HUESTON HENNIGAN LLP
Moez M. Kaba (SBN 257456)
mkaba@hueston.com
Christine Woodin (SBN 295023)
cwoodin@hueston.com
Hagan Scotten (*Pro Hac Vice Pending)*
hscotten@hueston.com
Billy Joe McLain (SBN 290682)
523 West 6th Street, Suite 400
Los Angeles, CA 90014
Telephone: (213) 788-4340
Facsimile: (888) 866-4825

Attorneys for Plaintiff
AMAZON.COM SERVICES LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

AMAZON.COM SERVICES LLC, a Delaware limited liability company,

Plaintiff,

v.

PERPLEXITY AI, INC., a Delaware corporation.

Defendant.

Case No.:

COMPLAINT FOR:

(1) VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT; AND

(2) VIOLATIONS OF THE CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT

DEMAND FOR JURY TRIAL

Plaintiff Amazon.com Services LLC ("Amazon") alleges as follows:

INTRODUCTION

1. Amazon brings this action to stop Perplexity AI, Inc.'s ("Perplexity" or "Defendant") persistent, covert, and unauthorized access into Amazon's protected computer systems in violation of federal and California computer fraud and abuse statutes. This case is not about stifling innovation; it is about unauthorized access and trespass. It is about a company that, after repeated notice, chose to disguise an automated "agentic" browser as a human user, to evade Amazon's technological barriers, and to access private customer accounts without Amazon's permission. Amazon's request is straightforward: Perplexity must be transparent when deploying its artificial intelligence ("AI") agent on Amazon.com (the "Amazon Store") and it must respect Amazon's right to limit the activity of Perplexity's AI agent in private customer accounts. No different than any other intruder, Perplexity is not allowed to go where it has been expressly told it cannot; that Perplexity's trespass involves code rather than a lockpick makes it no less unlawful. Perplexity's misconduct must end.

2. Amazon operates the Amazon Store, an online store serving hundreds of millions of customers. The Amazon Store is more than a catalog of webpages: it is an integrated, dynamic environment that provides Amazon customers with a secure, curated, and individualized shopping experience. To enable Amazon to provide the best customer experience, Amazon customers must register for an account using unique login credentials. After doing so, they can manage and track their orders, review their order history, receive personalized recommendations, store credit cards and delivery addresses, and process returns, among other things. To protect the Amazon Store and its customers' private information, and preserve customer trust, Amazon invests heavily in technical and organizational safeguards including numerous cybersecurity measures.

3. Perplexity operates AI-based products and services, including an application called Comet that includes "agentic AI" functionality. Unlike more familiar AI tools, which generate text or provide information in response to prompts from users, AI agents can, among other things, plan and carry out multi-step tasks for a user with little input. In practice, these AI tools can independently interact with third-party websites, use stored credentials, and perform actions on the

users' behalf—executing sequences that resemble a human-controlled browser session even when no human is actively clicking. Relevant here, Comet allows users to browse the internet and use the Comet AI agent to independently perform actions on users' behalf, including interacting with and placing orders in the Amazon Store through their private customer accounts.

4. Because agentic AI tools like Comet can act within protected computer systems, including private customer accounts requiring a password, they present risks to Amazon's customers and the Amazon Store. Amazon reasonably requires automated AI agents—that is, AI tools (like Comet) that access Amazon's Store and private account information on behalf of registered Amazon customers—to transparently identify themselves. This is necessary for Amazon to, among other things, ensure the AI agents do not pose risks to Amazon's customers in the Amazon Store. Amazon has communicated these requirements directly to companies operating AI agents, including Perplexity. Such transparent identification of AI agents is also required under Amazon's Conditions of Use, which are publicly available to everyone. These requirements protect Amazon's right to know and control who is accessing its private servers and are integral to Amazon's ability to protect its customer's data.

