CHRISTOPHER FROST (SBN 200336)
chris@frostllp.com
KEVIN S. DICKER (SBN 179315)
kevin@frostllp.com
FROST LLP
10960 Wilshire Boulevard, Suite 2100
Los Angeles, California 90024
Telephone: (424) 254-0441
Facsimile: (424) 600-8504

Attorneys for *Plaintiff and the Proposed Class*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

GUBER GLOBAL LLC, SOPHIA ALIAGA, SAMER TALLAUZE, and BRENNON LEWIS JR., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

NOTION LABS, INC., REPLIT, INC., FIREWORKS.AI, INC., and UBER TECHNOLOGIES, INC.,

Defendants.

Case No. 3:26-cv-14010

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE AGAINST FIREWORKS;**
2. **NEGLIGENCE AGAINST NOTION;**
3. **NEGLIGENCE AGAINST REPLIT;**
4. **NEGLIGENCE AGAINST UBER.**

JURY TRIAL DEMANDED

Plaintiffs GUBER Global LLC ("GUBER"), Sophia Aliaga ("Aliaga"), Samer Tallauze ("Tallauze"), and Brennon Lewis Jr. (“Lewis”), individually and on behalf of the classes defined below, allege the following against Defendants Notion Labs, Inc. ("Notion"), Replit, Inc. ("Replit"), Fireworks.ai, Inc. ("Fireworks"), and Uber Technologies, Inc. ("Uber"). Plaintiffs allege matters concerning their own conduct and experiences on personal knowledge and other matters on information and belief, based on counsel's investigation, the notices provided to GUBER and Aliaga, Uber's formal notices and regulatory disclosures, Defendants' public statements, and the other sources identified below. Further evidentiary support for matters within Defendants' possession is expected after a reasonable opportunity for discovery.

I. NATURE OF THE ACTION

1. This action concerns the loss of confidentiality of information entrusted to three widely used platforms and exposed through their common infrastructure provider or credentials entrusted to that provider. GUBER used Replit to develop commercial technology. Aliaga used Notion for university-related activities and startup development. Both platforms sent customer information to Fireworks and later notified GUBER and Aliaga that their account information was affected. On information and belief, the Uber records accessed through compromised Fireworks credentials included Tallauze's and Lewis’ driver’s license and extracted text data, including at least their names, addresses, dates of birth, and driver’s license numbers.

2. The information at issue includes private educational information, unreleased software-development material, proprietary technical designs, confidential business workflows, and sensitive government-issued identification records. An AI conversation can contain confidential information in the prompt, the response, or related session material. Removing an account label does not remove confidential facts appearing in the text, restore the secrecy of a technical design, or prevent the text from identifying its subject through context. A driver's-license image and extracted identifying fields present a separate, directly identifying category of nonpublic information.

3. Fireworks occupied the common position in this arrangement. Notion, Replit, and Uber offered the services with which the affected people and businesses interacted; Fireworks supplied infrastructure or received access authority for work supporting those services. These relationships form the hub-and-spoke structure relevant to this action: separate customer-facing businesses entrusted information or processing access to the same infrastructure provider. Each Defendant retained responsibility for the systems, access, and data-handling decisions within its own control.

4. The Notion spoke presents a particularly concrete discrepancy between an agreed safeguard and actual handling. Notion now reports that Fireworks made a contractual zero-retention commitment for Notion's use of its platform, yet Notion's investigation found that the Fireworks endpoints it used had retained data. That admission directly concerns why a downstream copy of customer content existed to be compromised.[1]

5. GUBER's and Aliaga's connections to the incident are account specific. Replit told GUBER that its account was affected and identified prompts from July 14 through July 29, 2026, together with related session data. Notion identified Aliaga's workspace and made affected-content records available to her. Aliaga reviewed records identifying 151 messages in seven conversation threads, with content dated October 5 through October 23, 2026. Tallauze's and Lewis' separate allegations concern the sensitive identification records described in Uber's formal disclosures.

6. The dates when Plaintiffs created their content are different from the dates of unauthorized access. Fireworks disclosed an initial credential incident in early October and later activity involving research-and-development machines on October 24. The precise path by which each Plaintiff's data was obtained, and the relationship between retained copies and the compromised systems, are matters primarily documented in Defendants' records.

7. Fireworks controlled its credentials, internal access paths, processing environments, and storage. Notion and Replit controlled their respective customer relationships,

[1] Notion, *Notice About the Fireworks AI Incident That May Impact Some Notion Workspaces*, https://www.notion.com/help/security-incident-involving-a-third-party-ai-vendor (last visited Nov. 17, 2026) (FAQs concerning retention and instructions for affected-content review).

the information they supplied to Fireworks, the purposes for which they supplied it, and their own vendor-selection and oversight practices. Uber controlled the storage environment and access arrangements it established for the provider's work. Plaintiffs lacked equivalent access to those systems and could not themselves inspect or correct the provider-side conditions that exposed their information.

8. Plaintiffs seek relief for their own injuries and those of the four classes defined below: the Fireworks Class, the Notion Class, the Replit Class, and the Uber Class. GUBER asserts its claims against Replit and Fireworks; Aliaga asserts hers against Notion and Fireworks; and Tallauze and Lewis asserts theirs against Uber and Fireworks. The Fireworks Class encompasses affected information received through any customer or intermediary, as well as information supplied directly to Fireworks or reached through compromised Fireworks credentials. The platform classes encompass affected users and other persons or entities whose information was contained in the compromised platform data.

9. The claims address each Defendant's own custody, transmission, retention, access controls, and security of nonpublic information. They rest on duties imposed by law in handling that information, not on a claim to enforce a subscription agreement or to obtain third-party-beneficiary rights under a vendor contract. Processing instructions and public security statements are relevant to the purposes, risks, and operational choices known to Defendants.

II. PARTIES

10. Plaintiff GUBER Global LLC is a limited liability company organized under Delaware law on December 30, 2025. It develops commercial AI technology and related applications. It maintains a mailing address in North Carolina. GUBER brings this action through its authorized representative, founder Dimetris Bowden, solely for the company's own rights and injuries.

11. GUBER used Replit in its commercial development work during July 2026. Its relevant information included nonpublic technical designs, development material, and business workflows. Replit's November 10, 2026 security notice identified the account used for that work as affected by the Fireworks incident.

12. Plaintiff Sophia Aliaga is a citizen of Nebraska and was a university student during the relevant period. She maintained a Notion account, upgraded to a paid Business subscription in August 2026, and used the service for academic activities and software-development work, including a startup project.

13. Plaintiff Samer Tallauze is an individual who maintains a United States mailing address in Austin, Texas. On information and belief, Uber held his nonpublic driver's-license image and related identifying information among the records accessed in the incident described below. Tallauze brings claims against Uber and Fireworks for the exposure of his own information.

14. Plaintiff Brennon Lewis Jr. is an individual domiciled in Angleton, Texas. Plaintiff Lewis received a notice letter from Defendant Uber dated November 10, 2026, informing him that his Private Information, including at least an image of his driver's license and text data that included his name, address, date of birth, and driver's license number, was impacted in the Breach. *See* **Exhibit 1.**

15. Defendant Notion Labs, Inc. is a Delaware corporation with its principal place of business and headquarters located at 685 Market Street, San Francisco, California 94105. Notion supplies a workspace platform, calendar products, and AI features, including the Notion AI service Aliaga used. Notion selects and contracts with providers that process information in connection with those features.[2] Notion's registered agent is CT Corporation System, which can be served at 330 N Brand Boulevard, Suite 700, Glendale, California 91203.

16. Defendant Replit, Inc. is a Delaware corporation with its principal place of business and headquarters located at 1001 E Hillsdale Boulevard, 400W, Foster City, California 94404. Replit supplies a platform for building and operating software, including an AI agent that receives development instructions and produces or interacts with code and other project material.[3]

[2] Notion Labs, Inc., *Notice of Exempt Offering of Securities (Form D)* (Oct. 12, 2021), https://www.sec.gov/Archives/edgar/data/1781814/000178181421000002/xslFormDX01/primary_doc.xml; Notion, *Privacy Policy*, https://www.notion.com/trust/privacy-policy (last visited Nov. 13, 2026).

