IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

ANYSOURCE, INC., d/b/a RUNLAYER, *Plaintiff*, v. PEOPLE CENTER, INC., d/b/a RIPPLING, *Defendant*.	Case No. _____ **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff Anysource, Inc., d/b/a Runlayer, upon knowledge as to itself and upon information and belief as to other matters, alleges the following in support of its Complaint against Defendant People Center, Inc., d/b/a Rippling, for trade secret misappropriation, unfair competition, and breach of contract.

INTRODUCTION

1. Runlayer pioneered one of the earliest Artificial Intelligence ("AI") enablement and governance platforms to deploy, connect, secure, manage, and govern AI agents and related capabilities. Runlayer's integrated platform includes a Model Context Protocol ("MCP") Gateway that enables AI agents to connect securely to tools, data sources, and enterprise applications. Founded by one of the earliest contributors to the enterprise AI ecosystem, Runlayer has invested substantial time and resources since its founding to build a platform that has attracted Fortune 500 customers and approximately $42 million in venture financing, thus positioning Runlayer as an early technical leader in a nascent and rapidly forming market for enterprise AI infrastructure.

2. In 2025, Rippling wanted to explore whether Runlayer's AI enablement and governance platform could support Rippling's internal AI development. Because that evaluation would require Runlayer to disclose closely guarded technical information about the architecture, operation, and future direction of its platform, the parties layered contractual protections around the relationship: an initial Mutual Non-Disclosure Agreement (the "NDA," attached as Exhibit 1), followed six weeks later by a written Anysource Trial Agreement (the "Trial Agreement," attached as Exhibit 2), giving Rippling a limited, evaluation-only license subject to strict use and confidentiality restrictions.

3. What followed was nearly a year of intensive engineering collaboration. In reliance on the parties' agreements, Runlayer disclosed extensive confidential information and trade secrets to Rippling—including Runlayer's source code—concerning the design, operation, implementation, and integration of Runlayer's AI enablement and governance platform. That information was shared with Rippling "solely" to enable Rippling's "evaluation" of Runlayer's platform, remained the property of Runlayer at all times, and was subject to Rippling's express written promises to hold it in "strict confidence," not to use it to "copy" or "create derivative works," and to cease using, return, or destroy any Runlayer information upon termination of the parties' trial arrangement.

4. By all outward indications, the trial was a great success. By May 2026, thousands of Rippling employees were using Runlayer's platform, and the parties were negotiating a longer-term, whole-company license to extend the platform across Rippling's entire enterprise. By early June 2026, however, it became apparent that the parties would not reach an agreement, and Runlayer suspended services to Rippling on June 12, 2026. What Runlayer did not know—and what it would only learn after announcing the suspension—was that, while Runlayer was

collaborating with Rippling and sharing confidential information and trade secrets to facilitate Rippling's evaluation, Rippling was, on information and belief, secretly using that information to build a competing AI enablement and governance platform of its own. A Rippling insider reported that there was "a project internally to build essentially a clone" of Runlayer and that it was "almost a 1 to 1 copy." The evidence further indicates that Rippling has placed an "MCP Gateway" feature in a customer-facing demo environment and may imminently release its competing platform for sale to a wider range of customers.

5. In building a competing product from Runlayer's technology, Rippling has not merely breached the express terms of the parties' agreements. It has misappropriated Runlayer's trade secrets and confidential information in violation of state and federal trade secret and unfair competition law, and it has done so under cover of the very evaluation the parties' agreements were designed to protect.

THE PARTIES

6. Plaintiff Runlayer is a corporation organized under the laws of the State of Delaware with its principal place of business located at 31 Bond Street, New York, New York 10012. As explained above, Runlayer is a specialized AI infrastructure company that pioneered one of the earliest AI enablement and governance platforms designed to solve authentication, authorization, security, governance, and auditability challenges in connection with the deployment of AI agents in enterprise applications.

7. Defendant Rippling is a corporation organized under the laws of the State of Delaware with its principal place of business located at 430 California Street, 11th Floor, San Francisco, California 94104. Rippling operates a workforce management platform for human resources, information technology, finance, payroll, and other enterprise functions.

JURISDICTION AND VENUE

8. This action arises, in part, under 18 U.S.C. § 1836 *et seq*., the Defend Trade Secrets Act ("DTSA"). This Court has subject matter jurisdiction over Runlayer's DTSA claim pursuant to 28 U.S.C. § 1331. This Court also has supplemental jurisdiction over Runlayer's trade secret misappropriation, unfair competition, and breach of contract claims arising under New York state common law pursuant to 28 U.S.C. § 1367(a).

9. This Court has personal jurisdiction over Rippling and venue is proper in this District pursuant to 28 U.S.C. § 1391(b)-(d). Rippling maintains a substantial presence in this District with approximately 500 employees based in its office located at 4 World Trade Center, 150 Greenwich Street, 59th Floor, New York, New York 10007. Moreover, a substantial part of the events giving rise to Runlayer's claims occurred in this District. Runlayer developed the trade secrets at issue at least in part at its principal place of business in this District and continues to maintain and protect them from that principal place of business. On information and belief, hundreds of Rippling personnel working out of Rippling's office in this District used Runlayer's platform, and several of those personnel were members of a private Slack channel through which Runlayer disclosed trade secrets and confidential information to Rippling. Finally, Rippling consented to arbitration seated in this District and governed by New York law.

FACTUAL ALLEGATIONS

A. Runlayer Developed a Unique AI Enablement and Governance Platform.

10. AI agents are rapidly changing how businesses interact with their internal software. Increasingly, AI agents are designed to retrieve information from and take actions inside the enterprise applications employees use every day. But allowing AI agents to reach directly into those systems presents substantial challenges of authentication, authorization, security, governance, and auditability. Many organizations therefore require an intermediary platform to

securely manage those interactions while maintaining centralized control over how AI agents access enterprise resources.

11. Runlayer developed one of the earliest enterprise AI enablement and governance platforms designed to solve those problems. Its platform includes an enterprise MCP gateway: a centralized control plane that sits between AI agents and enterprise software systems and governs how agents are authenticated, what tools they may access, and what actions they may perform. Runlayer's platform applies integrated, real-time security controls, monitors and audits those interactions, and provides granular model- and agent-level usage controls. Runlayer thus enables enterprises to deploy AI capabilities securely, govern their use, and control costs without having to build that infrastructure themselves.

