* xAI sent its original demand letter to Li. *Compare id. with* Pochron Decl. at ¶ 10. Li's surreptitious alteration of his [redacted] password on August 11 cannot be reconciled with his attorney's representation on August 18, only seven days later, that he "does not recall" the password. Worse, even though Li's iPhone reflected that the stored password associated with his [redacted] account was last updated on August 12, that password *still* failed to provide access to Li's account, which suggests that Li either changed the password ***again*** after August 11 or stored a fake password on his phone on August 12 to conceal the true password. Pochron Decl. at ¶¶ 12, 15, 16. Moreover, a forensic review of Li's phone revealed that Li also had another [redacted] account, a [redacted] account with xAI information, including potentially Confidential Information, and a [redacted] account, all of which Li failed to disclose, let alone provide access to, as required. Pochron Decl. at ¶ 17. When confronted, Li's counsel informed xAI's counsel that Li had "forgotten" the password to these accounts as well.

In short, Li only feigned granting access to his accounts. Despite the appearance of cooperation, Li's false representations and covert activity concerning the [redacted] accounts' and [redacted] account's passwords have deprived xAI of any actual access to those accounts. Thus, the data Li stole remains outside xAI's control. Applin Decl. at ¶¶ 28, 29; Pochron Decl. at ¶ 26. Li has continued to act suspiciously by keeping his luggage with him and staying at a hotel near the airport. Rivera Decl. at ¶¶ 3-8. And, he has the means to flee this Court's jurisdiction, given the financial resources gained from his stock sale. Also, Li is a Chinese national with a passport issued by the People's Republic of China. Applin Decl. at ¶

[redacted]

8, Ex. A. He also claims to be a permanent resident of Canada, and has traveled to Canada at least once in the last year. *Id.* at ¶ 24. xAI has suffered irreparable harm, and will continue to suffer that harm unless Li is enjoined.

III. THE COURT SHOULD GRANT THE TEMPORARY RESTRAINING ORDER

A. Legal Standard

The standard for issuing a temporary restraining order is identical to the standard for issuing a preliminary injunction. *Google LLC v. Point Fin., Inc.*, No. 5:25-CV-04033-BLF, 2025 WL 1616533, at *2 (N.D. Cal. June 6, 2025) (citing *Washington v. Trump*, 847 F.3d 1151, 1159 n.3 (9th Cir. 2017)). "A plaintiff seeking a preliminary injunction must establish that [they are] likely to succeed on the merits, that [they are] likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [their] favor, and that an injunction is in the public interest." *Doe v. San Diego Unified Sch. Dist.*, 19 F.4th 1173, 1176 (9th Cir. 2021) (citation omitted). A "TRO should be restricted to preserving the status quo and preventing irreparable harm just so long as is necessary to hold a preliminary injunction hearing and no longer." *Google LLC*, 2025 WL 1616533, at *2 (cleaned up, citing *E. Bay Sanctuary Covenant v. Trump*, 932 F.3d 742, 779 (9th Cir. 2018)). The Ninth Circuit applies a "sliding scale" approach to preliminary injunctions, granting preliminary relief even if serious questions as to the merits are raised, so long as the balance of hardships tips sharply in the plaintiff's favor. *Doe v. San Diego Unified Sch. Dist.*, 19 F.4th 1173, 1177 (9th Cir. 2021).

B. TRO Factor 1: xAI Is Likely To Prevail On The Merits

xAI is likely to succeed on the merits on two causes of action relevant here: (1) violation of the Defend Trade Secrets Act, 18 U.S.C. § 1831 et seq., and (2) breach of contract.

The DTSA requires "a plaintiff to show that it possessed a trade secret, that the defendant misappropriated the trade secret, and that the defendant's conduct damaged the plaintiff." *WeRide Corp. v. Kun Huang*, 379 F. Supp. 3d 834, 845 (N.D. Cal. 2019), *modified in part*, No. 5:18-CV-07233-EJD, 2019 WL 5722620 (N.D. Cal. Nov. 5, 2019). As defined in the DTSA, misappropriation means the "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means" or "disclosure or use of a trade secret of another without express or

[redacted]

implied consent by a person who … used improper means to acquire knowledge of the trade secret," while "improper means" includes "theft," "misrepresentation," and "breach of a duty to maintain secrecy." 18 U.S.C. § 1839(5)-(6).

In *Waymo LLC v. Uber Techs., Inc.*, the court found a likelihood of success on the merits where a company provided "compelling" evidence that an employee had "pilfered over 14,000 files" along with an initial showing that "at least some" of the stolen information "likely qualifies for trade secret protection[.]" No. C 17-00939 WHA, 2017 WL 2123560, at *7-10 (N.D. Cal. May 15, 2017). Here, as in *Waymo*, xAI has made a strong showing that Li "pilfered" [redacted] when he uploaded the files to [redacted] account—indeed, Li has admitted as much. Applin Decl. at ¶22; *id*. Ex. G. And the misappropriated information qualifies as confidential trade secret information because, as it "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information" and because xAI has "taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3); *see also Integral Dev. Corp. v. Tolat*, 675 F. App'x 700, 703 (9th Cir. 2017) ("Source code, which conveys facts or ideas, qualifies for trade secret protection" under California's nearly identical definition of trade secret) (citing *Altavion, Inc. v. Konica Minolta Sys. Lab. Inc.*, 226 Cal. App. 4th 26, 56 (2014)).[3]

[3] The DTSA provides that an "owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C.A. § 1836(b)(1). The interstate requirement is easily met here because xAI customers, including customers located across the U.S., access Grok 4 through the computer web browsers at grok.com, mobile apps and by API access. Applin Decl. ¶ 32. Internet traffic serving many of these customers crosses state boundaries. Grok 4 is thus a product or service used or intended for use in interstate commerce. *BarZ Adventures Inc. v. Patrick*, No. 4:20-CV-299, 2023 WL 2478550, at *9 (E.D. Tex. Mar. 13, 2023) (requirement satisfied where trade secrets relate to mobile apps); *Complete Logistical Servs., LLC v. Rulh*, 350 F. Supp. 3d 512, 520 (E.D. La. 2018) (requirement satisfied because defendant transacts business in other states by phone and internet, as well as by mail and in person); *Albert S. Smyth Co. v. Motes*, No. CV CCB-17-677, 2018 WL 3635024, at *3 (D. Md. July 31, 2018) (requirement satisfied because a court may "easily infer that an online" business "attracts out-of-state customers").

[redacted]

As to independent economic value, the xAI data Li misappropriated is the result of the culmination of billions of dollars of investment and multiple years of AI development and training. Applin Decl. at ¶ 13. The xAI data that Li uploaded is [redacted], and use the data to obtain a competitive advantage against xAI by preempting its product offerings and corporate objectives. *Id*. The data could be weaponized by competitors such as OpenAI to, at a minimum, improve competing products such as ChatGPT with Grok's more innovative and imaginative features which make Grok one of the most, if not the most, intelligent generative AI chatbots, undermine xAI's product roadmap, and disrupt its market expansion strategy. *Id*. It could save OpenAI and other competitors billions in R&D dollars and years of engineering effort, handing any competitor a potentially insurmountable advantage in the race to dominate the AI landscape. *Id*. Indeed, advanced AI models can cost greater than hundreds of millions of dollars to develop.[4]

And, xAI took at least reasonable measures to keep the information secret, including implementing all the technical measures described above, requiring employees to sign the Agreement and Termination Waiver, and even deploying the security software that detected Li's data exfiltration. *See*, e.g., *Posdata Co. v. Kim*, No. C-07-02504RMW, 2007 WL 1848661, at *5 (N.D. Cal. June 27, 2007) (in TRO context, finding plaintiff's use of confidentiality agreements and internal security measures constituted reasonable measures to protect trade secrets).

Li's trade secret misappropriation harmed and continues to harm xAI given the independent economic value (as discussed above) Li has put at risk, and for the reasons articulated in the next section, including diminished value of its Trade Secrets, loss of its competitive advantage, loss of business, and harm to its reputation and goodwill. Li already conceded in the Agreement that any breach thereof would result in irreparable injury to xAI. Applin Ex. B ¶ 9.1. To prevail on its breach of contract claim, xAI must prove: (1) the existence of the contract; (2) xAI's performance or excuse for nonperformance; (3) Li's breach; and (4) injury to xAI because of the breach. *Bodenburg v. Apple*, No. 24-3335, 2025 WL 2055748,

[4] Katharina Buchholz, *The Extreme Cost Of Training AI Models*, Forbes (Aug. 23, 2024), https://www.forbes.com/sites/katharinabuchholz/2024/08/23/the-extreme-cost-of-training-ai-models/.

[redacted]

at *3 (citing *Oasis W. Realty, LLC. v. Goldman*, 51 Cal. 4th 811, 821 (2011)). xAI is certain to succeed on the merits because Li has already admitted the first and third elements: the existence of the Agreement and his wrongful misappropriation of xAI's Confidential Information. Applin Decl. at ¶ 22; *id*. Ex. G. And, as to the second element, Li cannot dispute that xAI fully performed under the Agreement by compensating Li for his work as was stipulated in the Agreement.

As outlined above, Li has also clearly breached his Agreement, which required Li to protect the confidentiality of xAI's Confidential Information, by sending [redacted], to [redacted] account. Applin Decl. Ex. B ¶1.1; *id*. at ¶¶ 12, 22. He further breached the Agreement by refusing to return that information upon his departure, despite certifying his duty to do so and despite affirmatively representing that he had or would do so. *Id.* at ¶ 15, Ex. C. Li has admitted this in meetings with xAI while represented by counsel. Applin Decl. at ¶ 22; *id*. Ex. G.