[3] Replit, Inc., *Simple Agreement for Future Equity* 1 (2022), https://www.sec.gov/Archives/edgar/data/1920974/000167025422000289/document_4.pdf; Replit, *Replit Closes $250 Million in Funding to Build on Customer Momentum* (Sept. 10, 2025), https://replit.com/news/funding-announcement-series-c.

Replit's registered agent is Robert Kohse, who can be served at 1001 E Hillsdale Boulevard, 400W, Foster City, California 94404.

17. Defendant Fireworks.ai, Inc., doing business as Fireworks AI, is a Delaware corporation with its principal place of business and headquarters located at 900 Concar Drive, San Mateo, California 94402. Its own privacy notice identifies the operating entity as Fireworks.ai, Inc. Fireworks provides AI inference, training, and related infrastructure to business customers, including Notion and Replit. Uber has also identified Fireworks as the provider involved in its incident, as alleged below.[4] Firework's registered agent is National Registered Agents, Inc., which can be served at 330 N Brand Boulevard, Suite 700, Glendale, California 91203.

18. Defendant Uber Technologies, Inc. is a Delaware corporation with its principal place of business and headquarters located at 1725 3rd Street, San Francisco, California 94158. Uber operates a technology platform connecting users with transportation and other services. Its principal executive offices are located at 1725 3rd Street, San Francisco, California 94158. Uber selected the service-provider relationship and created the cloud environment described below for work involving Uber information.[5] Uber's registered agent is CT Corporation System, which can be served at 330 N Brand Boulevard, Suite 700, Glendale, California 91203.

19. Each Defendant is sued for its own acts, omissions, and obligations. Fireworks controlled the common processing infrastructure or provider credentials; Notion, Replit, and Uber selected and directed their respective processing arrangements and controlled their own data-handling functions. The following allegations identify the conduct and undertaking attributable to each.

/ / /

/ / /

[4] Fireworks.ai, Inc., *Statement of Information*, Cal. Sec'y of State filing no. BA20230319395 (Feb. 24, 2023), https://static.bizprofile.net/7/4/3/9/9/5/7439958.pdf; Fireworks AI, *Company Profile*, LinkedIn, https://www.linkedin.com/company/fireworks-ai (last visited Nov. 13, 2026); Fireworks, *Privacy Policy*, https://fireworks.ai/privacy-policy (last visited Nov. 13, 2026); Fireworks, *Fireworks Raises a $1.5 Billion Series D to Lead the Specialized Intelligence Revolution* (July 16, 2026), https://fireworks.ai/news/fireworks-raises-1-5-billion-series-d.

[5] Uber Techs., Inc., *Quarterly Report (Form 10-Q)*, cover & pt. I, item 1, note 1 (Nov. 4, 2026), https://www.sec.gov/Archives/edgar/data/1543151/000154315126000041/uber-20260930.htm.

III. JURISDICTION AND VENUE

20. **Jurisdiction.** Plaintiffs invoke the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), (5)(B), and (6). The proposed classes collectively contain at least 100 members. In addition to the affected Notion and Replit datasets, Uber's regulatory reporting identifies 4,296 affected Texans, as described in paragraph 81. Minimal diversity exists because Plaintiff Aliaga is a citizen of Nebraska and each Defendant is a citizen of Delaware headquartered in California. The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs, based on the scope of the incident and the compensatory relief sought for the Classes.

21. The proposed classes concern affected persons and entities throughout the United States. Their alleged injuries include disclosure of nonpublic personal and business information, impairment of proprietary interests, and recoverable investigation, containment, remediation, and other consequential losses where established. The jurisdictional amount concerns the claims actually asserted and accounts for overlapping class membership without counting the same injury more than once. Uber's reported incident total is not alleged to establish that every reported person belongs to the United States classes. Platform user totals and upper-bound incident percentages are not alleged to establish the number of affected persons.

22. This Court has personal jurisdiction over each Defendant because each maintains its principal place of business in California and is therefore at home in this State. In addition, the claims arise out of or relate to Defendants' operation of their California-based businesses and their decisions concerning the products, provider relationships, and data-handling practices described in this complaint.

23. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2). Defendants reside in this District for venue purposes, and a substantial part of the acts and omissions giving rise to the claims occurred here, including, on information and belief, decisions concerning provider selection, contractual safeguards, data retention, internal security, and incident response.

24. **Divisional Assignment.** Assignment to the San Francisco or Oakland Division is proper under Civil Local Rule 3-2(c) and (d), because the action arises in substantial part from conduct of businesses headquartered in San Francisco and San Mateo Counties. Fireworks and

Replit maintain their principal places of business in San Mateo County, and Notion and Uber maintain their principal places of business in San Francisco County.

25. Joinder is proper under Federal Rule of Civil Procedure 20(a). Plaintiffs' claims concern a series of related data-handling events and unauthorized-access incidents involving the same infrastructure provider and overlapping issues of retention, credential control, segmentation, investigation, and affected-data identification. The duties and conduct attributable to each platform are pleaded separately, permitting the Court to address common Fireworks issues and distinct platform issues without attributing one platform's conduct to another. The Uber allegations concern the earlier credential-access episode and do not depend on treating every spoke's records as one dataset or assigning every exposure to the October 24 event.

IV. FACTUAL ALLEGATIONS

A. Defendant Collected Plaintiff's and Class Members' Private Information

26. In an AI application, the visible interface and the systems processing a request may belong to different companies. A person may submit a message to Notion or an instruction to Replit while an outside infrastructure provider performs part of the computation. The outside provider can therefore receive the substance of the user's work even though the user has no direct account with that provider.

27. Provider access can also reach identification records maintained outside a conversational interface. A platform may make stored records available for a provider's work through credentials and permissions. If those credentials are compromised, the confidentiality risk extends to the records they can reach, even when the storage environment belongs to the customer rather than the provider.

28. A prompt is not merely a record that someone used a feature. It can be the document to summarize, the problem to solve, the software design to implement, or the factual context needed to produce a useful answer. A response can restate, organize, or derive further information from that same confidential material. A sequence of prompts and responses can disclose a project more fully than any single message.

29. In a development environment, related tool output can add information that was not manually typed into a prompt. Tool output may reflect the result of a program, a file operation, or another step in an agent's work. The exact tool output affected here must be determined from GUBER's records and Replit's disclosure. Replit's notice expressly included related tool outputs. Notion's notice to Aliaga described her affected transcripts as excluding tool-call results; its current broader guidance qualifies that exclusion as applying to most affected transcripts.

30. Operational metadata and content also serve different purposes. A token count or elapsed time may describe how a system operated. A technical design or business workflow describes what its owner is building. Combining both in a retained session record does not convert the proprietary content into an innocuous usage counter.

31. Plaintiffs' nonpublic information was held for processing in the services at issue. Authorization to process a private conversation, assist with a development task, or handle identification records does not itself authorize disclosure to an intruder or uncontrolled access through compromised credentials. The scope of authorized processing and the conditions under which Defendants held the information are relevant to the reasonable safeguards required for that information.

32. Nor does omitting a user's name from an outer record establish that the record is anonymous. A conversation may contain names, project details, organizational information, or combinations of facts that reveal its source. Confidentiality also protects information whose commercial or personal value would be impaired even if a recipient initially did not know its author's name.

33. The relevant security inquiry accordingly extends across the information's lifecycle: what was sent, why it was sent, which environment received it, what copies were made, how long they persisted, which credentials could reach them, and how the parties verified deletion and investigated access. Those are operational facts that can be established through routing configurations, storage inventories, access logs, job records, contracts, and incident records.

B. Fireworks was the common provider.

34. Fireworks markets infrastructure for adapting and serving models using customers' proprietary information and workflows. Its July 16, 2026 financing announcement described commercial use at substantial scale and reported more than $1 billion in annualized revenue run rate. Its business model thus contemplated receiving valuable enterprise information and supplying services that other companies would incorporate into their operations.[6]

35. The sensitivity of downstream information was foreseeable from those uses. An infrastructure provider supporting workspace analysis and software development would expect some customer payloads to contain personal records, nonpublic business plans, and proprietary technical material. Those are ordinary reasons customers use such tools, rather than an unforeseeable deviation from their commercial purpose.