12. Runlayer's founder and CEO Andrew Berman was among the earliest contributors to the enterprise AI ecosystem. By the time the parties began discussing a potential commercial relationship in 2025, Runlayer had established itself as an early technical leader in this space. And since that time, it has grown rapidly, securing multiple Fortune 500 customers and attracting approximately $42 million in funding. Runlayer has invested significant time and resources into research and development, sought intellectual-property protection for various inventions, and treated as proprietary the non-public aspects of its platform, including its source code, implementation know-how, product roadmap, customer-specific designs, and technical materials for deploying, authenticating, governing, securing, and auditing AI-agent access to enterprise systems.

13. The difficulty of building a platform like Runlayer's was later confirmed by Rippling itself. Rippling's Technology Lead for Developer Experience ("DevEx"), Tim Fall,

recounted in a customer research interview in April 2026 that Runlayer was the only vendor he was aware of that had solved the challenges posed by AI enablement and governance.

14. Runlayer operates in a nascent and fast-moving market in which enterprise customers are still deciding which platforms will become the trusted control layer for AI-agent access. In that market, first-mover credibility, customer trust, security reputation, and perceived technical leadership are critical to customer adoption. Runlayer's ability to compete depends not only on the technical value of its platform, but also on its ability to demonstrate to enterprise customers, investors, and strategic partners that Runlayer—not a larger incumbent using Runlayer's confidential work—is the source of the relevant innovation. At Runlayer's current stage of growth, investors' assessment of its technical differentiation and market leadership directly affects its ability to raise capital and the valuation and terms on which that capital is available. A launch by Rippling of a competing platform derived from Runlayer's confidential information and trade secrets would immediately and unjustly threaten Runlayer's position by allowing Rippling to present Runlayer's confidential architecture and implementation know-how as Rippling's own native product capability.

B. In an Attempt to Collaborate, Runlayer Granted Rippling Confidential Access to Its Software and Services on a Trial Basis, Subject to Use and Disclosure Restrictions.

15. Founded in 2016, Rippling had been operating for nearly a decade when the parties' relationship began in 2025 and had grown into an established provider of enterprise HR and workforce-management software with approximately 5,500 employees, a reported valuation of $16.8 billion, and nearly $2 billion in total financing. Runlayer, by contrast, had only five employees at the time. Against that backdrop, Runlayer viewed a potential commercial relationship with Rippling as an opportunity to demonstrate its platform at enterprise scale and strengthen its position in the emerging enterprise AI market.

1. Rippling Began Evaluating Runlayer's Platform Under Strict Confidentiality Protections.

16. Because Rippling's evaluation would require Runlayer to disclose confidential technical information and trade secrets concerning the architecture, implementation, operation, and future development of its platform, the parties layered contractual protections around the relationship, including protections designed to permit evaluation while prohibiting competitive use of Runlayer's proprietary information.

17. The parties first entered into the NDA before any substantive technical collaboration began. The NDA broadly defined "Confidential Information" to include trade secrets and other technical, business, and proprietary information, including software, algorithms, know-how, development work, design specifications, and information relating to each party's current and future products and services. (*See* NDA § 1.) It required each party to maintain such information in strict confidence, limited Rippling's use of Runlayer's Confidential Information only to uses "specifically authorized by the Disclosing Party," and prohibited Rippling from modifying, reverse engineering, or "creat[ing] other works" from Runlayer's platform:

> Each party agrees to hold the other's Confidential Information in strict confidence and not to disclose such Confidential Information to any third party or to use it for any purpose other than as specifically authorized by the Disclosing Party . . . .
>
> Each Party agrees that the software programs of the other Party contain valuable confidential information and each Party agrees that it will not modify, reverse engineer, decompile, create other works from, or disassemble any software programs contained in the Confidential Information of the other Party without the prior written consent of the other Party.

(*Id*. §§ 4, 14.)

18. The NDA further provided that "the obligation to protect the confidentiality of all Confidential Information disclosed by the parties to each other prior to a party's written termination of this Agreement shall survive the termination of the Agreement." (*Id*. § 9.)

19. The NDA also expressly recognized that unauthorized use or disclosure of Runlayer's Confidential Information could cause irreparable harm and warrant immediate injunctive relief:

> The parties acknowledge that the unauthorized disclosure, use, or disposition of Confidential Information could cause irreparable harm and significant injury that may be difficult to ascertain. Accordingly, the parties agree that the Disclosing Party shall have the right to an immediate injunction in the event of any breach of this Agreement.

(*Id*. § 7.)

20. Approximately six weeks later, the parties executed the Trial Agreement. The Trial Agreement gave Rippling a limited, non-exclusive license to deploy and use Runlayer's "Enterprise AI/MCP Gateway (self-hosted) and related support"—a core component of Runlayer's AI enablement and governance platform—during an initial four-month "Trial Period" and "solely for evaluation purposes." (*See* Trial Agreement, Services and Fees; Terms and Conditions, § 1.1.) The Trial Agreement expressly prohibited Rippling from copying, creating derivative works of, or reverse engineering Runlayer's software, and provided that Runlayer retained ownership of the platform and all improvements, enhancements, or modifications:

> During the Trial Period, [Rippling] may access and use the Services solely for evaluation purposes . . . .
>
> [Rippling] will not . . . copy, modify, create derivative works of, or distribute the Services . . . [or] reverse-engineer, disassemble or decompile the Services . . . .
>
> [Runlayer] owns and retains: (i) the Services (and any documentation related thereto), and all improvements, enhancements or modifications made thereto by any party; and (ii) [Runlayer's] name, logo, and other trademarks; and (iii) all intellectual property rights in and to any of the foregoing.

(*Id*., Terms and Conditions, §§ 1.1, 1.3, 3.2.)