5. Rather than be transparent, Perplexity has purposely configured its Comet AI software to not identify the Comet AI agent's activities in the Amazon Store: Perplexity falsely identifies its Comet AI agent activity as coming from Google Chrome, which is a separate, widely used web browser owned by Google. As a result, Perplexity's Comet AI agent covertly poses as a human customer shopping in the Amazon Store on a Google Chrome browser.

6. Perplexity creates considerable risks to Amazon's customers when it deploys its unauthorized and covert AI agent into the Amazon Store's private customer accounts. As just one example, Perplexity's Comet browser and AI agent are vulnerable to attacks from cyber criminals. These cyber criminals can exploit Perplexity's cybersecurity failures and leverage the Comet AI agent to compromise personal and private data from Amazon's customers who use the Comet AI agent. It has been publicly reported that cyber criminals and other bad actors can "hijack[] the AI

assistant embedded in the browser to steal data."[1] Comet's vulnerabilities place the private data of Amazon customers who use the Comet AI agent, and by extension, Amazon's hard-won customer trust, at risk.

7. Beyond security risks to Amazon's customers, Perplexity's Comet AI agent has degraded Amazon customers' shopping experience and interfered with Amazon's ability to ensure customers who use the Comet AI agent receive the benefits of the individualized shopping experience that Amazon has spent decades curating.

8. Since November 19, 2024, Amazon has told Perplexity's executives on at least five separate occasions that its AI agents may not covertly access the Amazon Store. First Perplexity agreed, then went back on its word. Next, after Amazon detected the Comet AI agent covertly accessing private customer accounts and told Perplexity to stop, Perplexity claimed that Comet AI was not agentic when its own marketing materials admit otherwise. Amazon then set up a technological barrier to restrict the Comet AI agent from covertly accessing private customer accounts. In response, Perplexity released a Comet software update specifically designed so that the Comet AI agent could evade that technological barrier. And when Amazon again addressed Perplexity's unauthorized conduct with Perplexity on two separate occasions, Perplexity refused to stop. Perplexity's CEO understood that Perplexity was deliberately flouting Amazon's rules, but had no legitimate justification for why Perplexity would not act honestly and transparently. Finally, on October 31, 2025, Amazon sent a cease-and-desist letter to Perplexity reiterating Amazon's prohibition against Perplexity using AI agents to covertly access Amazon's private customer accounts.

9. Perplexity's pattern is clear: when confronted, it denies; when blocked, it evades; and when warned, it persists. The law does not require Amazon to tolerate a concealed, automated actor that refuses to identify itself, gains unauthorized access to private customer accounts, and defeats access controls to continue to do so. Amazon, through this lawsuit, seeks to immediately stop Perplexity from its continuing injurious actions, from which Amazon has suffered irreparable

[1] Ex. 1, Ravie Lakshmanan, *CometJacking: One Click Can Turn Perplexity's Comet AI Browser Into a Data Thief*, The Hacker News (Oct. 4, 2025), https://thehackernews.com/2025/10/cometjacking-one-click-can-turn.html.

harm, and which will continue unless Defendant is enjoined from further trespass into Amazon's protected servers.

PARTIES

10. Plaintiff Amazon is a Delaware limited liability company.

11. Defendant Perplexity is a Delaware corporation with its principal place of business in San Francisco, California.

JURISDICTION AND VENUE

12. This Court has federal question jurisdiction over the violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) alleged in this Complaint pursuant to 28 U.S.C. § 1331.

13. The Court has supplemental jurisdiction over the violation of the California Comprehensive Computer Data Access and Fraud Act (California Penal Code § 502) pursuant to 28 U.S.C. § 1367 because this claim arises out of the same nucleus of operative facts as Amazon's federal claim.

14. This Court has personal jurisdiction over Defendant because Defendant's headquarters and principal place of business are in San Francisco.

15. Venue is proper under 28 U.S.C. § 1391(b)(1) because Defendant resides in San Francisco. Venue is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Amazon's claims occurred in San Francisco.