36. Fireworks knew which enterprise customers supplied data or access authority to its platform and, on information and belief, maintained account, resource, and job records reflecting the services used for those customers. It could identify processing environments and credential permissions that an individual Notion, Replit, or Uber user could neither see nor administer.

37. Fireworks's published security documentation describes encryption during transfer and storage, restricted access, monitoring, workload isolation, network safeguards, and vulnerability management. Its current descriptions identify controls that Fireworks recognizes as important when receiving and handling customer information.[7]

38. Fireworks's retention rules also depend on the product and configuration. Its current documentation describes zero retention for ordinary open-model requests absent an applicable opt-in, while identifying storage-dependent exceptions, including batch processing and

[6] Fireworks, *Fireworks Raises a $1.5 Billion Series D to Lead the Specialized Intelligence Revolution*, supra note 4.

[7] Fireworks, *Data Security*, https://docs.fireworks.ai/guides/security_compliance/data_security (last visited Nov. 13, 2026).

certain Responses API requests. The actionable Notion-specific retention facts are pleaded separately; Plaintiffs do not infer that all Fireworks products were technically incapable of storing information.[8]

39. The enterprise relationships supplied Fireworks with information or access authority for defined service purposes. Customer authorization to perform work did not eliminate the need to protect the information and credentials accepted for that work. The service-specific processing instructions, access permissions, and actual configurations are evidence of the custody and control Fireworks exercised.

C. Notion supplied conversation content to Fireworks.

40. Norton's notice to Aliaga identified Fireworks as one of Notion's vendors. It explained that Notion used Fireworks to serve open-weight models inside Notion's product and to perform classification jobs supporting a feature called Insights. The same notice identified chat transcripts used for Insights as part of the affected material.[9]

41. Insights helped customers understand their use of Notion AI. Performing that function involved supplying conversation content for analysis, not merely reporting that a workspace had made a specified number of requests. Notion selected the vendor and the processing arrangement that carried this content outside the direct Notion interface.

42. A customer-facing function and a downstream processing copy involve distinct security decisions. The relevant facts include the purpose of the downstream copy, its persistence, the access permitted to it, and the safeguards implemented for it. Paragraph 4 identifies Notion's reported discrepancy between the intended retention configuration and the endpoints actually used.

43. Notion was positioned to determine what data was included in the classification payload, whether less revealing material could serve the same purpose, which endpoints received

[8] Fireworks, *Zero Data Retention*, https://docs.fireworks.ai/guides/security_compliance/data_handling (last visited Nov. 13, 2026).
[9] Notion, *Important Security Notice About the Fireworks AI Incident That May Impact Your Notion Workspace* (Nov. 10, 2026) (notice to Aliaga, received Nov. 11, 2026; retained by counsel).

it, and what contractual and technical controls governed those endpoints. Aliaga could use her own permissions and account controls, but she could not audit Notion's vendor configurations or inspect Fireworks's stored copies.

44. Notion's published AI privacy practices describe customer-data protections, contractual requirements for model and inference providers, and review of subprocessors. They state that AI use respects the permissions governing workspace content and that customer data is not used for model training by default. These representations distinguish permission to provide a requested AI function from unrestricted exploitation of the underlying data.[10]

45. Notion's current security page also describes vendor assessments and contracts requiring subprocessors to process information under Notion's instructions. That is relevant to Notion's own role in selecting and directing the provider. The alleged failure includes the implementation and verification of safeguards governing that relationship, rather than an allegation that the mere use of a disclosed outside vendor was necessarily unlawful.[11]

46. Notion controlled the transfer of the affected conversation content and the configuration and oversight of the processing arrangement it selected. Its responsibility to exercise reasonable care in handling nonpublic information arose from that conduct and the foreseeable exposure risk. The negligence claim concerns those operational responsibilities.

D. Replit's relationship with Fireworks reached development content.

47. Replit's subprocessor list, updated in August 2026, identifies Fireworks AI, Inc. as a United States provider of AI infrastructure. The list explains that subprocessors help Replit deliver its services and process customer data. This independently corroborates the relationship later identified in GUBER's security notice.[12]

48. Replit further described Fireworks as its partner for open-weight model inference and training in an engineering article published October 28, 2026. The publication concerns Replit's

[10] Notion, *Notion AI Security & Privacy Practices*, https://www.notion.com/help/notion-ai-security-practices (last visited Nov. 13, 2026).
[11] Notion, *Security @ Notion*, https://www.notion.com/security (last visited Nov. 13, 2026).
[12] Replit, *Subprocessors* (updated Aug. 2026), https://replit.com/subprocessors.

software-development benchmark and corroborates an operational relationship extending beyond a passive listing of a vendor's name.[13]

49. The affected data described in GUBER's notice consisted of development-session material. The inference and training partnership identifies the operational relationship; the relevant job and dataset records will establish the particular functions for which GUBER's content was transmitted or retained.

50. GUBER supplied proprietary development instructions and related material for private development work. The nature and context of that material made its sensitivity foreseeable to a platform that accepted and processed it. The content could remain commercially sensitive even when an outer session record lacked a company or account label.

51. Before GUBER created the affected July content, Replit published a detailed security explanation on April 20, 2026, updated April 21. Replit described layered safeguards, minimum necessary privileges, authentication between internal services using short-lived tokens, and segmentation to limit the effect of a compromise. The publication described security for both development environments and Replit's own control plane.[14]

52. The use of an infrastructure subprocessor introduced an additional processing environment into the service Replit furnished. On information and belief, Replit controlled its selection of Fireworks, the permissions and data supplied under that relationship, and its own assessment and verification of the safeguards for that processing. Those decisions were outside GUBER's ability to administer its own project or account.

53. Replit's notice identifies July content affected in an incident disclosed in November. That establishes that the relevant historical content, or a copy of it, remained reachable somewhere in the processing chain when unauthorized access occurred. It does not by itself establish when Fireworks first received the content or whether every copy persisted continuously

[13] Preeya Kirani et al., *ViBench 2.0: A Benchmark for Long-Horizon Software Building*, Replit Frontier (Oct. 28, 2026), https://frontier.replit.com/vibench-2-long-horizon-software-benchmark/.
[14] Luis Héctor Chávez, *Defense in Depth: How Replit Secures Every Layer of the Vibe Coding Stack*, Replit (Apr. 20, 2026, updated Apr. 21, 2026), https://replit.com/blog/defense-in-depth-how-replit-secures-every-layer-of-the-vibe-coding-stack.

from July. Those questions are answerable from dataset creation records, transfers, storage history, and deletion records.

E. Fireworks disclosed two periods of unauthorized activity.

54. Fireworks's first bulletin reported discovery of unauthorized use of internal credentials on October 6, 2026. It described access to environment variables used in evaluation jobs, including API keys and tokens. Its timeline placed initial customer notifications on October 7, employee-key rotation on October 9, and additional credential revocation on October 10.[15]

55. The first bulletin expressly qualified its findings as preliminary. It reported no detected access to additional categories of information within Fireworks's security perimeter or control at that time. The later disclosures expanded both the categories affected and the environments implicated, making the scope and timing of Fireworks's investigation material to the claims.

56. In its November 9 update, Fireworks described an October 23 security incident at an unnamed cloud provider hosting Fireworks research-and-development machines. Fireworks reported that an unauthorized party used that access on October 24 to reach development machines and run a workload that caused additional customer-data impact. Fireworks stated that it detected that activity the same day.[16]

57. The update expanded the disclosed categories to account and billing information and, for certain accounts, secrets, datasets, and incomplete model material. It excluded stored payment-card numbers, which Fireworks said it did not hold. Fireworks described assistance from Palo Alto Networks Unit 42 and measures addressing credentials, permissions, network isolation, storage access, and logging.

58. The response addressed the same operational areas implicated by the disclosed events: credential scope, pathways between environments, access to stored data, and the ability to

[15] Fireworks, *Fireworks October 2026 Security Incident* (updated Oct. 10, 2026), https://fireworks.ai/security/bulletins/october-2026-security-incident.

