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.

Plaintiff xAI Protects its Confidential Information and Trade Secrets

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