16. The California Penal Code § 502 creates a private civil cause of action. Jurisdiction and venue are also proper in this Court under California Penal Code 502(j), which states: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

BACKGROUND

I. Background on the Amazon Store

17. Amazon owns and operates the Amazon Store, which is an online store accessible in the United States at www.amazon.com. Through the Amazon Store, customers can browse,

select, and purchase a wide variety of products and services. From its inception as an online bookstore, the Amazon Store has built its business around a simple principle: putting customers first. This customer-centric focus has allowed the Amazon Store to consistently deliver for its customers.

18. Over decades, Amazon has developed a distinctive shopping experience in the Amazon Store for each individual customer. That shopping experience is designed to help customers find and discover products that cater to their needs based on key elements, including reviews, price, availability, delivery speed, measures of post-purchase satisfaction like return rates, and each customer's browsing and shopping history.

19. To access that individualized shopping experience, customers must register a private account in the Amazon Store secured with unique login credentials. Within each private account, customers can, among other things, manage and track their orders; save items for later purchases; receive personalized recommendations; store payment, personal address and contact information; and receive updates regarding their purchases.

20. Amazon employs a range of cybersecurity measures—including encryption, multi-factor authentication options, and suspicious activity monitoring—to protect the data in customers' private accounts. These cybersecurity measures place Amazon among the best major providers at protecting customer information.

II. The Amazon Store's Conditions of Use

21. All activities in the Amazon Store and use of related Amazon services and products are governed by the Amazon Store's Conditions of Use.[2]

22. On May 30, 2025, Amazon updated the Amazon Store's Conditions of Use to add a dedicated section on AI Agents ("Agent Terms"). The Agent Terms require that AI agent providers like Defendant clearly identify AI agents and refrain from any actions to conceal or obscure agentic activities. They also explain that Amazon limits AI agents' access to the Amazon Store and requires AI agent providers to abide by such limits.

[2] Ex. 2, *Conditions of Use*, Amazon (May 30, 2025), https://www.amazon.com/gp/help/customer/display.html?nodeId=GLSBYFE9MGKKQXXM.

23. Among other things, the Conditions of Use include the following provisions:

> **LICENSE AND ACCESS**
>
> Subject to your compliance with these Conditions of Use and any Service Terms, and your payment of any applicable fees, Amazon or its content providers grant you a limited, non-exclusive, non-transferable, non-sublicensable license to access and make personal and non-commercial use of the Amazon Services. This license does not include any resale or commercial use of any Amazon Service, or its contents; any collection and use of any product listings, descriptions, or prices; any derivative use of any Amazon Service or its contents; any downloading, copying, or other use of account information for the benefit of any third party; or any use of data mining, robots, or similar data gathering and extraction tools. . . . No Amazon Service, nor any part of any Amazon Service or its contents, may be reproduced, duplicated, copied, sold, resold, visited, or otherwise exploited for any commercial purpose without express written consent of Amazon. . . . You may not frame or utilize framing techniques to enclose any trademark, logo, or other proprietary information (including images, text, page layout, or form) of Amazon without express written consent. . . . You may use the Amazon Services only as permitted by law. The licenses granted by Amazon terminate if you do not comply with these Conditions of Use or any Service Terms.
>
> . . .
>
> **ADDITIONAL AMAZON SOFTWARE TERMS**
>
> The following terms ("Software Terms") apply to any software (including any updates or upgrades to the software) and any related documentation we make available to you in connection with Amazon Services (the "Amazon Software").
>
> 1. **Use of the Amazon Software**. You may use Amazon Software solely for purposes of enabling you to use the Amazon Services as provided by Amazon, and as permitted by these Conditions of Use and any Service Terms. You may not incorporate any portion of the Amazon Software into other programs or compile any portion of it in combination with other programs, or otherwise copy (except to exercise rights granted in this section), modify, create derivative works of, distribute, assign any rights to, or license the Amazon Software in whole or in part. All software used in any Amazon Service is the property of Amazon or its software suppliers and is protected by United States and international copyright laws.
>
> . . .