[16] Fireworks, *Update on October 2026 Security Incident* (Nov. 9, 2026), https://fireworks.ai/security/bulletins/october-2026-security-incident-update.

reconstruct activity. The underlying access and configuration records will establish the controls in place and the failures that permitted the unauthorized activity affecting Plaintiffs.

59. The disclosed sequence is significant because the second period involved development infrastructure after Fireworks had already identified an internal-credential compromise. Reasonable incident response required assessing the reach of exposed credentials and protecting the environments through which customer information could be reached. Plaintiffs allege failures in those functions to the extent supported by the specific access and retention facts below.

60. Fireworks's use of an upstream cloud provider added another layer between Plaintiffs and the infrastructure holding or able to reach their information. Fireworks has not publicly identified that provider. Its contracts, network design, and development-environment records will establish the allocation of access and responsibilities at that layer.

F. Notion's investigation connected the retained data to affected users.

61. Notion's revised public timeline states that Fireworks notified it on November 2 about a dataset initially understood to contain synthetic testing information. Notion disconnected from Fireworks on November 3 and deleted its data there on November 4. Fireworks raised potential customer-data exposure on November 6, confirmed the affected dataset on November 8, and Notion began notifying affected customers on November 9.[17]

62. The notice sent to Aliaga was dated November 10, 2026; she received and reviewed it on November 11. It identified her workspace as among the fewer than one percent of Notion workspaces potentially affected. The notice instructed affected customers to review their records and treat the identified information as exposed.

63. Notion's notice to Aliaga described her affected sessions as lacking separate labels identifying their authors or workspaces and as containing no tool-call results. It expressly qualified

[17] Notion, *Fireworks AI Incident* (updated Nov. 12, 2026, with incident updates through Nov. 13, 2026), https://www.notion.com/en-gb/security/advisories/security-incident-involving-a-third-party-ai-vendor (last visited Nov. 17, 2026).

that description by referring to what appeared in the words of the transcripts. That qualification preserved the possibility that the text itself revealed confidential or identifying information.

64. Notion's current guidance further identifies complete user messages and AI responses as affected content. Selected page text and source fragments reproduced in responses could also appear. It limits its metadata and tool-use exclusions to most affected transcripts. Meeting Notes could be implicated when entered in messages or referenced in responses; original attachments and the rest of a selected page were outside the described content. These are incident-wide descriptions, while Aliaga's own affected material is identified through the records she reviewed.[18]

65. Notion's subsequent public updates disclosed concrete sensitive content in affected messages. It revoked exposed Notion API keys on November 11 and reported exposed third-party API keys to their issuers on November 12. This concerns the broader affected dataset; Plaintiffs do not allege from those disclosures alone that Aliaga's own messages contained an exposed credential.

66. Notion's incident instructions distinguish an affected-content export from an annotated export. The former supplies affected text. The latter adds context, including identifiers and dates, to help customers investigate. Notion says that added metadata was not itself exposed. Its affected-member records also link members, including deactivated members, to counts of affected material. These records provide a means to identify the population and distinguish compromised content from later investigative annotation.

67. The export structure permits two separate inquiries: what the unauthorized actor received and who owns or is identified in that material. The distinction supports both individualized injury analysis and administration of notice to affected members.

68. The account-specific evidence connects the retained material to downstream injury. The copy history, endpoint settings, access permissions, and investigation records will

[18] Notion, *Notice About the Fireworks AI Incident That May Impact Some Notion Workspaces*, supra note 1 (sections concerning affected content and affected-member records; last visited Nov. 17, 2026).

establish how the affected information remained available to the unauthorized actor and which operational failures permitted access.

69. The Notion claim concerns the affected conversation material and the information contained in it. Those conversations are the identified source of Aliaga's privacy and development-information injuries. Notion's notice supplies a defined affected dataset that can be examined without equating a connected external service with wholesale access to all of that service's records.

G. Replit confirmed GUBER's account was affected.

70. Replit sent the account used by GUBER a security notice on November 10, 2026, entitled "Security Notice: Third-Party Provider Security Incident Affecting Replit User Data." Replit identified Fireworks as the provider involved and stated that some data associated with GUBER's account was impacted.[19]

71. The notice stated that Fireworks informed its customers on November 9 that an unauthorized party had obtained access to certain data. Replit said its further investigation identified GUBER's account among the fewer than 0.05 percent of accounts affected. It identified a subset of prompts dated July 14 through July 29, 2026, together with token counts, timings, tool outputs, and settings.

72. Replit described the records as lacking labels tying them to a person, account, or organization, but warned that the prompt text could contain information identifying the source. It excluded account passwords and payment information outside the agent sessions from the described exposure. Those exclusions do not eliminate the proprietary development content within the affected sessions.

73. Replit recommended rotating potentially exposed credentials, reviewing activity in Replit and connected services, and watching for phishing. It distinguished credentials a user might have included in a prompt from ordinary account credentials outside the session. The notice accordingly required an account-specific assessment of the actual text and related material.

[19] Replit, *Security Notice: Third-Party Provider Security Incident Affecting Replit User Data* (Nov. 10, 2026) (notice to the account used by GUBER; retained by counsel).

74. GUBER requested an account-specific disclosure and preservation of evidence from Replit. As of its initial inquiry to counsel, it had not received enough information to determine the complete scope of exposure or additional resulting harm. The original notice supplies a direct affected-account link even though the complete payload and access history remain in Defendants' possession.

75. For GUBER, material unanswered questions include which prompts and tool outputs were retained; what project or file content those outputs contained; which copies reached Fireworks; the permissions governing those copies; the unauthorized access actually recorded; and what steps were taken to isolate, recover, or render unusable the exposed material. A percentage of all Replit accounts does not answer any of those questions.

H. Uber disclosed access to ID records via compromised provider credentials.

76. Uber's formal notice states that its provider warned it of compromised internal credentials on October 9, 2026. Uber disconnected the provider and investigated. By October 13, Uber had determined that the credentials had been used to access personal information. The notice is dated November 10.[20]

77. Uber's Iowa filing dates the unauthorized access to October 7. It describes Uber-created cloud storage supporting the provider's work, overseen by Uber's Cloud Security team. Alerts were enabled but did not trigger because the intruder used valid credentials and existing data flows. The filing identifies driver's-license images and extracted names, addresses, birth dates, and license numbers.[21]

[20] Uber Techs., Inc., *Notice of Security Incident* 1–2 (Nov. 10, 2026), https://oag.ca.gov/system/files/Multistate%20Template%20-%20Final.pdf (filed with the California Attorney General).

[21] Letter from Amelia M. Gerlicher, Counsel for Uber Techs., Inc., to Consumer Prot. Div., Off. of the Att'y Gen. of Iowa, Re: Notification of Security Incident 1–2 (Nov. 10, 2026), https://www.iowaattorneygeneral.gov/media/cms/11102026_Uber_Technologies_Inc_089721E61CBAB.pdf.

78. An Uber spokesperson identified Fireworks.ai as the third-party vendor involved in the notices sent to drivers, according to the Wall Street Journal. That identification connects the formally disclosed access mechanism to the common provider in this action.[22]

79. The access path involved two distinct security responsibilities: safeguarding provider credentials and restricting access to the records those credentials could reach. A system's recognition of a credential as valid does not establish that the person presenting it is authorized. On information and belief, reasonable safeguards required limiting the information reachable through those credentials and assessing misuse of authorized access paths.

80. The Iowa filing states that the credentials did not provide access to other Uber systems and that the investigation remained ongoing. The alleged exposure concerns the identified environment; it does not require access to every Uber system. The October 7 date also precedes the separate October 24 Fireworks development-machine event. Plaintiffs allege the chronology specific to this spoke rather than treating the later event as the date of the Uber access.