And xAI has suffered injury because of the breach. Indeed, Li already conceded in the Agreement that any breach thereof would result in irreparable injury to xAI. Applin Ex. B ¶ 9.1. Regardless, xAI has also suffered and will continue to suffer diminished value of its intellectual property and other injuries, as described below, from Li's breach of the Agreement. Applin Decl. at ¶ 13. xAI has thus established a strong likelihood of success on the merits of its claim for breach of contract.

Courts in this district have found likelihood of success satisfied in similar circumstances. *See, e.g.*, *Henry Schein, Inc. v. Cook*, 191 F. Supp. 3d 1072, 1077 (N.D. Cal. 2016) (finding likelihood of success on the merits on misappropriation and breach of contract claims when defendant breached employment agreement by "e-mail[ing] and download[ing] to her personal devices, confidential information . . . before leaving her employment to work at a competitor"); *Tesla Inc. v. Khatilov*, 2021 WL 624174, at *1 (N.D. Cal. Jan. 22, 2021) (finding "substantial likelihood" of success on misappropriation and contract claims where defendant transferred 26,377 files "to his personal cloud storage account"); *WeRide Corp.*, 379 F. Supp. 3d at 848 (finding likelihood of success on misappropriation claims when defendant downloaded plaintiff's confidential information onto personal devices before leaving company for competitor and deleted logs to cover his tracks); *Comet Techs. U.S. of Am. Inc. v. Beuerman*, No. 18-CV-01441-LHK, 2018 WL 1990226, at *6 (N.D. Cal. Mar. 15, 2018) (granting motion for TRO, expedited discovery, and evidence preservation where employee downloaded over a hundred confidential documents from plaintiff's servers, saved them to an external memory device, lied about it, and tried to conceal his misconduct when confronted); *see also Edwards Lifesciences Corp. v. Launey*, 2023 WL 4680774, at *4 (C.D. Cal. June 12, 2023) (finding strong likelihood of success on misappropriation and breach of contract claims where defendant breached employment agreements by transmitting confidential information to himself before leaving employment); *Pyro Spectaculars N., Inc. v. Souza*, 861 F. Supp. 2d 1079, 1099 (E.D. Cal. 2012) (granting TRO and motion for expedited discovery where employee downloaded plaintiff's confidential documents and information).

C. TRO Factor 2: xAI Will Suffer Irreparable Harm Absent Relief

Li's theft of xAI's sensitive Confidential Information poses a threat of irreparable harm for which there is no adequate remedy at law. *First*, Li already "agree[d] that any threat or actual violation of [the Agreement] or any of its terms will constitute immediate and irreparable injury to [xAI], and [xAI] will have the right to enforce [the Agreement] … by injunction, specific performance or other equitable relief, without bond …." Applin Decl. Ex. B ¶ 9.1. Li's "agree[ment] that his breach would cause irreparable harm" is "evidence of irreparable harm." *Mechanix Wear LLC v. Branson*, No. 2:24-CV-03090-RGK-AJR, 2024 WL 2846068, at *4 (C.D. Cal. Apr. 23, 2024); *see also Ticor Title Ins. Co. v. Cohen*, 173 F.3d 63, 68 (2d Cir. 1999).

Second, even setting Li's admission aside, irreparable harm is plain, because courts "in this district have presumed that [a] Plaintiff will suffer irreparable harm if its proprietary information is misappropriated." *Google LLC,* 2025 WL 1616533, at *5 (cleaned up); *see also DVD Copy Control Ass'n, Inc. v. Bunner*, 31 Cal. 4th 864, 875 (Aug. 25, 2003), *as modified*, (Oct. 15, 2003) ("California law clearly contemplates the use of injunctive relief as a remedy for trade secret misappropriation."). Li stole [redacted] and other development information. xAI has invested tremendous resources developing its AI products and services, including years of engineering effort and billions of dollars in financial investment. Applin Decl. at ¶ 13. *Comet Techs.*, 2018 WL 1990226, at *5 (granting TRO where defendant took data related to project that plaintiff spent "expenditure of

[redacted]

considerable time and resources on"). The harm from allowing continued access and misuse of xAI's data "cannot be unwound after the fact, nor can it be adequately compensated for with monetary damages." *Waymo LLC v. Uber Techs.*, Inc., 2017 WL 2123560, at *10-11 (N.D. Cal. May 15, 2017) (finding a likelihood of irreparable harm where defendant maintained possession of over 14,000 files, which the court categorized as "a treasure trove" presenting "an ever-present danger wholly at [defendant's] whim.").

Third, immediate relief is critical here because the stolen Confidential Information would give any competitor or adversary a competitive advantage in the AI race and harm xAI's own ability to compete. Applin Decl. at ¶ 13; *OOO Brunswick Rail Mgmt. v. Sultanov*, No. 5:17-CV-00017-EJD, 2017 WL 67119, at *3 (N.D. Cal. Jan. 6, 2017) (in trade-secret context, dissemination of confidential information to "[Claimant's] [] competitors … would cause [Claimant] irreparable harm."). The information would give a competitor or adversary a playbook into the development of the most advanced frontier AI model on the market, thus saving a competitor or adversary billions of dollars in investment and years of development time. Applin Decl. at ¶ 13. And this competitive harm is far from speculative, because Li already had an accepted job offer to work at OpenAI prior to resigning from xAI, making the risk of irreparable harm to xAI especially acute. Pochron Decl. at ¶¶ 22, 23. Allowing a competitor or adversary to incorporate xAI's confidential information into its own products will certainly result in a loss of prospective customers and goodwill to xAI. Applin Decl. at ¶ 13; *Henry Schein, Inc.*, 191 F. Supp. at 1077 ("threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm") (*quoting Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001)). Any xAI competitor or adversary that hires Li could thus gain an unfair advantage from Li's theft, and thus severely prejudice xAI's competitive position. Applin Decl. at ¶ 13. This remains true even if Li accesses the data without that competitor's knowledge or blessing, because Li could deceive his new employer—as he has deceived xAI here—by surreptitiously incorporating xAI's Confidential Information into the competitor's products and passing it off as his own original work. Moreover, Li may have already shared trade secrets with OpenAI, making an injunction to prevent further sharing imperative. Without immediate action by this Court, xAI thus risks irreparable harm that cannot be remedied by money damages or other post-

[redacted]

judgment relief.

Fourth, emergency relief is critical to ensure that Li cannot remove xAI's Confidential Information to another country and thus permanently beyond the reach of xAI and this Court. *Imi-Tech Corp. v. Gagliani*, 691 F. Supp. 214, 230 (S.D. Cal. 1986) (risk of use of trade secrets in another country supported finding of irreparable harm because defendant would be "placing the subject matter of this litigation beyond the jurisdiction of this court, thereby denying [plaintiff] the opportunity of obtaining complete relief"). As detailed above, Li arranged to have millions in cash on hand the day he downloaded xAI's data. Applin Decl. at ¶¶ 11, 12. He is also a Chinese national, and purports to be a permanent resident of Canada, where he traveled just last year. *Id.* at ¶¶ 8, 24; *id*. Ex. A. He thus has the means to flee to a foreign nation beyond the jurisdiction of the United States Courts, and take the Confidential Information with him. Indeed, Li was seen between August 13 and August 15 traveling with a suitcase and loitering in his car at the San Jose airport—even *after* he retained counsel. Rivera Decl. at ¶¶ 2-8.

D. TRO Factor 3: The Balance of Equities Weighs Heavily in Favor of Injunctive Relief

The balance of equities also strongly favors xAI. "To qualify for injunctive relief, [p]laintiff must establish that the balance of the equities tips in [its] favor." *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1138 (9th Cir. 2009) (quote omitted). A court has the "duty … to balance the interests of all parties and weigh the damage to each." *L.A. Mem'l Coliseum Comm'n v. Nat'l Football League*, 634 F.2d 1197, 1203 (9th Cir. 1980). As discussed above, the likely harm to xAI is substantial. *See supra* Section III.B.

Yet if enjoined, Li will sustain no injury, as all he must do is comply with the law and the Agreement and Authorization he signed. *See WeRide*, 379 F. Supp. 3d at 854 ("no burden for [defendant] to do what the law already requires"); *see also Henry Schein*, 191 F. Supp. 3d at 1077 (no undue burden from enjoining defendant from "conduct that is already prohibited under the provisions of" a confidentiality agreement). Indeed, in executing the Agreement, Li already agreed to maintain the confidentiality and security of xAI's Confidential Information after his employment, to refrain from disclosing, using or publishing the information, to return all such information to xAI and to grant the Company any information needed to access that information, duties he flagrantly breached. Applin Decl. Ex. B. The temporary restraining order, which seeks essentially the same relief that Li already agreed to,

[redacted]

cannot possibly be an impermissible burden on him. And the Authorization that Li agreed to seeks only to effectuate those same terms—the complete return of xAI's Confidential Information. Applin Decl. Ex. E.