21. The Trial Agreement also required that Rippling safeguard Runlayer's Confidential Information, restrict dissemination to representatives with a need to know, and return or destroy

such information upon expiration or termination, with confidentiality obligations surviving termination:

> The receiving party of . . . Confidential Information ("Recipient") shall keep confidential, and ensure its officers, directors, employees, accountants, attorneys, and other confidential advisors of Recipient (collectively, "Representatives") keep confidential, all Confidential Information and shall . . . use Confidential Information only as required to perform its obligations or as otherwise permitted under this Agreement ("Permitted Use"); . . . protect and safeguard Confidential Information to avoid unauthorized disclosure and use . . . . Recipient shall restrict disclosure of Confidential Information solely to those of its Representatives who "need to know" such Confidential Information to perform their responsibilities in connection with the Permitted Use . . . .
>
> Upon the earlier of termination or expiration of this Agreement or a written request by Discloser, Recipient shall, at Discloser's choice, (i) promptly return all Confidential Information . . . or (ii) destroy all of the aforementioned in a manner which preserves its confidentiality, and provide Discloser with a written certification thereof . . . .
>
> Upon termination: (a) access ceases immediately; (b) [Rippling] deletes all Services copies; (c) fees remain due; (d) Confidentiality survives.

(*Id*., Terms and Conditions, §§ 4.2, 4.4, 7.3.)

22. Taken together, the NDA and Trial Agreement reflected the parties' shared understanding of the evaluation they were about to undertake. Rippling could evaluate Runlayer's platform, but Rippling was not purchasing Runlayer's technology or acquiring any right to use Runlayer's Confidential Information or trade secrets to develop competing products. With those protections in place, the parties began what became nearly a year of intensive engineering collaboration.

2. The Trial Encompassed an Extensive Engineering Collaboration.

23. What began as a limited deployment inside Rippling's DevEx and Compute teams grew, over the ensuing months, into an enterprise-wide initiative. As part of this initiative, Runlayer disclosed at least seven categories of trade secrets, including: (i) its application source code, Gateway deployment architecture, topology, and operability; (ii) trade secrets relating to

customer-specific architecture, roadmap sequencing, and product-prioritization decisions; (iii) version-specific implementation materials concerning synchronization, governance, distribution, and custom conversion of internal services into governed MCP-backed capabilities; (iv) trade secrets relating to runtime security controls, including the design, composition, and tuning of its security-scanning and violation-handling systems and related engineering know-how, including negative know-how; (v) trade secrets relating to non-public, version-specific audit and observability implementations for capturing, associating, and evaluating agentic activity within sessions; (vi) trade secrets relating to non-public, version-specific authorization and delegated-identity designs; and (vii) trade secrets relating to its commercial operations and confidential pricing structures.

24. Runlayer's disclosures and implementation support gave Rippling insight into how Runlayer's platform could be deployed efficiently and effectively at enterprise scale.

25. The Trial Agreement contemplated an initial four-month Trial Period, but that period elapsed without Rippling terminating its evaluation, returning Runlayer's software, or converting the relationship into a paid commercial subscription. Instead, the parties continued working together, expanding the technical scope of the trial and negotiating a long-term enterprise deployment. Throughout this period, Rippling continued using Runlayer's platform and soliciting implementation-level assistance, while Runlayer continued providing engineering support, workshops, demonstrations, troubleshooting, and other requested information.

26. The number of Rippling engineers and other personnel using Runlayer's platform steadily increased, and by May 2026, thousands of Rippling employees were using it.

27. Throughout the parties' nearly year-long engineering collaboration, they maintained a shared Slack channel—"#ext-runlayer-rippling"—that grew into a broad

collaborative workspace. Runlayer engineers conducted recurring architecture reviews, security demonstrations, coding sessions, plugin-design meetings, deployment troubleshooting, roadmap discussions, and implementation workshops tailored to Rippling's internal engineering priorities to allow Rippling to confidentially evaluate Runlayer's platform and work toward a long-term agreement to license that platform. But as detailed below, no such license ever came.

3. Rippling Received Runlayer's Trade Secrets.

28. As the relationship progressed, Runlayer invested significant sums in infrastructure for the Rippling pilot and disclosed multiple categories of trade secrets to Rippling—including but not limited to those described below—solely to enable Rippling to evaluate Runlayer's platform, all under the strict confidentiality provisions to which the parties had agreed.

29. *First*, Runlayer disclosed trade secrets relating to its application source code, Gateway deployment architecture, topology, and operability. Runlayer provided Rippling with its complete application source code for Rippling's installation in July and August 2025. Runlayer also disclosed non-public deployment architecture and operational know-how for running its platform inside Rippling's infrastructure, including during a September 25, 2025 check-in call.

30. *Second*, Runlayer disclosed trade secrets relating to customer-specific architecture, roadmap sequencing, and product-prioritization decisions. For example, Runlayer memorialized its customer-specific architecture in a February 16, 2026 "Rippling x Runlayer POC [Proof of Concept] Success Document," which Runlayer shared with Rippling's SVP of Engineering, Gerhard Esterhuizen, and DevEx Technology Lead, Mr. Fall, for review and comment.

31. *Third*, Runlayer disclosed version-specific implementation materials concerning synchronization, governance, distribution, and custom conversion of internal services into governed MCP-backed capabilities. Runlayer provided these trade secrets to Rippling in response to Rippling's requests for help solving its internal plugin and skills distribution problems, including

during a January 28, 2026 "MCP Workshop" presentation attended by Mr. Esterhuizen, a February 4, 2026 Feature Flag Management Plugin call with Mr. Fall (as reflected in contemporaneous Slack messages), a February 20, 2026 meeting with Mr. Esterhuizen, and a March 5, 2026 check-in call.

32. *Fourth*, Runlayer disclosed trade secrets relating to runtime security controls, including the design, composition, and tuning of its security-scanning and violation-handling systems and related engineering know-how, including negative know-how. Those disclosures were made, among other times, during a December 18, 2025 check-in call with Rippling's Engineering Lead, Remy DeWolf; on or about January 15, 2026, through contemporaneous Slack messages and a related discussion with Rippling's security team; on April 29, 2026, when Runlayer Security Engineer Alex Frazer responded to a Slack report from Rippling's Director of Engineering and Infrastructure, Siddharth Palaniswami; and during a May 7, 2026 check-in call.

33. *Fifth*, Runlayer disclosed trade secrets relating to non-public, version-specific audit and observability implementations for capturing, associating, and evaluating agentic activity within sessions. For example, during a May 13, 2026 Slack exchange, a Rippling engineer requested details of Runlayer's solutions in these areas.