3. **No Reverse Engineering**. You may not reverse engineer, decompile or disassemble, tamper with, apply any other process or procedure to derive the source code or other underlying components (such as a model, model parameters, or model weights), or bypass any security associated with the Amazon Software, whether in whole or in part.

. . .

AGENTS

The terms in this section ("Agent Terms") apply if you use, allow, enable, or cause the deployment of an Agent to access, use, or interact with any Amazon Services. For the purposes of these Agent Terms, "Agent" means any software or service that takes autonomous or semi-autonomous action on behalf of, or at the instruction of, any person or entity.

1. **Transparency and Consent**. No Agent may access, use, or interact with Amazon Services unless, at all times, it identifies itself and operates in strict accordance with the requirements in section 3 of these Agent Terms. In addition, no Agent may access, use, or interact with Amazon Services if we have requested that the Agent refrain from accessing, using, or interacting with any Amazon Service.
2. **Limitation on Access**. At our sole discretion, we may limit, including by technical measures, whether and how any Agent accesses, uses, and interacts with Amazon Services.
3. **Technical Requirements**. Agents must:
    i. In all HTTP/HTTPS requests, identify that the request is from an Agent and disclose the name of the Agent by including the following in the request's user agent string:
    "Agent/[agent name]" (e.g., Agent/AmazonAgent)
    ii. Not conceal or obfuscate that any access, use, or interactions are from an Agent, such as by (a) mimicking the speed or pattern of human keystrokes, page navigation, or other interactions or (b) completing or circumventing CAPTCHAs or other measures intended to distinguish computers from humans.
    iii. Respond truthfully to any question or prompt seeking to determine if interactions are coming from a human or a computer.
    iv. Not circumvent or otherwise avoid any measure intended to block, limit, modify, or control whether

and how Agents access, use, or interact with an Amazon Service.

III. Background on Defendant and the Comet Browser

24. Defendant is a technology company founded in 2022.

25. Defendant develops and operates AI-based products and services, including a web browser application called Comet that Defendant first released to paying subscribers on July 9, 2025. Comet allows users to browse the internet and use Defendant's AI tools, including the Comet AI agent. Comet users can ask the Comet AI agent to independently perform actions on users' behalf, such as placing an order in the Amazon Store. On October 2, 2025, Defendant made the Comet browser and agent widely available to the public for free.

IV. Defendant's Covert and Unauthorized Access into the Amazon Store

26. Since at least November 2024, Defendant has repeatedly and deliberately gained unauthorized access to the Amazon Store.

A. Defendant Fraudulently Sets Up Amazon Prime Accounts to Facilitate its "Buy with Pro" Feature

27. In November 2024, Defendant launched its "Buy with Pro" feature, allowing its paying subscribers to ask Defendant to make purchases on third-party websites on their behalf, while promising to provide free shipping "as a thank-you for shopping with [Defendant]."[3] Defendant marketed the "Buy with Pro" function as powered by agentic AI.

28. Defendant used Amazon accounts, including Amazon Prime accounts, to facilitate "Buy with Pro." When Defendant's paying subscribers used the "Buy with Pro" feature in the Amazon Store, Defendant would place orders using Defendant's Amazon accounts, including its Amazon Prime accounts, thereby allowing some of those subscribers to make purchases and receive Prime benefits, such as free shipping, without having to create their own Amazon accounts or pay for Prime.

29. Defendant's "Buy with Pro" feature risked interfering with Amazon's customer relationships and potentially deprived Amazon of revenue by giving third parties Prime's benefits

[3] Ex. 3, *Shop like a Pro: Perplexity's new AI-powered shopping assistant*, Perplexity (Nov. 18, 2024), https://www.perplexity.ai/hub/blog/shop-like-a-pro.

even though those third parties may not have had Prime memberships. In addition, because users of Defendant's "Buy with Pro" feature did not transact using their own Amazon accounts, this created the risk that they would be unable to access all features of the Amazon Store. For example, they may not have received Amazon's timely updates about their orders and may have experienced difficulties with returns and exchanges through Amazon because they were not interacting directly with the Amazon Store.