81. Texas's published Uber report identifies 149,346 affected individuals in total, including 4,296 Texans. Oregon's listing independently reports 149,346 affected individuals. These are reported incident figures, not an allegation that every person counted resided in the United States or that the totals from the two states should be added together.[23]

82. Uber's consumer notice offers credit monitoring and fraud assistance and states that Uber had not identified misuse of the information as of that notice. The absence of identified misuse does not undo the access Uber reported. The offering also does not establish that Plaintiffs Tallauze or Lewis enrolled in monitoring or incurred a particular expense.

[22] Natalie Weger, *Uber Says Personal Data Was Exposed in Third-Party Data Breach*, Wall St. J. (Nov. 13, 2026), https://www.wsj.com/tech/uber-says-personal-data-was-exposed-in-third-party-data-breach-02e3a875 (reporting a statement by Uber's spokesperson identifying Fireworks.ai).

[23] Off. of the Att'y Gen. of Tex., *Data Security Breach Reports*, Uber Technologies, Inc., report no. BR-0005510 (published Nov. 13, 2026), https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Nov. 17, 2026); Or. Dep't of Just., *Data Security Breaches*, Uber Technologies, Inc. (reported Nov. 10, 2026), https://justice.oregon.gov/consumer/databreach/ (last visited Nov. 17, 2026) (corroborating the reported affected-person total).

83. The relevant common evidence includes the records placed in the provider-access environment, the affected-person mapping, credential privileges, access logs, alerting rules, and the chronology of revocation and investigation. Those records can establish the data reached, the scope of each Defendant's control, and whether the safeguards reasonably addressed the access mechanism disclosed by Uber.

I. Independent disclosures corroborate the provider access risks.

84. In a November 13 disclosure, Cursor reported that a key it had issued to Fireworks was exposed there and used to copy a shared read-only storage bucket. Cursor described the bucket as containing historical coding-agent traces from sessions outside Privacy Mode, some containing unredacted credentials. It reported further access through credentials found in those traces, affecting selected internal services and information. Cursor distinguished those historical records from active inference and said Privacy Mode prompts and code were unaffected.[24]

85. This account identifies an additional way compromised provider credentials can expose downstream information. The relevant information need not reside on the same physical system as the compromised credential. The account corroborates the importance of credential scope, customer-side access permissions, retained copies, and investigation across connected systems. Plaintiffs do not infer that Notion and Replit used Cursor's bucket or the same processing configuration.

86. Nikken's November 13 notice states that affected Notion AI material included business information and the names of contact people at business partners. It distinguishes attached files themselves from AI-generated content based on those files and describes continuing review and business-partner notifications.[25]

87. Information in an affected conversation may therefore concern someone other than the person who held the submitting account or received the workspace notice. A company

[24] Cursor Team, *An Update on Our Recent Security Incident*, Cursor (Nov. 13, 2026), https://cursor.com/blog/security-incident-update (sections entitled "What happened" and "What was not affected").

[25] Nikken Sekkei Ltd., *Notice Regarding a Data Breach in the Cloud Service (Notion AI) Used by Nikken Group Companies* §§ 2–4 (Nov. 13, 2026), https://www.nikken.co.jp/en/news/news/20261113j.html.

may own the development material in an employee's session, and a private conversation may contain another person's nonpublic information. The four classes below address those interests through the affected information itself.

J. Aliaga's affected educational and startup information.

88. Aliaga had a Notion account for several years before upgrading to the Business plan in August 2026. She subscribed for one paid seat at $24 per month. Her paid invoices are dated August 26, September 26, and October 26, 2026. The affected October conversations were created after that upgrade.

89. Aliaga used Notion to organize academic activities and to work on software development, including an early-stage startup project with other students. She supplied information for those tasks within her account. She did not intend the affected conversations to be disclosed to an unauthorized outsider.

90. Aliaga connected her Canvas calendar to Notion Calendar through her school email calendar. Her use of the connected services brought academic scheduling information into her Notion-related workflow. Separately, her review of the affected conversation records confirmed that the identified text included information about her academic activities and development projects.

91. After receiving the notice, Aliaga retrieved and reviewed the records Notion made available for her affected conversations. Those records identified 151 messages across seven threads, with content dates spanning October 5 through October 23, 2026. She recognized private material concerning her academic activities, scheduling, and software-development work.

92. On information and belief, the affected development material included Aliaga's proprietary startup information and nonpublic technical work, including information she maintained as confidential trade-secret information, and the unauthorized disclosure compromised the confidentiality of those materials. Their substantive contents can be identified in protected discovery without republishing the technical details in this complaint.

93. Aliaga asserts injury to her own privacy and, on information and belief, her interests in the affected startup and trade-secret information. Her claims concerning collaborative

work are limited to rights she holds. The allocation of rights in particular materials can be established through project records and agreements while protecting the underlying information.

94. The affected educational conversations concerned her own activities in a context she treated as private. Her decision to use an AI tool to organize or work with information did not eliminate that expectation as against an unauthorized third party. The ability of a provider to read data for a limited service purpose differs from unrestricted disclosure beyond that purpose.

95. The content itself carried details associated with Aliaga's activities and projects. Even without an added account label, contextual information could connect the material to her or reveal confidential project details. She became concerned about that possibility after examining the actual records, rather than solely from learning that some unrelated account had experienced an incident.

96. On information and belief, Aliaga's identified nonpublic conversation content was among the material accessed or acquired without authorization in the incident. That allegation is supported by Notion's workspace-specific notification, the affected-content records supplied to her, her recognition of their contents, and Notion's public explanation of its incident-review exports.

97. The resulting injury includes the disclosure and loss of confidentiality of private information. A conversation disclosed to an unauthorized person is no longer confined to the audience for which it was provided, regardless of whether the recipient has yet attempted financial fraud. Aliaga also spent time reviewing the identified material and determining its relevance to her private activities and development work.

98. The unauthorized disclosure and resulting loss of confidentiality are present injuries. The extent of additional legally recoverable loss will be established through evidence of actual consequences and expenses. Aliaga does not allege that every affected person suffered identity theft, fraud, or the same amount of monetary loss.

K. GUBER's affected commercial development information.

99. During July 14 through July 29, 2026, GUBER was actively using Replit to develop commercial AI technology and associated applications. Its founder acted for the company

in that work. The development sessions included instructions and technical context needed to make the software perform GUBER's intended business functions.

100. The affected subject matter included GUBER's proprietary technical designs, development material, and business workflows. These materials reflected how its commercial technology would operate and included information GUBER maintained as trade secrets. Their contents could reveal implementation choices and nonpublic functionality developed for the company.

101. GUBER treated the affected proprietary material as confidential company information and supplied it for its development work. It seeks recovery for the impairment of its rights in that material. The specific technical information and evidence of the measures used to protect it can be disclosed under appropriate discovery protections, preserving the confidentiality remaining in the information.

102. Replit's account-specific notice supports an allegation that GUBER's development-session information was within the affected data. Plaintiffs do not infer that every GUBER repository, application, line of code, or company record was obtained. The exposed subset and its significance can be determined by comparing the affected records with GUBER's development history.

103. The inclusion of tool outputs in Replit's notice increases the importance of comparing the affected records with GUBER's development history. An agent session can contain material beyond the instruction originally entered by the user. The identified tool output may show whether additional nonpublic development material was exposed during that work.

104. GUBER's affected development material was exposed to an unauthorized actor, impairing the confidentiality in which the company maintained that material. Its representative requested disclosure and preservation to identify what had been compromised and evaluate an appropriate response. The extent of any competitive injury will be determined by comparing the compromised information with the company's development records and evidence of subsequent use.

105. GUBER seeks recovery for legally cognizable injury caused by the exposure and established through evidence, including reasonable investigation and containment expenses, necessary remediation of specifically exposed material, and impairment of proprietary interests to the extent recoverable under the governing law. Its claim concerns the consequences of the affected disclosure rather than an undifferentiated valuation of the entire company.

L. Tallauze's affected identification information.

106. Uber obtained and maintained an image of Tallauze's driver's license and related identification information in connection with its platform operations. The information was supplied or maintained for a limited service purpose and was not intended for public dissemination or use by an unauthorized third party.

107. On information and belief, the affected Uber records included Tallauze's driver's-license image and extracted text containing his name, street address, date of birth, and driver's-license number, together with identifying information appearing on that image. These are the categories described in Uber's formal disclosures. Tallauze's actual license number, full birth date, street address, and document image are not reproduced in this public pleading.