34. *Sixth*, Runlayer disclosed non-public, version-specific authorization and delegated-identity designs. Those disclosures were made, among other times, during an April 10, 2026 check-in call with Rippling's Mike Harris, an April 23, 2026 check-in call with Mr. Fall, and a May 7, 2026 check-in call with Rippling Staff Software Engineer Nitish Krishna.

35. *Seventh* and finally, Runlayer disclosed trade secrets relating to its commercial operations and confidential pricing structures. Those disclosures were made, among other times, through a May 6, 2026 pricing proposal sent to Rippling's Head of Procurement, follow-on

pricing-related disclosures on May 14 and May 26, 2026, and a June 10, 2026 communication from Mr. Berman regarding Runlayer's per-account infrastructure costs for the pilot. Rippling also solicited confidential usage data through the shared Slack channel, including in an April 29, 2026 request from Rippling's Vice President of Sales, Paul Barber.

36. Taken together, these disclosures gave Rippling access to Runlayer's non-public source code and concrete implementation details, design choices, operational workflows, credential-boundary decisions, policy mechanisms, security-enforcement logic, audit/export architecture, and roadmap sequencing that went far beyond any generic or public knowledge of MCP, OAuth, AI agents, plugins, skills, audit logs, or enterprise security.

37. The disclosures were all made only to enable Rippling, subject to the parties' strict confidentiality agreements, to evaluate Runlayer's technology for a potential license. These disclosures also reached virtually every level of Rippling's engineering organization, from staff engineers up to the Chief Technology Officer. Runlayer's enterprise AI enablement and governance platform was ultimately deployed—for testing purposes and pursuant to the confidentiality provisions—to thousands of Rippling employees. Access to the underlying confidential technical information and trade secrets disclosed during the trial was more limited. The shared Slack channel included only a limited group of engineering, security, operations, sales, and executive employees, and only that limited group of individuals received Runlayer's most sensitive implementation-level guidance. Members of Rippling's executive management team, including Chief Technology Officer Albert Strasheim and President and Chief Operating Officer Matt MacInnis, also engaged directly with Runlayer regarding its technology.

38. Runlayer derives substantial independent economic value, actual and potential, from the secrecy of these trade secrets. The trade secrets are not generally known or readily

ascertainable through proper means and embody substantial technical development, testing, customer-specific implementation work, and lessons learned. Runlayer offers the resulting capabilities through paid enterprise licenses, and their secrecy supports Runlayer's technical differentiation, pricing, and competitive position. A competitor with access could compress its development timeline, avoid costly dead ends, reproduce Runlayer's non-public architecture and roadmap, tune security and authorization systems using Runlayer's lessons learned, and compete using Runlayer's confidential pricing and commercial information. Rippling's own conduct confirms the information's value to a competitor: after obtaining extensive trial-only access to Runlayer's Confidential Information, Rippling apparently built a near "1 to 1 copy" for potential external sale.

C. Rippling Failed to Negotiate an Enterprise-Wide License and Runlayer Suspended Service as a Result.

39. As the parties' technical collaboration expanded throughout early 2026, they worked in parallel to negotiate a long-term commercial relationship. But during those negotiations, it became clear that Rippling would not pay a market rate for the platform it had spent nearly a year using.

40. Runlayer nevertheless attempted to reach a commercial agreement by offering a whole-company license, at a significant discount from Runlayer's standard pricing, after a similarly discounted earlier engineering-only proposal. Rippling's Procurement team, however, continued to press for substantially lower pricing while seeking to confine any paid subscription to a narrow deployment. The narrowed proposal reflected a growing disconnect between Rippling's engineering organization—which continued to press for broader adoption (and related Confidential Information)—and Rippling's Procurement team. Even as Procurement refused to

pay for the broader platform, Rippling's engineers continued to press Runlayer for non-public guidance on its agent, security, audit, and policy capabilities.

41. On June 10, 2026, after months of negotiations that had gone nowhere, Runlayer informed Rippling's Procurement team that it had reached the limit of the concessions it could make and that, unless Rippling committed to move forward, Runlayer would suspend the pilot. Rippling's Procurement team never responded. Runlayer accordingly suspended service on June 12, 2026.

D. Runlayer Discovered Rippling's Misuse of Its Confidential Information and Trade Secrets.

42. Only after Runlayer announced the suspension did it learn facts indicating why Rippling had refused to consummate a commercial agreement. While Rippling was continuing to solicit and receive Runlayer's Confidential Information, trade secrets, and technical know-how, it was apparently secretly building its own competing enterprise AI enablement and governance platform, including an MCP Gateway.

43. The same day Runlayer suspended service, Runlayer received evidence that Rippling had been misusing Runlayer's Confidential Information and developing its own competing platform. On June 12, a Rippling insider reached out to Mr. Berman by personal text message, writing: "There's some things happening on the Rippling side that you should probably know about but I didn't want to put them in Slack." The insider explained: "There's been a project internally to build essentially a clone o[f] Runlayer. When I raised objections originally I was told it was just for MCP support in Rippling AI, but that seems to have changed and it's being considered for a product at this point." The insider added: "It's not feature complete by any means but it's almost a 1 to 1 copy of Runlayer." Further, the insider indicated that Rippling planned to sell its clone externally to the market as a separate commercial product: "From what I hear it will

even be offered as a stand alone SKU." The insider also apologized: "I'm sorry I couldn't tell you sooner. They kept me out of most of it." Finally, the insider suggested that these decisions were made by Rippling's CEO, Parker Conrad: "it smells like a Parker thing."

44. Since the suspension, Runlayer has identified a series of public Rippling job postings describing some of the same categories of enterprise functionality Runlayer had spent nearly a year disclosing under the parties' contractual agreements, including a Senior Software Engineer, AI Governance role describing a team that sits at the intersection of identity, access control, model routing, MCP security, data protection, spend management, and auditability with the goal of giving companies one governed path for AI usage across employees, agents, models, and business tools; a Product Lead, AI Platform role owning Rippling's skills framework, routing, tool orchestration, and multi-step agent reasoning; and a Senior Staff Software Engineer, Identity role responsible for agent authentication, delegated permissions, and deploying autonomous agents at scale.

45. The post-suspension evidence has continued to mount. It suggests that Rippling is preparing to launch its competing platform imminently and has placed an "MCP Gateway" feature in a customer-facing demo environment.