Without the requested relief, xAI cannot be assured that the threat of imminent harm has been neutralized and that any further copying and misuse of its Confidential Information has been remediated or ruled out. Any slight burden on Li is thus no more than is necessary to protect xAI's rights in the face of Li's admitted misconduct and the irreparable harm it poses. *See Waymo*, 2017 WL 2123560, at *11; *Implicit Conversions, Inc. v. Stine*, 2024 WL 4112335, at *12 (N.D. Cal. Sept. 6, 2024) (granting preliminary injunction because it "will serve all parties' interests while the questions driving this litigation are resolved"); *Cutera, Inc. v. Lutronic Aesthetics, Inc.*, 444 F. Supp. 3d 1198, 1209 (E.D. Cal. 2020) (where employees were found to engage in deliberate misappropriation, the court found that an injunction "specially focused" on preventing the use of misappropriated trade secrets was appropriate); *Bank of Am., N.A. v. Immel*, No. C 10-02483 CRB, 2010 WL 2380877, at *3 (N.D. Cal. June 11, 2010) (in trade-secret context, an injunction seeking "only the return of [Plaintiff's] confidential information and a prohibition on the use of that information by [Defendant]" imposes only "slight" harm).

Thus, the equities strongly weigh in favor of granting the equitable relief sought.

E. TRO Factor 4: Granting The Temporary Restraining Order Is In The Public Interest

Issuing an injunction will also serve the public good, because the public has a strong interest in protecting xAI's Confidential Information. *WeRide*, 379 F. Supp. 3d at 854 ("Courts often find that the public has a strong interest in protecting intellectual property rights"). "[T]here is also a public interest in favor of enforcing employment agreements." *Branson*, 2024 WL 2846068, at *5; *see also Henry Schein*, 191 F. Supp. 3d at 1078 (the "public interest is served when [a] defendant is asked to do no more than abide by trade laws and the obligations of contractual agreements signed with [his] employer"). When, as here, a party has shown that it meets all other grounds for the issuance of a temporary restraining order, "it follows that the public's interest in these circumstances favors an injunction 'specifically focused' on [Li's] use of any misappropriated trade secrets." *Cutera, Inc.*, 444 F. Supp. 3d at 1120.

Indeed, granting this temporary restraining order is critical not only to xAI, but to the maintenance

[redacted]

of a fair and free market and robust competitive landscape, which are foundational to the public interest. The protection and enforcement of valid intellectual property rights are essential to maintaining a level playing field among competitors, preventing unfair advantages, and fostering the innovation and investment that drive economic growth. When a company such as xAI invests tremendous resources into developing leading AI models and protecting the Confidential Information associated therewith, those investments represent not only the company's own resources, but the collective efforts and careers of its employees. To permit the brazen misappropriation of such Confidential Information would profoundly undermine the integrity of the competitive process and disserve the national interest in maintaining and furthering leadership in AI innovation. The United States has ardently and unambiguously expressed its continued interest in preserving its position of leadership in the AI industry.[5] The public interest is thus served in ordering Li to honor his contractual obligations, and preventing him from using or disclosing xAI's Confidential Information.

F. Requested Relief

xAI respectfully requests the relief set forth in the Proposed Order Granting Plaintiffs' Motion for Temporary Restraining Order. The relief falls loosely into two buckets: (1) an Order that Li abide by his obligations in the Agreement, Termination Waiver and Authorization, including importantly that xAI be granted forensic access to find and remove its Confidential Information from Li's accounts and devices; (2) an Order preventing Li from having a role or responsibility at, or communications with, OpenAI or other xAI competitor that would jeopardize xAI's trade secrets.

Regarding the former, while xAI seeks a Court order compelling Li to comply with his obligations under the Agreement and Termination Waiver, Li has demonstrated a willful disregard for both the law and his contractual commitments—even after receiving counsel from criminal defense and employment attorneys. As a result, xAI requires more than mere enforcement. It must be able to recover its intellectual

[5] *Removing Barriers to American Leadership in Artificial Intelligence*, Presidential Action, The White House, Jan. 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers -to-american-leadership-in-artificial-intelligence/ ("It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security.").

[redacted]

property and ensure it is no longer in Li's possession. This can only be achieved through a Court order authorizing a forensic examination, by a qualified expert, of all of Li's personal accounts and devices. Notably, Li has already agreed to this relief, though his agreement appears to be yet another unfulfilled promise. xAI respectfully requests that the Court grant the relief to which Li has already consented.

As to the latter, the court in *Waymo,* on very similar facts, granted Waymo similar relief against competitor Uber. The court noted that its order "mainly prohibits" Waymo's former employee "from working on" the competing technology which Uber had already "implemented on its own initiative." *See Waymo*, 2017 WL 2123560, at *13. The court concluded that "the hardship on defendants will be minimal. On the other hand, this will provide considerable protection to Waymo against [their former employee's] potential misuse of its proprietary information in competing technology." *Id*. Noting that even if the former Waymo employee committed not to use the trade secrets, "his word under these circumstances would be cold comfort against the danger of trade secret misappropriation for Uber's benefit." *Id*. at *5, 13 (ordering that the defendants including Uber "(a) remove [the former Waymo employee] from any role or responsibility pertaining to [the competing technology]; [and] (b) take all steps in their power to prevent him from having any communication on the subject of [the competing technology] with any officer, director, employee, agent, supplier, consultant, or customer of defendants."). The same reasoning applies with even more force here where not only has OpenAI already developed the competing generative AI technology and commanded 80 percent of the market, but where Li has continually engaged in subterfuge and shows no ability to keep his word. Moreover, because Li has not yet commenced employment at OpenAI and remains at risk of joining another xAI competitor before xAI can fully recover its trade secrets, xAI respectfully requests that the Court extend the scope of its order to encompass other potential competitors as well.

IV. THE COURT SHOULD PERMIT EXPEDITED DISCOVERY

xAI seeks expedited discovery to determine (a) the current location of its misappropriated Confidential Information, (b) whether and under what circumstances Confidential Information has been disclosed and (c) whether Li or anyone else is currently using it. xAI also seeks discovery to investigate Li's communications with others about the Confidential Information and to conduct a forensic

[redacted]

examination of Li's devices and accounts. Finally, xAI seeks discovery to uncover details about Li's new employer. Proposed interrogatories and inspection requests are attached to the Declaration of Carson Swope as Exhibits B and C. Finally, xAI seeks a deposition to explore the topics therein with Li.

A. Expedited Discovery Is Necessary to Prevent Further Irreparable Harm to xAI

Although parties generally may not seek discovery before the conference required by Federal Rule of Civil Procedure 26(f), a "[c]ourt may authorize early discovery … if the requesting party establishes 'good cause' for" it. *Strike 3 Holdings, LLC v. Doe*, No. 24-CV-03852-PHK, 2024 WL 4445129, at *3 (N.D. Cal. Oct. 8, 2024) (quoting *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002)); *see also* Fed. R. Civ. P. 26(d)(1) (permitting discovery before Rule 26(f) conference "by court order"). "Good cause may be found where the need for expedited discovery, in consideration of the administration of justice, outweighs prejudice to the responding party." *Strike 3 Holdings*, 2024 WL 4445129, at *3.

Protecting xAI from further irreparable harm is reason enough to permit expedited discovery here. *See Comet Techs.*, 2018 WL 1990226, at *7 (granting expedited discovery in a trade secrets case because it "is essential in order to minimize any harm to Plaintiff's competitive position"); *WeRide Corp.*, 379 F. Supp. 3d at 854 (expedited discovery "will help to minimize harm to WeRide's competitive position and to protect WeRide's trade secrets from disclosure"). xAI needs the requested expedited discovery to determine the whereabouts and potential use or disclosure of its Confidential Information. xAI has no other source of obtaining this information, except through interrogation of Li and his devices and accounts, and subpoenas of at least OpenAI, [redacted], and [redacted]. Without expedited discovery, xAI will be unable to mitigate the ongoing irreparable harm caused by Li's misappropriation, and thus good cause is met.

B. Additional Factors Favor Expedited Discovery Here

In balancing the need for discovery against the prejudice to the defendant, some courts also consider: (a) whether a preliminary injunction is pending; (b) the breadth of the discovery requests; (c) the purpose for requesting the expedited discovery; (d) the burden to comply with the requests; and (e) how far in advance of the typical discovery process the request was made. *Strike 3 Holdings*, 2024 WL 4445129, at *3. These factors do not impose a rigid test. Rather, the "good cause" standard is "flexible,"

[redacted]

and courts have "broad discretion" in determining whether to grant early discovery *Semitool*, 208 F.R.D. at 275; *Strike 3 Holdings*, 2024 WL 4445129, at *3. Each factor supports permitting expedited discovery here.

Preliminary Injunction: This Motion seeks an order to show cause for a preliminary injunction and the expedited discovery will support that request. The discovery will also help the Court fashion appropriate relief, and thus this factor "weigh[s] in favor of" xAI's "request to conduct expedited discovery." *Light Salt Invs., LP v. Fisher*, No. 13CV1158- MMA DHB, 2013 WL 3205918, at *2 (S.D. Cal. June 24, 2013) (finding first factor weighed in favor of expedited discovery because plaintiff "indicates that it plans to file a motion for preliminary injunction in the near future").