108. On information and belief, Tallauze's identification records were among the Uber information accessed or acquired through the compromised provider credentials. The allegation concerns the Uber environment described above and the access permitted through Fireworks; it does not depend on a direct subscription relationship between Tallauze and Fireworks or on an allegation that he personally supplied credentials to Fireworks.

109. On information and belief, that unauthorized acquisition disclosed Tallauze's sensitive identification records beyond their intended custodians and caused a present loss of confidentiality. A government-issued identification image combined with the identifying fields extracted from it can enable impersonation and targeted misuse. The alleged privacy injury arises from the completed unauthorized access and disclosure, without an allegation that a particular fraudulent transaction has already occurred.

110. Uber's account records and affected-person mapping, together with the storage and access records, will further establish Tallauze's connection to the compromised records. Tallauze seeks compensatory relief for legally cognizable injury caused by the disclosure and any additional recoverable consequences established by evidence. He does not allege a presumed monetary value for each exposed field or an unverified expenditure.

M. Lewis' affected identification information.

111. Plaintiff Lewis received a notice letter from Defendant dated November 10, 2026, informing him that his Private Information, including at least an image of his driver's license and text data that included his name, address, date of birth, and driver's license number, was impacted in the Breach.[26]

112. Lewis' identification records were among the Uber information accessed or acquired through the compromised provider credentials. The allegation concerns the Uber environment described above and the access permitted through Fireworks; it does not depend on a direct subscription relationship between Lewis and Fireworks or on an allegation that he personally supplied credentials to Fireworks.

113. The unauthorized acquisition disclosed Lewis' sensitive identification records beyond their intended custodians and caused a present loss of confidentiality. A government-issued identification image combined with the identifying fields extracted from it can enable impersonation and targeted misuse. The alleged privacy injury arises from the completed unauthorized access and disclosure, without an allegation that a particular fraudulent transaction has already occurred.

N. Specific security oversight failures caused the exposure.

114. Having accepted nonpublic information or authority to access it for service processing, Fireworks was required to exercise reasonable care within the scope of that custody

[26] Exhibit 1

and control. The affected population was bounded by identifiable customer relationships and the information reached through them. Fireworks's conduct directly determined whether downstream data subjects and owners faced unauthorized access, while Fireworks derived a commercial benefit from the processing.

115. On information and belief, Fireworks failed to restrict credential access and the reach of internal accounts sufficiently to prevent the unauthorized access affecting Plaintiffs. The factual basis includes Fireworks's disclosed misuse of internal credentials, the Uber access mechanism described in paragraph 76, and the later access to development machines that caused additional customer-data impact. The particular credentials, privileges, and affected storage paths remain within its records.

116. On information and belief, Fireworks failed to maintain sufficient separation between systems vulnerable to the unauthorized activity and customer content reachable from those systems. This allegation is grounded in Fireworks's account of an unauthorized workload on development machines causing customer-data impact. It concerns the actual connection between those environments, rather than an assumption that all development infrastructure must operate without any customer data.

117. For the Notion material, the discrepancy described in paragraph 4 identifies retained conversation content at endpoints expected to discard it. On information and belief, Fireworks failed to apply and verify retention and access controls appropriate to that content and processing purpose. Those operational failures were substantial factors in leaving the affected conversations available for unauthorized access.

118. Reasonable operation of the relevant systems required verifying the settings, copies, and access permissions governing the nonpublic information accepted for processing. On information and belief, inadequate verification allowed the conditions described above to persist. The claim concerns those security practices independently of a demand that Plaintiffs receive performance under a vendor agreement.

119. On information and belief, Notion, Replit, and Uber each failed to exercise reasonable care in configuring, supervising, and verifying the processing or access arrangements

for their respective affected data. These allegations concern each platform's own data flows, permissions, and oversight. They do not rest solely on the proposition that a vendor suffered an attack.

120. For Notion, the factual basis includes the identified data flow and retention discrepancy described in paragraphs 39 and 4. Reasonable oversight required verification of the material safeguards governing that processing arrangement. On information and belief, Notion's verification was inadequate.

121. For Replit, the factual basis includes its use of Fireworks and its identification of GUBER's historical prompts and tool outputs in the affected data. On information and belief, Replit failed to apply or verify safeguards sufficient for the duration, sensitivity, and access paths of those development records. GUBER's unanswered request for fuller disclosure separately demonstrates why the complete scope and resulting response needs remain unresolved.

122. For Uber, the factual basis includes the disclosed provider-access environment and failure of its enabled alerting to identify the use of compromised credentials. On information and belief, Uber failed to implement or verify access restrictions and monitoring reasonably suited to that environment and the sensitivity of the identification records. The claim concerns the permissions and safeguards Uber controlled, including protection against misuse of an otherwise valid provider credential; it does not assume that Uber had no monitoring or that every authorized provider connection was improper.

123. Each Defendant also had responsibilities within its own role to investigate the reach of compromised credentials and identify affected data accurately. Plaintiffs do not treat a later notification date, without the accompanying investigation facts, as proof of a particular statutory notification violation. The relevant questions include when a Defendant learned of access affecting the relevant data, what it could reasonably determine, and what information it supplied to enable a meaningful response.

124. Plaintiffs could manage their own access and content choices, but they could not revoke a Fireworks employee credential, segregate its development network, inspect a retained processing dataset, administer Uber's provider-access environment, or determine which

downstream copies had been accessed. The alleged failures concern those functions rather than an unsupported assertion that a Plaintiff disclosed an account password or disabled a protection.

125. The exposure alleged here is the foreseeable result of failures to protect information accepted for processing. Restricting credentials reduces the records an intruder can reach; separating environments limits movement into customer-data systems; and eliminating an unnecessary retained copy removes it from the available target set. On information and belief, failures in those controls were substantial factors in the unauthorized access to Plaintiffs' identified information.

126. Protecting nonpublic data against unauthorized actors is a principal purpose of the credential, access, retention, and vendor controls at issue. The malicious actor's intervention presented the very category of risk those safeguards were intended to address. Plaintiffs allege failures to exercise reasonable care in the functions each Defendant actually controlled.

127. The causal allegations combine the specific platform-to-provider relationships, the allegations concerning each Plaintiff's affected information, GUBER's and Aliaga's affected-account notices, Lewis' notice letter from Uber informing him he was affected by the data breach, Uber's regulatory disclosures, the categories and dates supplied by Defendants, and the disclosed access and retention conditions. Tallauze's inclusion in the affected Uber records is alleged on information and belief. Defendants' account mappings, storage inventories, and forensic records will further establish the connection between the identified access paths and each Plaintiff's information.

O. Common evidence can establish the extent of the incident.

128. The principal sources of common proof include the affected datasets; mappings between those datasets and customer accounts; notices; routing and job records; storage and deletion records; credential and permission histories; forensic access records; and the instructions and agreements governing processing. These materials concern how Defendants handled the same categories of information through centralized systems.

129. Common records can distinguish the scope of system access from the records actually obtained, permitted storage from retention exceeding an applicable instruction, and compromised content from later investigative annotations. Those distinctions will establish the reach and consequences of the common processing failures.

130. Individual evidence will establish the content of a claimant's affected records, the claimant's interest in that information, and any recoverable personal or business loss. That evidence can be considered through phased proceedings and appropriate damages procedures without requiring every class member to reproduce the same proof about Fireworks's internal systems or a platform's common security practices.

131. The precise contents of the affected private conversations and proprietary technical material can be exchanged under an appropriate protective order and, where the legal standard is met, presented to the Court through narrowly tailored sealing procedures. The public complaint describes the categories and circumstances necessary to plead the claims without republishing the sensitive material whose confidentiality Plaintiffs seek to protect.