46. Taken together, this evidence makes it highly likely that Rippling exploited the evaluation-only access Runlayer granted—and the Confidential Information and trade secrets disclosed through that access—to build a near "1 to 1 copy" of Runlayer intended for internal deployment and external commercialization. Rippling's misappropriation of Runlayer's Confidential Information and trade secrets violates state and federal trade secret and unfair competition law, constitutes a material breach of the Trial Agreement, and will imminently and

irreparably harm the value of Runlayer's trade secrets and Confidential Information, market position, goodwill, and bargained-for contractual rights.

47. Rippling's conduct was deliberate, willful, and malicious. Rippling knew that its access was limited to evaluation and that the parties' agreements prohibited use outside that purpose, copying, derivative works, and reverse engineering. On information and belief, members of Rippling's senior engineering leadership who received Runlayer's non-public implementation guidance participated in or supervised the parallel build. While concealing that project, Rippling continued to present itself as a prospective customer and to solicit additional non-public assistance; the project continued even after a Rippling employee raised objections; and Rippling is apparently preparing to offer the resulting competing platform externally. Rippling thus acted to appropriate Runlayer's work and obtain an unfair development head start and to compete unfairly for customers in conscious disregard of Runlayer's rights.

48. Rippling's continued use and threatened launch would cause harms that cannot be fully measured or repaired with money damages. Once Runlayer's non-public design choices and implementation architecture are embodied in a competing customer-facing product, their secrecy and Runlayer's first-mover advantage cannot be restored. A launch by Rippling—a much larger company with an existing enterprise customer base—would allow Rippling to present Runlayer-derived capabilities as its own native offering, eroding Runlayer's customer trust, security reputation, perceived technical leadership, customer pipeline, pricing power, goodwill, and market share. The resulting perceived loss of differentiation also could deter or delay prospective investment, reduce follow-on support from existing investors, depress Runlayer's valuation, force Runlayer to accept financing on less favorable terms, and constrain the capital available to fund growth. Those injuries are inherently difficult to quantify because Runlayer cannot identify every

customer or investor who never engages, every procurement or investment decision that is delayed or abandoned, or the extent to which Rippling's misappropriated head start affects future pricing and financing terms. Those harms also would deprive Runlayer of meaningful arbitral relief and effectively nullify its contractual right to have the dispute resolved, to the extent possible, through arbitration.

49. On information and belief, Rippling has placed an "MCP Gateway" feature of its competing platform in a customer-facing demo environment and may imminently release the platform more broadly before the arbitration can determine whether it was developed using Runlayer's Confidential Information and trade secrets. If that occurs, the secrecy of Runlayer's trade secrets, its market position, and its ability to obtain meaningful arbitral relief will be irretrievably compromised.

50. On July 23, 2026, Runlayer sent a letter to Rippling regarding the termination of the parties' Trial Agreement and asking Rippling to confirm, among other things, that Rippling has not used and is not using Runlayer's Confidential Information and trade secrets in any product development or commercialization, or in any other way inconsistent with the parties' agreements. On July 27, 2026, Rippling acknowledged receipt without responding substantively. Runlayer is filing its Complaint at this time given the importance and urgency of protecting its Confidential Information and trade secrets.

51. Runlayer therefore brings this Action asserting its trade secret misappropriation, unfair competition, and breach of contract claims to preserve its rights and to obtain, among other things, emergency interim relief in aid of arbitration.

COUNT I

Misappropriation of Trade Secrets Under the DTSA (18 U.S.C. § 1836 *et seq.*)

52. Runlayer incorporates each allegation set forth in the preceding Paragraphs 1 through 51.

53. As explained in more detail above, pursuant to, and in reliance on, the parties' NDA and Trial Agreement, Runlayer disclosed to Rippling at least seven categories of trade secrets, including: (i) its application source code, Gateway deployment architecture, topology, and operability; (ii) trade secrets relating to customer-specific architecture, roadmap sequencing, and product-prioritization decisions; (iii) version-specific implementation materials concerning synchronization, governance, distribution, and custom conversion of internal services into governed MCP-backed capabilities; (iv) trade secrets relating to runtime security controls, including the design, composition, and tuning of its security-scanning and violation-handling systems and related engineering know-how, including negative know-how; (v) trade secrets relating to non-public, version-specific audit and observability implementations for capturing, associating, and evaluating agentic activity within sessions; (vi) trade secrets relating to non-public, version-specific authorization and delegated-identity designs; and (vii) trade secrets relating to its commercial operations and confidential pricing structures.

54. Runlayer's trade secrets were not publicly known and Runlayer took extensive measures to preserve their secrecy. Pursuant to the terms of the NDA and Trial Agreement, Runlayer's trade secrets were provided to Rippling solely for its evaluation of Runlayer's AI enablement and governance platform, and Rippling agreed to hold the trade secrets in strict confidence and not to use the trade secrets to copy, create other works from, create derivative works of, modify, reverse engineer, decompile, disassemble, or distribute Runlayer's platform.

(*See* NDA §§ 1, 4, 9, 14; Trial Agreement, Terms and Conditions §§ 1.1, 1.3, 4.2.) Runlayer also disclosed its trade secrets to Rippling through controlled, non-public channels including private recorded check-ins, a joint POC document, targeted engineering demos, and a private shared Slack channel.

55. Runlayer's trade secrets derive substantial independent economic value, actual and potential, from not being generally known or readily ascertainable through proper means. Runlayer invested substantial time and resources to develop and refine them and offers the resulting capabilities through paid enterprise licenses. A competitor with access could compress its development timeline, avoid costly dead ends, reproduce Runlayer's non-public architecture and roadmap, tune security and authorization systems using Runlayer's lessons learned, and compete using Runlayer's confidential pricing and commercial information. Rippling's own conduct confirms that value: after Rippling obtained extensive trial-only access to Runlayer's Confidential Information and trade secrets, Rippling apparently built a near "1 to 1 copy" for potential external sale. Runlayer offers its platform to current and prospective enterprise customers across the United States, and its trade secrets relate to products and services used or intended for use in interstate commerce.