Breadth of the Discovery: The requested discovery is narrowly tailored to support this Motion and xAI's request for a preliminary injunction. *Comet Techs.*, 2018 WL 1990226, *7 (granting request for expedited discovery to "[q]uickly determin[e] what information [d]efendant removed from Plaintiff, and whether and how [p]laintiff's information is being used by [p]laintiff's competitors"). The same is true for the requested forensic examination of Li's devices and accounts. *Charles Schwab & Co. v. Newton*, No. 16-cv-00236, 2016 WL 1752767, at *1 (M.D. La. May 2, 2016) (ordering defendant to "make any and all such data, devices and media available for inspection, imaging and duplication by [p]laintiff's counsel and/or [p]laintiff's computer forensic consultants"); *Ameriwood Indus., Inc. v. Liberman*, No. 06-cv-524, 2006 WL 3825291, at *4 (E.D. Mo. Dec. 27, 2006), *amended*, 2007 WL 685623 (E.D. Mo. Feb. 23, 2007) ("allegations that a defendant downloaded trade secrets onto a computer provide a sufficient nexus between plaintiff's claims and the need to obtain a mirror image of the computer's hard drive"). And, as noted above, Li has already deleted files *and* made false and misleading representations in an attempt to conceal his wrongdoing. Pochron Decl. at ¶ 25. Expedited discovery, including an order requiring Li to turn over his personal accounts and devices for inspection, is necessary to prevent any further loss of evidence from similar misdeeds. *See, e.g., WeRide Corp.,* 379 F. Supp. 3d at 854 (granting motion for expedited discovery in trade secret and breach of contract case against former employees that had "already deleted computer files on at least two relevant devices").

Purpose of the Discovery: The discovery seeks (a) to determine the scope of misappropriation of

[redacted]

confidential and proprietary information and trade secrets, (b) to mitigate ongoing irreparable harm from the misappropriation, and (c) to aid the Court in fashioning appropriate preliminary relief, all proper purposes in a stolen-information case like the one here. *See, e.g., Beuerman*, 2018 WL 1990226, at *7 (granting expedited discovery to "[q]uickly determin[e] what information [d]efendant removed from [p]laintiff, and whether and how [p]laintiff's information is being used by [p]laintiff's competitors"); *Advanced Portfolio Techs., Inc. v. Advanced Portfolio Techs. Ltd.*, No. 94-cv-5620, 1994 WL 719696, at *4 (S.D.N.Y. Dec. 28, 1994) (allowing expedited discovery before preliminary injunction motion because "[plaintiff's] contention that [defendant] has misused confidential or proprietary information … sufficiently support[s] the requested expedited discovery"); *Fisher*, 2013 WL 3205918, at *2 (authorizing expedited discovery because plaintiff "has shown that it needs" the discovery "to support its contemplated motion for preliminary injunction"); *Wachovia Sec., LLC v. Stanton*, 571 F. Supp. 2d 1014, 1049-50 (N.D. Iowa 2008) (granting plaintiff's motion for expedited discovery to prepare for preliminary injunction hearing in trade secret misappropriation case).

Burden on Li: xAI has crafted narrowly tailored discovery requests to obtain information without undue burden. Indeed, Li already agreed, in the Agreement and Authorization, to provide xAI with access to Li's devices and accounts so that xAI can identify and delete its Confidential Information, obligations that mirror the proposed discovery here. Applin Decl. Ex. B ¶ 8, Ex. E. It is no burden to require Li to comply with his prior agreements.

Timing of Request: "[T]his factor, alone, does not make the requested [discovery] unreasonable." *Fisher*, 2013 WL 3205918, at *2. Indeed, as noted above, courts routinely permit expedited discovery where, as here, xAI has shown good cause otherwise exists for allowing it.

V. CONCLUSION

For the foregoing reasons, xAI respectfully requests that the Court issue (a) the Proposed Temporary Restraining Order and Order Permitting Expedited Discovery without bond and (b) the Proposed Order to Show Cause re Preliminary Injunction on an urgent and expedited basis.

[redacted]

Dated: August 28, 2025

WINSTON & STRAWN LLP

By: */s/ Kathi Vidal*
KATHI VIDAL
ALEXANDER H. COTE
CARSON SWOPE

Attorneys for Plaintiffs X.AI Corp. and X.AI LLC

KATHI VIDAL (State Bar No. 194971)
kvidal@winston.com
CARSON SWOPE (State Bar No. 353352)
cswope@winston.com
WINSTON & STRAWN LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
Telephone: (650) 858-6500
Facsimile: (650) 858-6550

ALEXANDER H. COTE (State Bar No. 211558)
accote@winston.com
WINSTON & STRAWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071-1543
Telephone: (213) 615-1700
Facsimile: (213) 615-1750

Attorneys for Plaintiffs X.AI Corp. and X.AI LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

X.AI Corp., a Nevada corporation, and X.AI LLC, a Nevada limited liability company,

Plaintiffs,

vs.

XUECHEN LI, an individual

Defendant.

Case No. 3:25-cv-07292

COMPLAINT FOR:

(1) BREACH OF EMPLOYEE CONFIDENTIAL INFORMATION AND INVENTION ASSIGNMENT AGREEMENT AND TERMINATION CERTIFICATE AND AUTHORIZATION;
(2) MISAPPROPRIATION OF TRADE SECRETS (18 U.S.C. § 1836 ET SEQ.);
(3) VIOLATION OF COMPUTER DATA AND ACCESS FRAUD ACT (CAL. PENAL CODE § 502); AND
(4) FRAUD

JURY TRIAL DEMANDED

Plaintiffs X.AI Corp. and X.AI LLC (collectively "Plaintiff" or "xAI") for their Complaint against Defendant Xuechen Li ("Defendant") state as follows:

NATURE OF ACTION

1. This is an action for willful and malicious misappropriation of xAI's confidential information and trade secrets under (18 U.S.C. § 1836 et seq.) by Defendant, as well as for breach of contract, fraud, and violation of the Computer Data Access Fraud Act (Cal. Penal Code § 502).

PARTIES

2. X.AI Corp. is a Nevada corporation with its principal place of business located in Palo Alto, California.

3. X.AI LLC is a Nevada limited liability company and wholly owned subsidiary of X.AI Corp., having a principal place of business in Palo Alto, California.

4. Defendant is a Chinese national, with a passport issued by the People's Republic of China. He also purports to be a permanent resident of Canada. At all relevant times, he has been a resident of Mountain View, California.

JURISDICTION AND VENUE

5. Jurisdiction is proper in this district pursuant to 28 U.S.C. § 1331 because xAI asserts claims under the federal Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq.* This Court has supplemental jurisdiction over xAI's additional claims because they form part of the same case or controversy. 28 U.S.C. § 1367(a).

6. This Court has personal jurisdiction over Defendant because Defendant expressly consented to personal jurisdiction in a written agreement with xAI. *See Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 458 (9th Cir. 2007).

7. Venue is proper in this district under 28 U.S.C. §§ 1391(b)(1) and (b)(2) because Defendant resides in this district, a substantial part of the events or omissions giving rise to xAI's claims occurred in

this district, and because Defendant expressly consented to venue in this district in a written agreement with xAI.

GENERAL ALLEGATIONS

The Ascent of Artificial Intelligence ("AI")

8. The rise of generative AI products for public use is one of the most transformative technological shifts of the 21st century. Generative AI refers to systems that can create new content—text, images, music, code, and more—by learning patterns from massive datasets. Unlike traditional AI, which classifies or predicts, generative AI produces original outputs.

9. The advent of modern generative AI is often credited to the rapid rise and popularization of large language models (LLMs), a class of AI systems designed to understand and generate human-like text, images, code, and other forms of content. However, LLMs represent but one of the groundbreaking advancements in artificial intelligence. Generative AI has seen extremely rapid development in other areas in recent years, particularly in the fields of image generation, video generation, speech generation, and multimodal generation—the simultaneous generation of multiple output modalities at once.

10. These generative AI models are built upon sophisticated neural architectures—a complex network of nodes and edges, analogous to the neurons and synapses of a human brain—which enable the models to generate content that demonstrates human-like semantic and conceptual understanding, but at speeds far exceeding human capability. Such generative AI models have become a foundational technology across industries, powering virtual assistants, educational platforms, creative tools, and enterprise automation systems. Their ability to scale across domains and adapt to user needs has made them indispensable in modern digital infrastructure.

11. The development of such generative AI models requires extraordinary financial and technical resources. Building a state-of-the-art model involves data acquisition and processing, computational infrastructure, and expert talent. Immense capital investment is necessary to curate high-quality datasets, operate thousands of high-performance GPUs, and employ top-tier AI researchers.

12. Generative AI models have delivered immense value to individuals and society at large. They enhance productivity by, among other things, automating routine tasks, improving access to education through personalized tutoring, supporting healthcare professionals with diagnostic assistance, and empowering creators with tools for content generation. Their ability to operate seamlessly across languages facilitates global communication, while their scalability allows organizations to process and generate vast amounts of content with unparalleled efficiency. The societal benefits of generative AI are profound, and the next steps in advancing generative AI depend greatly on the protection of intellectual property and trade secrets that underpin their development.

13. OpenAI took seven years to develop and finally release its first generative AI chatbot product, ChatGPT, in November 2022 which marked the beginning of widespread public access to conversational generative AI tools. ChatGPT uses versions of its generative pre-trained transformer (hence, "Chat**GPT**") models—such as GPT-3.5, GPT-4, and GPT-o3—as its underlying LLMs.

14. Since ChatGPT's public debut in late 2022, generative AI—particularly in the form of conversational chatbots capable of back-and-forth messaging streams—has rapidly become a fixture in daily life. By August 2024, nearly 40% of U.S. adults aged 18 to 64 reported using generative AI tools, either at work or at home.[1] This widespread adoption occurred at a pace faster than that of the personal computer or the internet, making generative AI one of the most swiftly embraced technologies in modern history.

15. During this same period, OpenAI's ChatGPT quickly rose to dominance. Today, OpenAI has over 80 percent of the generative AI chatbot market.