V. CLASS ACTION ALLEGATIONS

132. Plaintiffs bring this action under Federal Rule of Civil Procedure 23(a) and (b)(3), and alternatively seek certification of appropriate common issues under Rule 23(c)(4). They propose only the following four classes. For these definitions, the "Fireworks Security Incidents" are the unauthorized-access events described above and disclosed by Fireworks and affected customers in October and November 2026. "Persons and entities in the United States" includes individuals who resided in the United States when their information was accessed or acquired, and entities then organized under the laws of a United States jurisdiction or maintaining their principal place of business in the United States.

133. **Fireworks Class:** All persons and entities in the United States whose nonpublic information or content was accessed or acquired by an unauthorized person in the Fireworks Security Incidents, including information held by Fireworks or reached through credentials compromised in those incidents.

134. **Notion Class:** All persons and entities in the United States whose nonpublic information or content was contained in data supplied or made accessible through Notion and accessed or acquired by an unauthorized person in the Fireworks Security Incidents.

135. **Replit Class:** All persons and entities in the United States whose nonpublic information or content was contained in data supplied or made accessible through Replit and accessed or acquired by an unauthorized person in the Fireworks Security Incidents.

136. **Uber Class:** All persons and entities in the United States whose nonpublic information or content was contained in data supplied or made accessible through Uber and accessed or acquired by an unauthorized person in the Fireworks Security Incidents.

137. The four classes include affected current and former users, account holders, workspace or organization members, guests, and persons or entities whose information others supplied. Membership does not depend on whether access was free or paid, personal or commercial, or obtained through an individual or organizational account. Receipt of an incident notice, use of a particular subscription plan, and a direct account with Fireworks are not required. The Fireworks Class is not limited to information supplied through Notion, Replit, or Uber.

138. The Fireworks Class is asserted against Fireworks; the Notion Class against Notion; the Replit Class against Replit; and the Uber Class against Uber. Aliaga, GUBER, Tallauze and Lewis seek to represent the Fireworks Class, Aliaga the Notion Class, GUBER the Replit Class, and Tallauze and Lewis the Uber Class. A person or entity may belong to more than one class. Each Defendant's liability and each claimant's legally protected interest and recoverable injury must be established under the applicable claim, without duplicating recovery for the same injury.

139. Excluded are Defendants; their officers and directors; entities they control; persons who participated in the unauthorized access; the judicial officers assigned to this action and their immediate families; and persons who timely and validly request exclusion from a certified damages class. Membership requires nonpublic information or content about or belonging to the member within the affected data. Platform use alone does not establish membership.

140. **Numerosity.** On information and belief, the proposed classes are sufficiently numerous that joinder is impracticable. Uber's reported total and Texas population are set out in

paragraph 80. Notion and Replit describe affected data across multiple accounts and workspaces and maintain member-mapping or account records. The precise membership of each class, including overlap and the applicable United States population, can be determined from those records. The reported Notion and Replit percentages are not treated as counts of persons or as proof that every platform account was affected.

141. **Commonality.** Common questions include the nature and reach of the Fireworks access paths; which data copies were retained; what retention and access controls applied; whether reasonable safeguards were implemented; whether the alleged failures caused unauthorized access to the identified data; and what common remediation or disclosure obligations remain.

142. For the Notion Class, additional common questions concern the actual processing arrangement, the endpoint and retention conditions described in paragraph 4, vendor oversight, the identification of affected content, and whether Notion exercised reasonable care in transmitting and supervising the processing of that content.

143. For the Replit Class, additional common questions include the content and duration of retained development-session records; the instructions governing Fireworks's processing; the nature of the affected tool outputs; the access paths reaching the records; and whether Replit reasonably assessed, implemented, and verified the safeguards for that processing.

144. For the Uber Class, additional common questions concern the provider-access environment, the scope and protection of credentials, the permissions and monitoring governing that environment, identification of the affected records, and whether Uber exercised reasonable care in safeguarding information reachable through the provider's access.

145. **Typicality.** Each named Plaintiff alleges loss of confidentiality of nonpublic information reached through a platform's relationship with Fireworks. Aliaga's claims arise from affected Notion conversations and GUBER's from affected Replit development sessions; their respective notices identify their own workspace or account. On information and belief, Tallauze's and Lewis' claims arise from the affected Uber identification records and the credential-access path Uber disclosed. Their claims challenge the security and processing failures applicable to the information and classes each seeks to represent.

146. The proposed common questions concern the handling and protection of affected information. Differences in a member's status as a user, data subject, or information owner do not change the identity of the affected systems or the challenged security practices. Plaintiffs will establish the protected interests and remedies applicable to their own injuries and to the claims presented for certification.

147. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the classes they seek to represent. Their interests in establishing the relevant failures, obtaining appropriate relief, and preserving the confidentiality of affected material align with those classes. They have retained counsel to prosecute the action and will discharge their duties as representatives, subject to the Court's supervision.

148. If discovery identifies material differences in the applicable law, processing paths, or recoverable injuries, Plaintiffs will propose appropriate issue certification, trial procedures, additional representatives where warranted, or refinement of the four class definitions under Rule 23(c)(1)(C). Plaintiffs do not assume that all members suffered the same loss or that one business's proprietary material has the same value as another's.

149. **Predominance.** The central liability evidence concerns centralized systems, retained datasets, provider instructions, access controls, and common security practices. It will substantially overlap across members of the applicable class. Individual questions concerning the amount of loss can be addressed separately where the common liability issues otherwise satisfy Rule 23(b)(3).

150. Plaintiffs seek application of California law where supported by the applicable choice-of-law rules and facts, including the locations of Defendants and the relevant conduct. The location of a headquarters alone does not supply California law for every claim nationwide. Plaintiffs will address material differences in governing law through the certification analysis, proposed common issues, and any necessary refinement of the four classes.

151. **Superiority.** Common proceedings would avoid duplicating discovery and adjudication of Defendants' processing arrangements and security systems. Many individual claims concerning unauthorized disclosure would be uneconomic to litigate separately. The class

procedure also permits owners with materially different business losses to evaluate their own interests and exercise applicable exclusion rights.

152. **Manageability.** Defendants' affected-account notices, member records, and dataset mappings provide objective starting points for identifying members. Claimant evidence can verify ownership or personal connection to particular material and resulting losses, including claims by persons who did not hold the submitting account or receive the original notice. Any distribution or damages process can account for reimbursements, overlapping accounts, and duplicate claims so that the same injury is not compensated more than once.

153. Alternatively, Plaintiffs seek certification of particular issues under Rule 23(c)(4), including applicable common duties, retention or access practices, breach, and common causation questions, to the extent those issues can be resolved fairly on a class basis. Plaintiffs request a certification structure responsive to the evidence and the Court's choice-of-law analysis.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
NEGLIGENCE AGAINST FIREWORKS
(GUBER, Aliaga, Tallauze, and Lewis on behalf of themselves and the Fireworks Class)

154. Plaintiffs incorporate the preceding factual and class allegations applicable to Fireworks and the Fireworks Class. GUBER, Aliaga, Tallauze, and Lewis assert this claim for their respective affected information and injuries.

155. Fireworks owed a duty to use reasonable care in receiving, processing, retaining, securing, and controlling access to Plaintiffs' nonpublic information, including protecting credentials capable of reaching that information. The duty arises from Fireworks's own acceptance of custody or access authority and its control of the systems and permissions through which an unauthorized actor could reach the information.

156. The relationship was concrete and bounded: Fireworks received information or access authority through identifiable enterprise customers for particular processing functions; the

downstream subjects and owners could not administer Fireworks's security; the disclosure risk was foreseeable from the substance and purpose of the processing; and Fireworks benefited commercially from that work. The responsibility asserted concerns the foreseeable effect of Fireworks's own conduct on the people and businesses whose information it handled.

157. Reasonable care included restricting credential scope, applying effective authorization, segregating relevant environments, limiting unnecessary retention, verifying the operation of material controls, and investigating known compromises sufficiently to identify and contain access affecting customer information. The appropriate safeguards depended on the sensitivity, purpose, and duration of the processing.

158. Fireworks breached that duty through the failures alleged in paragraphs 114 through 123, including the access paths by which unauthorized activity reached affected data and the retention and verification failures affecting Notion information. Plaintiffs will establish the technical details through the records of the affected systems and investigation.