56. Rippling knew or had reason to know that Runlayer's trade secrets had been acquired under circumstances imposing duties to maintain their secrecy and limit their use. In breach of the parties' NDA and Trial Agreement, Rippling knowingly and without Runlayer's consent used those trade secrets to develop a competing platform that a Rippling insider described as a near "1 to 1 copy of Runlayer." Rippling's misappropriation was deliberate, willful, and malicious: Rippling knew that its access was evaluation-only and expressly restricted, yet continued to solicit Runlayer's non-public assistance while concealing a parallel internal build,

continued that project despite an employee's objections, and prepared to commercialize the resulting product, all in conscious disregard of Runlayer's rights. The evidence indicates that Rippling has placed an "MCP Gateway" feature in a customer-facing demo environment and may imminently make its competing platform available for external sale.

57. Rippling's continued use and threatened commercialization will cause immediate and irreparable harm to the secrecy and value of Runlayer's trade secrets, first-mover credibility, customer trust, security reputation, market position, customer pipeline, pricing power, goodwill, fundraising prospects, access to growth capital, and valuation. Once Runlayer's non-public design choices and implementation architecture are embodied in a competing customer-facing product, Runlayer's control over those trade secrets and its competitive position cannot be restored. Those harms cannot be fully quantified because Runlayer cannot identify every customer or investor who never engages, every procurement or investment decision that is delayed or abandoned, or the effect of Rippling's misappropriated head start on future pricing and financing terms. A launch before arbitration also would impair Runlayer's bargained-for right to meaningful arbitral relief. Rippling itself acknowledged in the NDA that "the unauthorized disclosure, use, or disposition of Confidential Information could cause irreparable harm and significant injury" and expressly agreed that Runlayer "shall have the right to an immediate injunction in the event of any breach." (NDA § 7.)

58. Rippling's actions constitute a violation of the DTSA for which Runlayer has no adequate remedy at law. Runlayer is entitled to recover its actual losses, Rippling's unjust enrichment not otherwise included in actual-loss damages, and/or a reasonable royalty, together with exemplary damages and reasonable attorneys' fees based on Rippling's willful and malicious misappropriation. Rippling should also be enjoined from continuing to use, access for business

purposes, disclose, transfer, or otherwise misappropriate Runlayer's trade secrets and from launching, marketing, selling, or otherwise commercializing any product or functionality developed through use of or reference to those trade secrets.

COUNT II

Misappropriation of Trade Secrets Under New York Law

59. Runlayer incorporates each allegation set forth in the preceding Paragraphs 1 through 58.

60. As explained in more detail above, pursuant to, and in reliance on, the parties' NDA and Trial Agreement, Runlayer disclosed to Rippling at least seven categories of trade secrets, including: (i) its application source code, Gateway deployment architecture, topology, and operability; (ii) trade secrets relating to customer-specific architecture, roadmap sequencing, and product-prioritization decisions; (iii) version-specific implementation materials concerning synchronization, governance, distribution, and custom conversion of internal services into governed MCP-backed capabilities; (iv) trade secrets relating to runtime security controls, including the design, composition, and tuning of its security-scanning and violation-handling systems and related engineering know-how, including negative know-how; (v) trade secrets relating to non-public, version-specific audit and observability implementations for capturing, associating, and evaluating agentic activity within sessions; (vi) trade secrets relating to non-public, version-specific authorization and delegated-identity designs; and (vii) trade secrets relating to its commercial operations and confidential pricing structures.

61. Runlayer's trade secrets were not publicly known and Runlayer took extensive measures to preserve their secrecy. Pursuant to the terms of the NDA and Trial Agreement, Runlayer's trade secrets were provided to Rippling solely for its evaluation of Runlayer's AI

enablement and governance platform, and Rippling agreed to hold the trade secrets in strict confidence and not to use the trade secrets to copy, create other works from, create derivative works of, modify, reverse engineer, decompile, disassemble, or distribute Runlayer's platform. (*See* NDA §§ 1, 4, 9, 14; Trial Agreement, Terms and Conditions §§ 1.1, 1.3, 4.2.) Runlayer also disclosed its trade secrets to Rippling through controlled, non-public channels including private recorded check-ins, a joint POC document, targeted engineering demos, and a private shared Slack channel.

62. Runlayer's trade secrets are not generally known or readily ascertainable through proper means and derive substantial independent economic value from their secrecy. Runlayer invested substantial time and resources to develop and refine them and offers the resulting capabilities through paid enterprise licenses. A competitor with access could compress its development timeline, avoid costly dead ends, reproduce Runlayer's non-public architecture and roadmap, tune security and authorization systems using Runlayer's lessons learned, and compete using Runlayer's confidential pricing and commercial information. Rippling's own conduct confirms that value: after Rippling obtained extensive trial-only access to Runlayer's Confidential Information and trade secrets, Rippling apparently built a near "1 to 1 copy" for potential external sale.

63. Rippling knowingly and without Runlayer's consent misappropriated Runlayer's trade secrets to develop a competing platform that a Rippling insider described as a near "1 to 1 copy of Runlayer." That misconduct exceeded a mere failure to perform the parties' contracts: Rippling exploited the parties' confidential relationship and the limited-purpose evaluation process to obtain additional non-public disclosures while, on information and belief, concealing its competitive use of those disclosures. Rippling's conduct was deliberate, willful, wanton, and

undertaken in conscious disregard of Runlayer's rights. The evidence indicates that Rippling has placed an "MCP Gateway" feature in a customer-facing demo environment and may imminently make its competing platform available for external sale.

64. Rippling's continued use and threatened commercialization will cause immediate and irreparable harm to the secrecy and value of Runlayer's trade secrets, first-mover credibility, customer trust, security reputation, market position, customer pipeline, pricing power, goodwill, fundraising prospects, access to growth capital, and valuation. Once Runlayer's non-public design choices and implementation architecture are embodied in a competing customer-facing product, Runlayer's control over its trade secrets and competitive position cannot be restored. Those harms cannot be fully quantified because Runlayer cannot identify every customer or investor who never engages, every procurement or investment decision that is delayed or abandoned, or the effect of Rippling's misappropriated head start on future pricing and financing terms. A launch before arbitration also would impair Runlayer's bargained-for right to meaningful arbitral relief. Rippling itself acknowledged in the NDA that "the unauthorized disclosure, use, or disposition of Confidential Information could cause irreparable harm and significant injury" and expressly agreed that Runlayer "shall have the right to an immediate injunction in the event of any breach." (NDA § 7.)