[1] https://news.harvard.edu/gazette/story/2024/10/generative-ai-embraced-faster-than-internet-pcs/ ("As of August, nearly 40 percent of U.S. adults aged 18-64 had used generative AI …. That pickup rate is significantly faster than the public embrace of the internet (20 percent after two years) or the personal computer (20 percent after three years, the earliest researchers could measure).")

Plaintiff xAI and its Technology

16. xAI entered the market in November 2023 and in two short years, through extensive investment in human capital and technology, it has become a leading generative AI company. xAI's vision is to advance human comprehension and capabilities through its advanced AI, including xAI's generative AI model, Grok. Grok is a preeminent frontier model, representing the cutting edge of AI research and development and pushing the boundaries of what AI can do across multiple domains. Competing alongside OpenAI's ChatGPT, Google's Gemini and China's DeepSeek, xAI's newest release—Grok 4—is one of the most, if not the most, advanced and powerful generative AI systems in the world, leading industry benchmarks in reasoning and pretraining capabilities.

17. Grok 4 is the culmination of years of research and development, and billions of dollars in investments. These efforts have required the collaboration of highly skilled teams of engineers, scientists, and other professionals, all working to advance the state of the art in AI.

18. Grok is a conversational generative AI developed by xAI that is capable of many functions, including (a) performing natural language processing tasks, including answering questions, retrieving information, writing creatively, and assisting with coding, (b) interpreting, editing, and generating images or videos in various styles from fanciful to photorealistic, and also (c) generating natural language audio responses in response to oral prompts from a user.

19. xAI operates in a highly competitive landscape for AI models, with several key players developing advanced AI systems. xAI's direct domestic competitors include OpenAI's ChatGPT, Google's Gemini and Anthropic's Claude, among others.

20. Experts predict that the market value of AI technology will exceed hundreds of billions of dollars this year, and over a trillion dollars by decade's end.[2] Moreover, advanced AI models can cost

[2] Statista projects the size of the artificial intelligence market to reach $244,220,000,000 in 2025, and expects the market size to show an annual growth rate of 26.6% over the course of the next six years, culminating in a market volume of $1 trillion by 2031. https://www.statista.com/outlook/tmo/ artificial-intelligence/worldwide.

greater than hundreds of millions of dollars to develop.[3] As such, maintaining the utmost secrecy in the development of AI models is of critical importance.

21. xAI's trajectory is unprecedented. It has delivered in a mere two years arguably the most advanced AI model in the world including features more innovative and imaginative than those offered by its competitors including OpenAI. xAI's innovation is protected by xAI's confidential information and trade secrets.

22. Trade secrets protect nearly all of xAI's developments—model weights, training data, tuning methods, system prompts, know-how, and more. With xAI's daily innovative advancements, its ability to rely on trade secrets protection is critical not only to its competitive position but for its ongoing operations and protection of its investments in its technology.

<u>Plaintiff xAI Protects its Confidential Information and Trade Secrets</u>

23. To maintain its competitive position, and protect its confidential and proprietary information, including its trade secrets, xAI has implemented a variety of industry standard—and industry leading—practices, such as: routinely conducting security awareness training for all employees; conducting background checks on employees and contractors who may access xAI data; conducting secure development and data handling training for employees with access to sensitive data, after which such employees must complete an assessment to demonstrate understanding; employing a team dedicated to information security; adopting the NIST 800-171 Rev.3 framework as a baseline for internal security standards; achieving SOC 2, Type II compliance; securing endpoints, including employee devices, with ongoing patch maintenance and full disk encryption; and maintaining a formal written information security policy, among other practices.

24. In addition, as a condition of employment, xAI requires each employee to enter into an Employee Confidential Information and Invention Assignment Agreement ("Agreement") of the form

[3] Katharina Buchholz, *The Extreme Cost Of Training AI Models*, Forbes (Aug. 23, 2024), https://www.forbes.com/sites/katharinabuchholz/2024/08/23/the-extreme-cost-of-training-ai-models/.

seen in **Exhibit A**. The Agreement imposes clear obligations on xAI employees regarding xAI's Confidential Information. The Agreement defines "Confidential Information" to mean "any and all confidential knowledge, data or information" belonging to xAI, including most relevantly here:

> (a) trade secrets, proprietary technology, inventions, mask works, ideas, processes, formulas, software in source or object code, data, programs, other works of authorship, know-how, improvements, discoveries, developments, designs and techniques, and any other work product of any nature and all Intellectual Property Rights (as defined below) therein (collectively, "Inventions"), including all Company Inventions (as defined below); [and]
>
> (g) any other non-public information that a competitor of Company could use to Company's competitive disadvantage. (**Ex. A** ¶ 1.2.)

25. Among other things, the Agreement:

a. Requires that the employee acknowledge that the employment "creates a relationship of confidence and trust" with respect to xAI's Confidential Information, which the company "has a protectable interest therein" (**Ex. A** ¶ 1.1);

b. Requires the employee to maintain confidentiality "during and after [the employee's] employment," and prohibits disclosure, use, or publication of Confidential Information unless required for the employee's work or expressly authorized by an officer of xAI (*id.* ¶ 1.1);

c. Requires the employee, upon termination, to return "any and all" materials containing or disclosing Confidential Information, including documents, notes, and devices, along with all copies, and "any other material containing or disclosing . . . Confidential Information." (*id.* ¶ 8);

d. Requires the employee to provide xAI with a computer-usable copy of any Confidential Information stored on personal devices or systems and to "permanently delete and expunge" such information from those systems (*id.* ¶ 8);

e. Requires the employee to "agree to provide [xAI] access to [the employee's] system as reasonably requested to verify that the necessary copying and/or deletion is completed" (*id.* ¶ 8); and

f. Requires the employee to "agree to: (a) provide [xAI] any and all information needed to access any [xAI] property or information returned or required to be returned . . . , including without limitation any login, password, and account information." (*id.* ¶ 8)

26. By signing the Agreement, employees agree that "any threatened or actual violation" of the Agreement would "constitute immediate and irreparable injury" to xAI. (*Id.* ¶ 9.) They also agree that xAI may remedy those violations with injunctive, specific performance or equitable relief without bond. (*Id.*)

27. By signing the Agreement, employees also agree that prior to leaving the company they will complete and sign the xAI's "termination statement if required to do so by [xAI]." (*Id.*)

28. By signing the termination statement ("Termination Certification") of the form seen in **Exhibit B**, employees verify that they have complied with all the Agreement's terms. (**Ex. B** at 1.) The Termination Certification also requires departing employees to certify that they have undertaken a diligent search for all xAI documents and returned them to the company. (*Id.*) It provides that "if [the employee has] used any personal computer, server, or e-mail system to receive, store, review, prepare or transmit any . . . Confidential Information, [the employee] agree[s] to provide Company with a computer-useable copy of all such Confidential Information and then permanently delete and expunge such Confidential Information from those systems." (*Id.*)[4] To ensure compliance, the Certification requires the employee to "agree to provide [xAI] access to [the employee's] system as reasonably requested to verify that the necessary copying and/or deletion is completed." (*Id.*)

[4] The Termination Certificate and Agreement share a common definition of the term "Confidential Information."

Defendant's Employment With xAI

29. Defendant is an accomplished researcher in the AI community. He earned a Ph.D. in Computer Science from Stanford University in 2024, and has authored numerous AI-related articles published in various scholarly journals.

30. On or about February 26, 2024, Defendant began working for xAI as a Member of the Technical Team. Defendant was among the company's initial group of approximately 20 engineers.

31. Defendant's responsibilities included developing and training Grok, xAI's advanced AI model. In this role, Defendant had access to and responsibility for components across the entirety of xAI's technology stack.

32. To support his job responsibilities, xAI granted Defendant restricted and controlled access to its confidential documents and proprietary information. xAI provided this access only for the purpose of enabling Defendant to perform his job duties.

33. As a condition for his employment and access to xAI's Confidential Information and trade secrets, xAI required Defendant to sign the Agreement, which he executed on February 26, 2024. **Exhibit A**.

34. xAI also awarded stock options and shares to Defendant as part of his compensation package.

35. To provide liquidity to its employee-stockholders like Defendant, xAI facilitated the purchase of some of Defendant's shares, for more than $4.7 million, in June 2025. Defendant received the cash proceeds of this sale on July 23, 2025.

36. Seeking additional liquidity, Defendant persuaded xAI to facilitate the purchase of more shares from him for an additional $2.2 million in July 2025. xAI facilitated this transaction for Defendant because xAI valued his contributions, and wanted to retain him as a productive and successful employee. Defendant received the cash proceeds of this sale on July 25, 2025.

37. All told, Defendant sold approximately $7 million of his company stock.

Defendant Stole xAI's Confidential Information and Trade Secrets

38. On July 25, 2025–the same day he concluded his second sale of equity and had millions in cash on hand–Defendant betrayed the trust and faith xAI had placed in him by willfully and maliciously copying xAI Confidential Information (as defined in the Agreement) and trade secrets from his xAI-issued laptop to one or more non-xAI physical or online storage systems within his personal control (collectively, "Personal System").

39. The trade secrets Defendant willfully and maliciously misappropriated include without limitation cutting-edge AI technologies with features superior to those offered by ChatGPT and other competing products.

40. The trade secrets Defendant willfully and maliciously misappropriated could be weaponized by competitors such as OpenAI to, at a minimum, improve competing products such as ChatGPT with xAI's more innovative AI and imaginative features which make Grok one of the most, if not the most, intelligent AI models, undermine xAI's product roadmap, and disrupt its market expansion strategy.