159. Those failures were substantial factors in permitting access to Plaintiffs' identified information. The unauthorized actor's intervention was within the category of risk the safeguards were intended to address. The allegations concerning each Plaintiff and the access paths described above, including Tallauze's allegations on information and belief, connect the alleged provider-side conduct to the affected information.

160. Aliaga suffered unauthorized disclosure of her nonpublic personal information and related response burdens and, on information and belief, impairment of her interests in the affected startup and trade-secret information. GUBER suffered loss of confidentiality and impairment of its interests in its development information. Lewis suffered unauthorized acquisition and disclosure of his sensitive identification records and the resulting loss of confidentiality. On information and belief, Tallauze suffered unauthorized acquisition and disclosure of his sensitive identification records and the resulting loss of confidentiality. Each seeks damages proximately caused by Fireworks's breach and recoverable under the governing law for the injury established, without duplicating another recovery.

SECOND CAUSE OF ACTION
NEGLIGENCE AGAINST NOTION
(Aliaga on behalf of herself and the Notion Class)

161. Aliaga incorporates the preceding factual and class allegations applicable to her, Notion, and the Notion Class.

162. Notion owed a duty of reasonable care in its own handling and transmission of nonpublic information and in the configuration and oversight of the processing arrangements it selected for that information. Aliaga entrusted personal and development content through Notion's service, while Notion controlled the vendor relationship and the information routed for Insights.

163. Notion's custodial responsibility concerned protection against unauthorized disclosure of private information already entrusted to it. Notion chose the outside recipient and controlled the purpose and parameters of the transfer. Its independent conduct exposed Aliaga to a privacy injury beyond the failure to furnish an ordinary product feature.

164. Notion breached the duty through the failures alleged in paragraphs 114 through 123, including inadequate implementation and verification of the controls governing the relevant processing. The particular operational discrepancy described above supplies a factual basis for the claim beyond the occurrence of a vendor attack.

165. Notion's conduct was a substantial factor in the exposure of Aliaga's identified conversations. Notion supplied the material for the relevant processing and was responsible for its own choices and oversight within that arrangement. The data included private educational information and, on information and belief, confidential startup and trade-secret information, as described without republishing the material in this complaint.

166. Aliaga and members of the Notion Class suffered the unauthorized disclosure of their affected information and resulting legally cognizable injuries. Aliaga seeks compensatory damages according to proof under the governing law, without duplicating any recovery under another claim.

/ / /

/ / /

/ / /

THIRD CAUSE OF ACTION
NEGLIGENCE AGAINST REPLIT
(GUBER on behalf of itself and the Replit Class)

167. GUBER incorporates the preceding factual and class allegations applicable to it, Replit, and the Replit Class.

168. Replit owed a duty to exercise reasonable care in receiving, transmitting, and securing nonpublic development information and in configuring and supervising the processing arrangements it selected for that information. GUBER supplied proprietary material for development work, while Replit controlled the provider relationship, the data it transmitted, and its assessment and oversight of the relevant safeguards.

169. The duty asserted concerns Replit's own handling of information entrusted to it and protection against unauthorized access to that information. The challenged conduct includes operational decisions about the data supplied to an outside processor, the duration and location of retained copies, the permissions capable of reaching them, and verification of the security controls governing that processing.

170. The risk to the owners and subjects of the information was foreseeable from the nature of Replit's development service and the prompts and related session material it accepted. The affected population was bounded by the information Replit caused to be processed. GUBER could not inspect the provider's retained datasets, configure its internal permissions, or revoke its compromised credentials. Replit was positioned to assess and supervise the processing arrangement it selected.

171. Reasonable care required safeguards appropriate to the sensitivity and persistence of the development records, including appropriately restricted provider access, evaluation of the processing purpose and retention settings, verification of material security controls, and investigation of unauthorized access affecting the information. These precautions concern the actual processing functions Replit directed or controlled.

172. On information and belief, Replit breached that duty through the failures described in paragraphs 114 through 123. The account-specific notice, the identified historical prompts and tool outputs, and the documented processing relationship supply the factual basis for the allegation.

Routing records, dataset histories, permissions, vendor reviews, and incident records will establish the particular conditions that permitted access.

173. On information and belief, Replit's failures were substantial factors in permitting unauthorized access to GUBER's affected development information. Protecting that information from an outside actor was within the purpose of the safeguards at issue. Replit's own notice identifies GUBER's account and the affected content period, connecting the alleged failures to GUBER's information.

174. The unauthorized access impaired the confidentiality of GUBER's affected development material and the proprietary interests described above. GUBER seeks damages according to proof for legally cognizable injury proximately caused by Replit's conduct, including reasonable response and remediation expenses to the extent established and recoverable. It does not seek a presumed value for every affected record or duplicate recovery for the same injury.

FOURTH CAUSE OF ACTION
NELIGENCE AGAINST UBER
(Tallauze and Lewis on behalf of himself and the Uber Class)

175. Tallauze and Lewis incorporate the preceding factual and class allegations applicable to them, Uber, and the Uber Class. Tallauze's allegations concerning the inclusion and exposure of his identification records are made on information and belief.

176. Uber owed a duty to exercise reasonable care in obtaining, maintaining, securing, and controlling access to Tallauze's and Lewis' nonpublic identification information. The duty arises from Uber's own handling of sensitive records and its control over the environment and permissions through which the provider could reach them.

177. The relationship was concrete and bounded by the people whose identification records Uber maintained in the affected environment. Those people could not configure that environment, restrict the provider's credential privileges, or administer Uber's security monitoring. Unauthorized disclosure of sensitive identifying records was a foreseeable consequence of inadequate safeguards for that access.

178. Reasonable care required access restrictions, credential controls, monitoring, and verification appropriate to the information's sensitivity and the purpose of the provider's work. Uber's responsibilities included evaluating the reach of provider access and whether its controls reasonably addressed misuse of valid credentials. The claim concerns those operational duties independently of enforcement of a subscription or driver agreement.

179. On information and belief, Uber breached that duty through the failures described in paragraphs 114 through 123. Its disclosures identify a specific storage environment, provider access mechanism, and monitoring result that support investigation of the controls at issue. The permissions, configurations, and access records will establish the particular failures within Uber's control.

180. Uber's failures were substantial factors in permitting unauthorized access to Tallauze's and Lewis' identification records. Safeguarding those records against misuse of provider credentials was within the purpose of the duties alleged. The intruder's intervention presented the category of foreseeable risk that reasonable data-security controls were intended to address.

181. Tallauze and Lewis suffered unauthorized disclosure and loss of confidentiality of the sensitive information described in paragraphs 106 through 113. They and the Uber Class seek compensatory damages according to proof for legally cognizable injury proximately caused by Uber's conduct, without duplicating recovery against Fireworks or presuming that every member suffered identity theft or incurred the same loss.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request judgment against the Defendant or Defendants responsible for each claim, as follows:

A. Certifying the Fireworks Class, the Notion Class, the Replit Class, and the Uber Class, or appropriate common issues under Federal Rule of Civil Procedure 23; appointing the appropriate named Plaintiffs as representatives; and appointing class counsel under Rule 23(g);

B. Awarding compensatory and consequential damages to the extent authorized by the governing law and established by proof, with appropriate allocation among the responsible Defendants and no double recovery;

C. Granting appropriate equitable relief, if supported by a named Plaintiff's standing and the substantive claim established, concerning any continuing handling or threatened disclosure of that Plaintiff's affected confidential information;

D. Awarding pre-judgment and post-judgment interest as allowed by law;

E. Awarding reasonable attorneys' fees and costs where authorized by applicable law, or from a common fund or other basis properly approved by the Court; and

F. Granting such other and further relief as the Court deems just and proper.

VIII. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38, Plaintiffs demand a trial by jury on all issues so triable.

DATED: November 17, 2026

FROST LLP

By: 

CHRISTOPHER FROST
KEVIN S. DICKER

Nicholas Hall *(Pro Hac Vice Forthcoming)*
HALL ATTORNEYS PC

Ryan Myers *(Pro Hac Vice Forthcoming)*
FEDERMAN & SHERWOOD

Attorneys for Plaintiff and the Proposed Class