65. Rippling's actions constitute a violation of New York trade-secret misappropriation law for which Runlayer has no adequate remedy at law. In addition to compensatory and punitive damages where permitted under New York law, Rippling should be enjoined from continuing to use, access for business purposes, disclose, transfer, or otherwise misappropriate Runlayer's trade secrets and from launching, marketing, selling, or otherwise commercializing any product or functionality developed through use of or reference to those trade secrets.

COUNT III

Unfair Competition Under New York Law

66. Runlayer incorporates each allegation set forth in the preceding Paragraphs 1 through 65.

67. As explained in more detail above, pursuant to, and in reliance on, the parties' NDA and Trial Agreement, Runlayer disclosed to Rippling extensive confidential commercial and technical information, including at least seven categories of trade secrets: (i) its application source code, Gateway deployment architecture, topology, and operability; (ii) trade secrets relating to customer-specific architecture, roadmap sequencing, and product-prioritization decisions; (iii) version-specific implementation materials concerning synchronization, governance, distribution, and custom conversion of internal services into governed MCP-backed capabilities; (iv) trade secrets relating to runtime security controls, including the design, composition, and tuning of its security-scanning and violation-handling systems and related engineering know-how, including negative know-how; (v) trade secrets relating to non-public, version-specific audit and observability implementations for capturing, associating, and evaluating agentic activity within sessions; (vi) trade secrets relating to non-public, version-specific authorization and delegated-identity designs; and (vii) trade secrets relating to its commercial operations and confidential pricing structures.

68. Runlayer's trade secrets and Confidential Information were not publicly known and Runlayer took extensive measures to preserve their secrecy and confidentiality. Pursuant to the terms of the NDA and Trial Agreement, Runlayer's trade secrets and Confidential Information were provided to Rippling solely for its evaluation of Runlayer's AI enablement and governance platform, and Rippling agreed to hold the trade secrets and Confidential Information in strict

confidence and not to use the trade secrets and Confidential Information to copy, create other works from, create derivative works of, modify, reverse engineer, decompile, disassemble, or distribute Runlayer's platform. (*See* NDA §§ 1, 4, 9, 14; Trial Agreement, Terms and Conditions §§ 1.1, 1.3, 4.2.) Runlayer also disclosed its trade secrets and Confidential Information to Rippling through controlled, non-public channels including private recorded check-ins, a joint POC document, targeted engineering demos, and a private shared Slack channel.

69. Runlayer's Confidential Information and trade secrets embody the labors, skills, expenditures, and goodwill of Runlayer. Runlayer's trade secrets derive substantial independent economic value from not being generally known or readily ascertainable through proper means, and Runlayer's broader Confidential Information has substantial commercial value because it reflects Runlayer's non-public technical and business work even where a particular item may not independently qualify as a trade secret. A competitor with access to that information could compress its development timeline, avoid costly dead ends, reproduce Runlayer's non-public architecture and roadmap, tune security and authorization systems using Runlayer's lessons learned, and compete using Runlayer's confidential pricing and commercial information. Rippling's own conduct confirms that value: after Rippling obtained extensive trial-only access to Runlayer's Confidential Information and trade secrets, Rippling apparently built a near "1 to 1 copy" for potential external sale.

70. Rippling acted in bad faith when, in breach of the parties' NDA and Trial Agreement, it knowingly misappropriated Runlayer's trade secrets and Confidential Information without Runlayer's consent to build a competing platform that a Rippling insider described as a near "1 to 1 copy of Runlayer" and secure an unfair commercial advantage against Runlayer. Rippling also acted in bad faith by continuing to present itself as a prospective customer,

prolonging the trial relationship, and soliciting additional confidential technical assistance while, on information and belief, it was secretly developing a competing platform for internal use and external commercialization. This misconduct was not merely a failure to perform a contractual promise; Rippling exploited the parties' relationship of trust and the evaluation process as a means of obtaining additional benefits from Runlayer's confidential work while concealing its competing use of that work. Rippling acted deliberately, concealed the competing project, continued it despite internal objections, and proceeded in conscious disregard of Runlayer's rights. The evidence indicates that Rippling has placed an "MCP Gateway" feature in a customer-facing demo environment and may imminently make its competing platform available for external sale.

71. Rippling's continued use and threatened commercialization will cause immediate and irreparable harm to the value of Runlayer's trade secrets and Confidential Information, first-mover credibility, customer trust, security reputation, market position, customer pipeline, pricing power, goodwill, fundraising prospects, access to growth capital, and valuation. Once Runlayer's non-public design choices, implementation architecture, and confidential work are embodied in a competing customer-facing product, the competitive value of that information and Runlayer's market position cannot be restored. Those harms cannot be fully quantified because Runlayer cannot identify every customer or investor who never engages, every procurement or investment decision that is delayed or abandoned, or the effect of Rippling's improper head start on future pricing and financing terms. A launch before arbitration also would impair Runlayer's bargained-for right to meaningful arbitral relief. Rippling itself acknowledged in the NDA that "the unauthorized disclosure, use, or disposition of Confidential Information could cause irreparable harm and significant injury" and expressly agreed that Runlayer "shall have the right to an immediate injunction in the event of any breach." (NDA § 7.)

72. Rippling's actions constitute a violation of New York unfair competition law for which Runlayer has no adequate remedy at law. In addition to being found liable in an amount including compensatory and punitive damages as permitted under New York law, Rippling should be enjoined from continuing to use, access for business purposes, disclose, transfer, or otherwise misappropriate Runlayer's trade secrets and Confidential Information and from launching, marketing, selling, or otherwise commercializing any product or functionality developed through use of or reference to that protected information.

COUNT IV

Breach of Contract Under New York Law

73. Runlayer incorporates each allegation set forth in the preceding Paragraphs 1 through 72.

74. The Trial Agreement is a valid and enforceable contract.

75. Runlayer has fully complied with its obligations under the Trial Agreement at all relevant times.

76. Rippling entered into the Trial Agreement solely for purposes of evaluating Runlayer's AI enablement and governance platform. (*See* Trial Agreement, Terms and Conditions § 1.1.) In signing the Trial Agreement, Rippling agreed to hold any Runlayer trade secrets and Confidential Information provided to it in strict confidence and not to use that information to copy, modify, create derivative works of, distribute, reverse engineer, disassemble, or decompile Runlayer's platform. Rippling also acknowledged that Runlayer retained ownership of the platform and related intellectual property. (*See id.* Terms and Conditions, §§ 1.3, 3.2, 4.2.)