41. The trade secrets Defendant willfully and maliciously misappropriated could save OpenAI and other competitors billions in R&D dollars and years of engineering effort, handing any competitor a potential overwhelming edge in the race to dominate the AI landscape.

42. Defendant took extensive measures to conceal his misconduct. He deleted his browser history and system logs, renamed files, and compressed files prior to uploading them to his Personal System.

43. ***These facts are beyond dispute, as Defendant, with his attorney present, admitted in a handwritten document he provided to xAI that he misappropriated xAI's Confidential Information and trade secrets, and again, with his attorney present, admitted verbally during in-person meetings with xAI that he engaged in such misappropriation and further admitted that he tried to hide his theft.***

44. These misappropriated Confidential Information and trade secrets have independent economic value in the AI market. The data could be used by xAI's competitors, such as OpenAI, and/or foreign entities to preempt xAI's product offerings and market expansions, and understand and use its current and in-development product features to strengthen their own AI models, thus giving any competitor or entities with access to the data a potentially insurmountable competitive advantage in the AI race.

45. xAI has invested billions of dollars in developing its intellectual property, including the Confidential Information and trade secrets stolen by Defendant.

46. Defendant had no legitimate reason to copy the company's data to his Personal System.

Defendant's Departure From xAI

47. On July 28, 2025, three days after uploading xAI's data to his Personal System and selling approximately $7 million of his company stock, Defendant suddenly resigned.

48. Prior to his resignation, Defendant had accepted an offer to join xAI's direct competitor OpenAI with a start date of August 19, 2025.

49. As part of his offboarding process with xAI, Defendant signed a Termination Certificate on his last day of work, August 1, 2025. A true and correct copy of the Termination Certificate is attached hereto as **Exhibit B**.

50. In the Termination Certificate, Defendant represented that he had complied with all terms of the Agreement, which necessarily included his obligations to preserve the confidentiality and security of xAI's Confidential Information, and his obligation to return any xAI Confidential Information in his possession, and his obligation to destroy any xAI Confidential Information he had uploaded or copied to another storage service. (**Ex. B** at 1.)

51. Defendant also represented in the Termination Certificate that he had returned all xAI documents, "including but not limited to Company files, notes, drawings, records, plans, forecasts, reports, studies, analyses, proposals, agreements, financial information, research and development information,

sales and marketing information, customer lists, prospect information, pipeline reports, sales reports, operational and personnel information, specifications, code, software, databases [and] computer-recorded information." (**Ex. B** at 1.)

52. He also represented that he had "made a diligent search to locate any such documents, property and information" and reiterated his false promise to return and delete any such data, which would include the files he had uploaded to his Personal System. (**Ex. B** at 1.)

53. These representations were each knowingly false. Defendant not only knew he had not returned or destroyed xAI's documents, property, and information in his possession, but he brazenly absconded with xAI's Confidential Information and trade secrets by downloading them onto his Personal System.

54. Defendant did not just misrepresent his past compliance in the Termination Certificate. He also falsely promised to protect xAI's Confidential Information going forward while at the same time absconding with the same. He falsely promised to "hold in confidence and [] not disclose, use or publish any of the Company's Confidential Information." (**Ex. B** at 1.)

55. He also broke his promise in the Termination Certificate that if he had "used any personal computer, server, or e-mail system to receive, store, review, prepare or transmit any [xAI] information, including but not limited to, Confidential Information, [he would] provide [xAI] with a computer-useable copy of all such Confidential Information and then permanently delete and expunge such Confidential Information from those systems."

56. And he also broke his promise to provide xAI with "access to [his] system as reasonably requested to verify that the necessary copying and/or deletion is completed." (**Ex. B** at 1.)

57. Defendant never honored these faithless commitments, but used them to lull xAI into a false sense of security, to give him the opportunity to conceal that he had stolen xAI's Confidential Information.

58. Specifically, when Defendant signed the Termination Certificate, he (1) retained xAI's Confidential Information on his Personal System while engaged in discussions to join Chat GPT maker OpenAI, xAI's competitor and (2) never deleted the Confidential Information or made his complete Personal System available to xAI.

59. Defendant made the false promises in the Termination Certificate, intentionally deceiving and defrauding xAI, and induced xAI to permit his departure without any further investigation into his conduct or taking additional steps to protect its Confidential Information, all as part of his plan to violate his obligations to his employer and then cover his tracks.

60. Defendant's fraudulent scheme worked. Because of the faith and trust Defendant had nurtured as one of xAI's first employees, xAI reasonably relied on Defendant's representations in the Termination Certificate.

61. xAI has suffered and will continue to suffer injury because of Defendant's actions, including diminished value of its Trade Secrets, loss of its competitive advantage, loss of business and harm to its reputation and goodwill.

xAI Discovers Defendant's Theft of its Confidential Information

62. Defendant took affirmative steps to conceal his exfiltration of data, xAI discovered Defendant's theft of its Confidential Information and trade secrets on August 11, 2025 during a routine review of logs from security software designed to detect and prevent data exfiltration.

63. That same day, xAI sent a demand letter by email to Defendant regarding his theft of the company's data. The letter advised Defendant that xAI had learned that Defendant had "exfiltrated xAI confidential data" to his Personal System in violation of xAI's "policies and practices, constituting a flagrant violation of his legal and contractual obligations to xAI."

64. xAI's letter demanded the return and deletion of the data. It also requested that Defendant provide a detailed written description of misappropriated data, a copy of any data still on his Personal System and access to his Personal System. The letter also requested written confirmation as to whether

Defendant made any unauthorized disclosure or use of xAI's confidential, proprietary or trade secret information, and if so, details of that use or disclosure.

65. Instead of immediately providing the requested information, Defendant retained criminal defense counsel, and then had his criminal attorney with him to meet with xAI in an attempt to talk his way out of facing consequences for his theft.

66. In that in-person meeting on August 14, 2025 and a subsequent in-person meeting on August 15, 2025, both at the at the offices of Winston & Strawn, LLP at 255 Shoreline Drive, Suite 520, Redwood City, CA 94065, Defendant, in the presence of his criminal defense counsel, admitted to intentionally taking xAI's files and covering his tracks by deleting his system logs, renaming files, and compressing them prior to uploading them. He also admitted to understanding the gravity of his actions. He also provided a handwritten statement with these admissions.

67. Through multiple days of negotiations from August 14, 2025, through August 18, 2025, Defendant – fully represented by criminal defense and also employment counsel – engaged in more false assurances, fraud and deceit.

68. After two in-person negotiations on Thursday and Friday, August 14-15, 2025, and further negotiations over the weekend, during a portion of which time Defendant allowed xAI to hold (but not access) two of his personal laptops and his personal cell phone "as a showing of good faith," on Monday, August 18, 2025, Defendant yet again fraudulently entered into a contract with xAI, this time the "Authorization for Access to Accounts and Personal Devices" ("Authorization").

69. In that Authorization, Defendant authorized a "forensic investigator or expert firm(s) retained by x.AI and/or Winston & Strawn (the "Expert"), to create a forensic image or copy of the Data in [Defendant's] Account and on [Defendant's] Devices for the purposes of investigating [Defendant's] access, possession, and/or transmission of xAI information, including Relevant Data." The Authorization defined "Relevant Data" as: "(i) Confidential Information as defined in the Employee Confidential Information and Invention Assignment Agreement executed on February 26, 2024 and (ii) any

communications, correspondence, notes, data, records, files, or documents–regardless of form or medium–relating to xAI, xAI competitors, artificial intelligence ("AI"), large language models ("LLMs"), or generally within [Defendant's] field of work that does not otherwise constitute Confidential Information." "Data" was broadly defined as "all information residing or stored on Account or Devices, and any files or forensic artifacts located in or on the Account, or on a Device, regardless of file type, content or format of the information, and includes Relevant Data, Personal Data and any information derived from or related to such data, including but not limited to metadata, logs, system-generated attributes, and any other embedded or associated informational elements." And the "Account" was defined to include all of Li's other online account(s) associated with Xuechen Li, including accounts associated with each of" several specified "email addresses of Xuechen Li" and "associated services."

70. The Authorization also provided that Li "understand[s] and agree[s] that, in connection with the purposes set forth in this authorization, xAI will search the Data, Account and Devices to locate xAI information, including Relevant Data, and evidence of access, possession and/or transmission of xAI information."

71. The Authorization also provided that if xAI found its Confidential Information on any of the Defendant's devices or in any of the Defendant's accounts, xAI would be "authorize[d] . . . to delete that Confidential Information from the Account and/or Devices."

72. In the Authorization, Defendant represented that he was providing "passwords, credentials, keys, MultiFactor Authentication information, and other information necessary to fully Access [his]Accounts, Devices, and files," which he agreed that he would "not modify until September 15, 2025 (or such date upon which xAI has completed all forensic images [], if later)." "Access" was defined broadly to include: "any access of any kind, including: (i) reading, viewing, editing, examining; (ii) copying (including making a forensic copy); (iii) disclosing, transmitting or distributing (but only to the extent necessary to effectuate the purpose of this Agreement and subject to any restrictions specified herein); or (iv) executing."

73. In reliance on Defendant's execution of the Authorization and appearance of cooperation, xAI refrained at that time from filing this suit and seeking other emergency relief.

74. After Defendant returned the signed Authorization, xAI discovered that the credentials Defendant provided in the Authorization did not include the password (which had been changed by Defendant on August 11, 2025, after he received the demand letter from xAI) for the critical account to which Defendant uploaded xAI's Confidential Information and Trade Secrets, thwarting the very purpose of the Authorization, which was to allow xAI to "investigat[e] [Defendant's] access, possession, and/or transmission of xAI information, including Relevant Data."

75. While conducting a forensic analysis of the information that could be accessed on Li's personal devices provided to xAI, xAI also discovered that Defendant had a number of other accounts that he did not even disclose, let alone provide passwords for, including accounts to which he uploaded xAI material. This included other accounts with xAI information, including potentially Confidential Information.

76. After xAI confronted Defendant about these omitted accounts and credentials, Defendant's counsel merely responded that Defendant did not "remember" the password for the critical account that he had changed only seven days earlier and similarly did not "remember" the other accounts, even though he had used them recently.

77. Given Defendant's continued fraud and deceit, xAI had no choice but to urgently bring this action to protect its proprietary interests in the Confidential Information and trade secrets misappropriated by Defendant.

FIRST CAUSE OF ACTION

(Breach of Contract: Employee Confidential Information and Invention Assignment Agreement)

78. xAI realleges and incorporates by reference Paragraphs 1 through 77 as though fully set forth herein.

79. Defendant entered into the Agreement with xAI on or about February 26, 2024.

80. The Agreement is a valid and enforceable contract, intended to protect xAI's legitimate business interests, including protection of its proprietary, confidential and trade secret information.

81. xAI hired Defendant and provided him with employment and compensation, in exchange for his execution of the Agreement.

82. Consistent with the Agreement's terms, xAI also granted Defendant access to its Confidential Information to enable him to perform his job duties at xAI.

83. By executing the Agreement, Defendant agreed to (a) preserve the security and confidentiality of xAI's Confidential Information, (b) not use or disclose the Confidential Information, except as authorized in the Agreement, (c) return all Confidential Information in his possession at the end of his employment and (d) delete any copies of the Confidential Information he copied to personal storage accounts during his employment. (Ex. A ¶¶ 1.1, 8.)

84. xAI has fully performed its contractual obligations to Defendant under the Agreement.

85. Defendant breached the Agreement by, among other things, (a) uploading xAI's Confidential Information to his Personal System just three days before announcing his resignation, (b) falsely representing that he had deleted any copies of xAI's Confidential Information when he departed the company, and then (c) refusing to return that Confidential Information to xAI and delete all copies of it upon his departure from xAI.

86. xAI has suffered and will continue to suffer injury because of Defendant's breach of the Agreement, including diminished value of its Confidential Information, loss of its competitive advantage, loss of business, and harm to its reputation and goodwill.

87. Defendant's breach has caused and will continue to cause immediate and irreparable harm to xAI. Given the nature of the breach and the difficulty in quantifying the competitive and economic impact of Defendant's actions, monetary damages alone would be inadequate, and the full extent of harm may be impossible to assess. Defendant's actions will continue to cause irreparable harm to xAI if not enjoined.

88. As Defendant acknowledged when he signed the Agreement, his breach has caused and will cause immediate and irreparable injury to xAI, and it may be impossible to assess the damages caused by that breach. Defendant thus agreed that xAI will have the right to enforce the Agreement's terms by injunction, specific performance, or other equitable relief without bond, without prejudice to other rights and remedies available to xAI.

89. The burden on Defendant of issuing an injunction would be slight compared to the ongoing injury xAI would suffer if injunctive relief is not granted. And granting an injunction will serve, rather than harm, the public interest, including by protecting innovation, competition, and lawful business practices.

SECOND CAUSE OF ACTION

(Breach of Contract: Termination Certification)

90. xAI realleges and incorporates by reference Paragraphs 1 through 89 as though fully set forth herein.

91. Defendant signed the Termination Certification on August 1, 2025.

92. The Termination Certification is a valid and enforceable contract.

93. xAI hired Defendant and provided him with employment and compensation, in exchange for him agreeing to sign the Termination Certification.

94. xAI has fully performed its contractual obligations to Defendant under the Termination Certification.

95. By executing the Termination Certificate, Defendant agreed to comply with all of the terms of the Agreement, return all of xAI's documents and data (and all copies thereof), and represented that Defendant will not disclose, use, or publish any of xAI's Confidential Information. Again, the Termination Certification was intended to protect xAI's legitimate business interests, including protection of its proprietary, confidential, and trade secret information.

96. Defendant breached the Termination Certification by, among other things, (a) uploading a copy of data containing xAI's Confidential Information to his Personal System three days before announcing his resignation, (b) falsely representing that he had deleted any copies of xAI's Confidential Information when he departed the company, and then (c) refusing to return that Confidential Information to xAI and delete all copies of it upon his departure from xAI.

97. xAI has suffered and will continue to suffer injury because of Defendant's breach of the Termination Certification, including diminished value of its Confidential Information, loss of its competitive advantage, loss of business, and harm to its reputation and goodwill.

98. Defendant's breach has caused and will continue to cause immediate and irreparable harm to xAI. Given the nature of the breach and the difficulty in quantifying the competitive and economic impact of Defendant's actions, monetary damages alone would be inadequate, and the full extent of harm may be impossible to assess. Defendant's actions will continue to cause irreparable harm to xAI if not enjoined.

99. The burden on Defendant of issuing an injunction would be slight compared to the ongoing injury xAI would suffer if injunctive relief is not granted. And granting an injunction will serve, rather than harm, the public interest, including by protecting innovation, competition and lawful business practices.

THIRD CAUSE OF ACTION

(Trade Secrets Misappropriation, 18 U.S.C. § 1836 *et seq*.)

100. xAI realleges and incorporates by reference Paragraphs 1 through 99 as though fully set forth herein.

101. The Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq*., ("DTSA") allows an "owner of a trade secret that is misappropriated" to "bring a civil action [if] the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1).

102. The DTSA defines a trade secret to include "all forms and types of financial, business, scientific, technical, economic, or engineering information" that "(A) the owner thereof has taken reasonable measures to keep ... secret; and (B) ... derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3).

103. The DTSA defines misappropriation to include "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means" and "disclosure or use of a trade secret of another without express or implied consent by a person" who "used improper means to acquire knowledge of the trade secret." 18 U.S.C. § 1839(5). "Improper means" include theft, misrepresentation, and "breach of a duty to maintain secrecy." 18 U.S.C. § 1839(6).

104. The DTSA permits the Court to grant an injunction "to prevent any actual or threatened misappropriation" of the plaintiff's trade secrets, among other remedies. 18 U.S.C. § 1836(b)(3).

105. xAI dedicated and continues to dedicate substantial time and resources towards developing its trade secrets, as detailed above.

106. As described above, at all relevant times, xAI has made reasonable efforts to ensure its trade secrets remain confidential, proprietary, secret, and available for xAI's commercial use only.

107. In his role on xAI's engineering team, Defendant had access to and knowledge of xAI's trade secrets.

108. Defendant acknowledged that he had a duty to maintain the secrecy of xAI's trade secrets in the Agreement.

109. Despite this, Defendant misappropriated xAI's trade secrets by among other things, (a) uploading a copy of data containing xAI's trade secrets to his Personal System three days before his termination, (b) falsely representing that he had deleted any copies of xAI's trade secrets when he departed the company, and then (c) refusing to return those trade secrets to xAI and delete all copies of it upon his departure from xAI.

110. The xAI trade secrets Defendant misappropriated included without limitation cutting-edge AI technologies with features superior to those offered by ChatGPT and other competing products. Defendant had no legitimate reason to copy the company's data to his Personal System. xAI continues to investigate the full extent of Defendant's misappropriation.

111. This conduct amounted to misappropriation because Defendant acquired xAI's trade secrets by improper means: theft, misrepresentation, and breach of his duty to maintain their secrecy.

112. The trade secrets Defendant took relate to Grok, xAI's advanced AI model. xAI customers, including customers located throughout the U.S. states, access Grok through the internet, including by using web browsers (grok.com), mobile phone apps, and by API access. Internet traffic serving some of these customers crosses state boundaries. Grok is thus a product or service used or intended for use in interstate commerce.

113. The trade secrets identified above and others almost certainly contained on Defendant's Personal System have independent economic value in the AI market. The trade secrets Defendant misappropriated are the result of the culmination of billions of dollars of investment and multiple years of AI development and training.

114. The trade secrets Defendant misappropriated could be weaponized by competitors such as OpenAI to, at a minimum, improve competing products such as ChatGPT with Grok's more innovative

and imaginative features which make Grok one of the most, if not the most, intelligent generative AI chatbots, undermine xAI's product roadmap, and disrupt its market expansion strategy.

115. The trade secrets Defendant misappropriated could save OpenAI and other competitors billions in R&D dollars and years of engineering effort, handing any competitor a potential overwhelming edge in the race to dominate the AI landscape.

116. xAI has suffered and will continue to suffer injury because of Defendant's misappropriation of trade secrets, including diminished value of its Trade Secrets, loss of its competitive advantage, loss of business, and harm to its reputation and goodwill.

117. xAI has no adequate remedy at law for such present and future harm and is thus entitled to injunctive relief in addition to compensatory relief.

118. Defendant's breach has caused and will continue to cause immediate and irreparable harm to xAI. Given the nature of the breach and the difficulty in quantifying the competitive and economic impact of Defendant's actions, monetary damages alone would be inadequate, and the full extent of harm may be impossible to assess. Defendant's actions will continue to cause irreparable harm to xAI if not enjoined.

119. Additionally, because Defendant has committed the acts alleged herein willfully, in bad faith, from an improper motive amounting to malice, and in conscious disregard of xAI's rights, xAI is entitled to recover punitive damages from Defendant, in an amount according to proof at trial.