77. As explained in more detail above, pursuant to, and in reliance on, the parties' NDA and Trial Agreement, Runlayer disclosed to Rippling extensive confidential business and technical

information, including at least seven categories of trade secrets: (i) its application source code, Gateway deployment architecture, topology, and operability; (ii) trade secrets relating to customer-specific architecture, roadmap sequencing, and product-prioritization decisions; (iii) version-specific implementation materials concerning synchronization, governance, distribution, and custom conversion of internal services into governed MCP-backed capabilities; (iv) trade secrets relating to runtime security controls, including the design, composition, and tuning of its security-scanning and violation-handling systems and related engineering know-how, including negative know-how; (v) trade secrets relating to non-public, version-specific audit and observability implementations for capturing, associating, and evaluating agentic activity within sessions; (vi) trade secrets relating to non-public, version-specific authorization and delegated-identity designs; and (vii) trade secrets relating to its commercial operations and confidential pricing structures.

78. Rippling has materially breached the Trial Agreement. For example, Rippling has apparently misused Runlayer's Confidential Information, including by using and continuing to use Runlayer's Confidential Information, including trade secrets, for a purpose other than evaluating Runlayer's platform—namely, to develop a competing platform that a Rippling insider described as a near "1 to 1 copy of Runlayer" without Runlayer's consent. The evidence indicates that Rippling has placed an "MCP Gateway" feature in a customer-facing demo environment and may imminently make its competing platform available for external sale. Rippling may also have breached other provisions, including with respect to its handling of Runlayer's Confidential Information.

79. As a direct and proximate result of Rippling's breach of the Trial Agreement, Runlayer has suffered damages, including the loss of the commercial opportunity created by the

trial and the substantial engineering and infrastructure costs Runlayer incurred to support Rippling's evaluation. Runlayer also faces significant and irreparable harm to the value of its trade secrets and Confidential Information, first-mover credibility, customer trust, security reputation, market position, customer pipeline, pricing power, goodwill, fundraising prospects, access to growth capital, valuation, and bargained-for contractual rights. Those harms cannot be fully quantified or repaired after the fact, particularly if Rippling releases a competing customer-facing platform developed through use of or reference to Runlayer's protected information before the parties' arbitration can be completed.[1]

80. Rippling's actions constitute a material breach of the Trial Agreement under New York law for which Runlayer has no adequate remedy at law. In addition to being found liable in an amount including compensatory damages, Rippling should be enjoined from continuing to use, access for business purposes, disclose, transfer, reference, or consult Runlayer's trade secrets and Confidential Information and from launching, marketing, selling, or otherwise commercializing any product or functionality developed through use of or reference to that protected information.

JURY DEMAND

Runlayer requests a jury trial of all issues in this action so triable, including factual issues that form the basis for the requested equitable relief.[2]

[1] Although Runlayer is not currently asserting claims for breach of the NDA against Rippling in this action, Rippling itself acknowledged in the NDA that "the unauthorized disclosure, use, or disposition of Confidential Information could cause irreparable harm and significant injury" and expressly agreed that Runlayer "shall have the right to an immediate injunction in the event of any breach." (NDA § 7.)

[2] Runlayer is initiating arbitration with the American Arbitration Association in New York, New York. Runlayer files this Complaint to preserve its claims and to seek expedited discovery and a preliminary injunction in aid of arbitration. Runlayer seeks a jury trial and the remaining relief described herein to the extent needed based on the scope and/or outcome of the arbitration.

PRAYER FOR RELIEF

WHEREFORE, Runlayer respectfully requests that this Court enter an order:

A. Preliminarily enjoining Rippling from (i) designing, developing, using, marketing, selling, offering to sell, transferring, or otherwise commercializing any product or functionality designed or developed using or with reference to Runlayer's Confidential Information or trade secrets, and (ii) disclosing, using, referencing, or otherwise consulting any of Runlayer's trade secrets, Confidential Information, non-public proprietary materials, or other non-public technical know-how during the pendency of arbitration between the parties;

B. Granting Runlayer expedited discovery concerning Rippling's use of Runlayer's trade secrets and Confidential Information and Rippling's design, development, use, marketing, sale, offer to sell, transfer, or commercialization of any product or functionality designed or developed using or with reference to Runlayer's Confidential Information or trade secrets, in support of Runlayer's forthcoming request for a preliminary injunction;

C. Permanently enjoining Rippling from (i) designing, developing, using, marketing, selling, offering to sell, transferring, or otherwise commercializing any product or functionality designed or developed using or with reference to Runlayer's Confidential Information or trade secrets, and (ii) disclosing, using, referencing, or otherwise consulting any of Runlayer's trade secrets, Confidential Information, non-public proprietary materials, or other non-public technical know-how;

D. Awarding Runlayer damages in a sum to be determined at trial, as permitted under the DTSA and New York law;

E. Awarding Runlayer punitive and/or exemplary damages, as permitted under the DTSA and New York law;

F. Awarding Runlayer pre- and post-judgment interest at the maximum legal rate on all sums awarded, as permitted under the DTSA and New York law;

G. Awarding Runlayer its reasonable attorneys' fees, costs, and disbursements incurred in this action, as permitted under the DTSA and New York law; and

H. Granting Runlayer such further and other relief as the Court deems just and appropriate.

Dated: July 28, 2026

Respectfully submitted,

/s/ Alexander N. Gross
Alexander N. Gross
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, NY 10004
Telephone: (212) 558-4000
Facsimile: (212) 558-3588
grossa@sullcrom.com

Andrei Iancu (*pro hac vice forthcoming*)
Amy E. Proctor (*pro hac vice forthcoming*)
Avalee Statner (*pro hac vice forthcoming*)
SULLIVAN & CROMWELL LLP
1888 Century Park East
Los Angeles, CA 90067
Telephone: (310) 712-6600
Facsimile: (310) 712-8800
iancua@sullcrom.com
proctora@sullcrom.com
statnera@sullcrom.com

Counsel for Plaintiff Anysource, Inc., d/b/a Runlayer