FOURTH CAUSE OF ACTION

(Violation of Comprehensive Computer Data Access and Fraud Act)

120. xAI realleges and incorporates by reference Paragraphs 1 through 119 as though fully set forth herein.

121. California Penal Code § 502(e) provides a civil remedy against anyone who, in violation of California Penal Code § 502(c)(2), "[k]nowingly accesses and without permission takes, copies, or

makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network."

122. Defendant knowingly accessed and without xAI's permission took, copied, and made use of xAI's data from its computer by among other things, (a) uploading a copy of data containing xAI's data to his Personal System three days before his termination, (b) falsely representing that he had deleted any copies of xAI's data when he departed the company, and then (c) refusing to return that data to xAI and delete all copies of it upon his departure from xAI.

123. As a direct and proximate result of his violation of California Penal Code § 502(c)(2), Defendant caused loss to xAI.

124. xAI has no adequate remedy at law for such present and future harm and thus is entitled to injunctive relief in addition to compensatory relief under California Penal Code § 502(e).

125. Defendant's actions will continue to cause irreparable harm to xAI if not enjoined.

126. Additionally, because Defendant has committed the acts alleged herein willfully, in bad faith, maliciously, and in conscious disregard of xAI's rights, xAI is entitled to recover punitive damages from Defendant, in an amount according to proof at trial

127. xAI is also entitled to recover its attorneys' fees pursuant to California Penal Code § 502(e)(2).

FIFTH CAUSE OF ACTION

(Fraud: Termination Certificate)

128. xAI realleges and incorporates by reference Paragraphs 1 through 127 as though fully set forth herein.

129. In executing the Termination Certificate, Defendant falsely represented the material fact that he had "complied with all the terms" of the Agreement, which necessarily included the Agreement's

obligation that he "[a]t all times during and after [his] employment … hold in confidence and … not disclose, use, or publish any of [AI's] Confidential Information." (**Ex. B** at 1 (incorporating **Ex. A** at § 1.1).)

130. He also falsely represented in the Termination Certificate the material fact that he had returned all xAI documents, "including but not limited to [xAI] files, notes, drawings, records, plans, forecasts, reports, studies, analyses, proposals, agreements, financial information, research and development information, sales and marketing information, customer lists, prospect information, pipeline reports, sales reports, operational and personnel information, specifications, code, software, databases [and] computer-recorded information." (**Ex. B** at 1.)

131. He also falsely represented the material fact that he had "made a diligent search to locate any such documents, property and information" and reiterated his promise to return and delete any such data, which would include the files he had uploaded to his Personal System. (**Ex. B** at 1.)

132. Each of Defendant's representations in the certification was knowingly false. Defendant knew he had not returned or destroyed xAI's documents, property, and information in his possession. He instead retained xAI's documents, property and information—including xAI's Confidential Information and trade secrets—on his Personal System. Defendant thus also knew that he had not held xAI's data in confidence but instead had misappropriated it for his own use.

133. Defendant also falsely promised in the Termination Certification that if he had "used any personal computer, server, or e-mail system to receive, store, review, prepare or transmit any [xAI] information, including but not limited to, Confidential Information, [he would] agree to provide [xAI] with a computer-useable copy of all such Confidential Information and then permanently delete and expunge such Confidential Information from those systems."

134. He also agreed to provide xAI with "access to my system as reasonably requested to verify that the necessary copying and/or deletion is completed." (**Ex. B** at 1.)

135. Defendant also repeated his prior promise to "hold in confidence and [] not disclose, use or publish any of [xAI's] Confidential Information" after he left xAI. (**Ex. B** at 1.)

136. Defendant knowingly made these promises falsely with no intent to honor them. Instead, he intended to retain and did retain xAI's Confidential Information on his Personal System, with the intent to use, disclose, and/or publish it. He never intended to delete and did not delete xAI's Confidential Information. And he never intended to provide xAI with access to his Personal System. He instead intended to conceal and did conceal his Personal System from xAI, in order to prevent xAI from discovering his misconduct.

137. Defendant made the knowingly false representations in the Termination Certificate with the intent to deceive and/or defraud xAI and conceal his theft of Confidential Information, and to induce xAI to permit his departure without any further investigation into his conduct or taking additional steps to protect its Confidential Information.

138. xAI reasonably relied on Defendant's representations in the Termination Certificate by refraining from investigating him as an active threat.

139. As a result, Defendant was able to perpetuate and conceal his misappropriation, damaging xAI in an amount to be proven at trial.

140. Defendant's actions will continue to cause irreparable harm to xAI if not enjoined.

141. xAI has no adequate remedy at law for such present and future harm and is thus entitled to injunctive relief in addition to compensatory relief.

142. Defendant performed the foregoing acts, conduct, and omissions fraudulently, oppressively, and maliciously, with the intent and design to damage xAI. By reason of this conduct, xAI is thus entitled to recover punitive damages in an amount to be determined.

PRAYER FOR RELIEF

xAI prays for the following relief:

1. a Temporary Restraining Order against Defendant ordering him to, within three business days of the execution of this Order,
   a. temporarily surrender control and access (for a period of 14 days to allow for a forensic examination to identify, remediate, and/or delete Confidential Information belonging to xAI) to any personal electronic devices (e.g., cellular devices, computers), online storage repositories (e.g., Gmail, Google Drive, iCloud), or other electronic storage devices that are currently accessible by Defendant or in Defendant's possession, custody, or control;
   b. return to xAI, through its counsel of record, all Confidential Information belonging to xAI currently in Defendant's possession, custody, or control, that exists in any physical form (e.g., notepad, paper files);
   c. provide a written statement identifying all personal locations, personal devices, personal accounts, or personal storage media–whether physical or electronic–where any Confidential Information belonging to xAI is or has been stored, maintained, or accessed;
   d. provide, and not modify for the 14-day period referenced in (A) above, the passwords, credentials, keys, MultiFactor Authentication information, and other information necessary to fully access all devices, repositories, storage media, and accounts listed in (A); and
   e. for any password or credentials listed in relation to (A) which Defendant claims he has forgotten or is unsure how to readily access, cooperate and work with xAI to reset or recover the same and/or to otherwise cooperate with xAI as necessary to provide xAI access to such accounts and devices listed in (A).
2. a Temporary Restraining Order, Preliminary Injunction, and Permanent Injunction enjoining Defendant, his agents, employees, partners, and any others acting in concert with him or on his behalf, from:
   a. Controlling, logging into, or otherwise accessing (other than as required by 1(E) above) any personal electronic devices (e.g., cellular devices, computers), online storage

repositories (e.g., Gmail, Google Drive, iCloud), or other electronic storage devices that are currently accessible by Defendant or in Defendant's possession, custody, or control;

b. Possessing, using, copying, reproducing, disclosing, transferring (including to a third party), disseminating, or otherwise exploiting, any Confidential Information, including the xAI files uploaded to his Personal System, and any copies, derivatives, or materials created therefrom;

c. Destroying, deleting, changing, altering, or otherwise eliminating any version (whether hard copy, native, or electronic) of any documents or electronically stored information on any device or in any account (whether in printed form or downloaded to any remote storage system, computer, hard drive, server, disk drive, flash drive, cellular telephone, CD, DVD, USB drive, or any other device that can be used to electronically store data or information) relating to the Confidential Information;

d. Disposing of, deleting, changing, altering, wiping, tampering with, or destroying any remote storage systems (including cloud storage accounts), computers, hard drives, servers, disk drives, flash drives, cellular telephones, CDs, DVDs, USB drives, and any other devices that can be used to electronically store data or information that are: (a) currently accessible by Defendant or in Defendant's possession, custody, or control; or (b) have been accessible by Defendant or in Defendant's possession, custody, or control, since February 26, 2024, and any data, files, information, forensic remnants or digital artifacts, stored on or within the device;

e. Destroying, deleting, changing, altering, or otherwise eliminating any emails to or from any email accounts used by Defendant since February 26, 2024, either in printed form or downloaded to any computers, laptops, online storage repositories, cloud storage, or electronic storage devices;

f. Destroying, deleting, changing, altering, or otherwise eliminating any text, electronic postings, or other application messages from any cellular telephones or devices, computers, laptops, online storage repositories, cloud storage, or electronic storage devices (a) currently accessible by Defendant or in Defendant's possession, custody, or control; or (b) have been accessible by Defendant, or in Defendant's possession, custody, or control, since February 26, 2024; and

g. Violating, aiding, or participating in the violation of any terms of the Agreement or Termination Certification;

3. a Temporary Restraining Order and Preliminary Injunction enjoining Defendant from having any role or responsibility at OpenAI or any other competitor of xAI pertaining to generative AI, including without limitation OpenAI's ChatGPT until xAI has confirmed that all of xAI's Confidential Information in Li's possession, custody, or control has been deleted;
4. a Temporary Restraining Order and Preliminary Injunction enjoining Defendant from having any communication on the subject of generative AI with any officer, director, employee, agent, supplier, consultant, or customer of OpenAI or any other competitor of xAI until xAI has confirmed that all of xAI's Confidential Information in Li's possession, custody, or control has been deleted;
5. actual, compensatory, treble, punitive, and exemplary damages to be determined at trial;
6. attorneys' fees and costs; and
7. such other and further relief the Court deems as just.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Complaint.

Dated: August 28, 2025

WINSTON & STRAWN LLP

By: */s/ Kathi Vidal*
KATHI VIDAL
ALEXANDER COTE
CARSON SWOPE

Attorneys for Plaintiffs X.AI Corp. and X.AI LLC