30. On November 19, 2024, Amazon discovered Defendant's misuse of Prime memberships.

B. Amazon Informs Defendant that Access to the Amazon Store through "Buy with Pro" is Unauthorized

31. On November 19, 2024, Amazon contacted and informed Defendant that its use of Amazon Prime accounts violated the terms and conditions for Amazon Prime, which forbid Prime members from "purchas[ing] products for the purpose of resale, rental, or to ship to their customers or potential customers using Prime benefits."[4] Amazon also advised Defendant—given Defendant's advertising of "Buy with Pro" as an AI-powered shopping assistant—that it did not have permission to deploy any AI agents in the Amazon Store. In response, Defendant agreed that it would halt the deployment of AI agents in the Amazon Store unless Amazon and Defendant reached mutually agreed-upon terms for such deployment.

C. Defendant Deploys its AI Agent in the Amazon Store through Private Customer Accounts

32. On July 9, 2025, Defendant released Comet, a web browser application, to its paying subscribers. Without prior notice to Amazon, and without authorization, Defendant deployed its Comet AI agent in the Amazon Store through private Amazon customer accounts, in contravention of Defendant's prior agreement not to deploy AI agents in the Amazon Store without Amazon's consent to mutually-agreed terms.

33. Within a Comet browser session, the Comet AI agent can perform numerous tasks

[4] Ex. 4, *Amazon Prime Terms & Conditions*, Amazon (May 11, 2021), https://www.amazon.com/gp/help/customer/display.html?nodeId=G2B9L3YR7LR8J4XP.

in response to user prompts. To deploy the Comet AI agent to make purchases in the Amazon Store, the Comet AI agent directs users to the Amazon Store's sign-in page and instructs them to log into their Amazon accounts (if the user has not already logged in). Once a user is logged in, no further human action is required in the Amazon Store: the Comet AI agent has access to the user's private account information (that the Comet AI agent transmits back to Perplexity's servers for processing), the Comet AI agent will add items to the user's shopping cart, make purchases, and take other agentic actions in the Amazon Store on the user's behalf, all without the user having to make another click in the Amazon Store.

34. Defendant does not identify the Comet AI agent deployed in the Comet browser sessions, but rather conceals its agentic activities. When the Comet AI agent accesses the Amazon Store, it does not use a unique browser identifier and instead transmits the same "user-agent" string that is used by Google Chrome. A "user-agent" string is a standard piece of information sent by a web browser to identify itself to a third-party website.

35. It is considered responsible practice on the web to use a user-agent string that distinguishes requests initiated by an AI agent from requests resulting directly from human action. Unlike Comet, other web browsers with agentic AI capabilities use unique user-agent strings to identify both the browser identity and whether browsing activity is being conducted by an AI agent. Thus, by using the same user-agent string as Google Chrome, the Comet AI agent makes it deceptively appear that a human user is visiting the Amazon Store using the Google Chrome browser.

36. Defendant's covert deployment of the Comet AI agent into the Amazon Store through private customer accounts violates Amazon's License and Access Terms, the Amazon Software Terms, and the Agent Terms, as well as Amazon's prior request, to which Defendant agreed, that Defendant refrain from deploying covert AI agents in the Amazon Store.

D. Amazon Informs Defendant that Comet's Agentic Access Is Unauthorized and Implements a Technological Barrier, which Defendant Evades

37. On August 4, 2025, shortly after Amazon detected Defendant's renewed and unauthorized deployment of the Comet AI agent in the Amazon Store, Amazon contacted

Defendant's CBO, Mr. Shevelenko, and explained that Amazon requires all AI agents to act transparently in the Amazon Store and that Defendant was not permitted to deploy the Comet AI agent in the Amazon Store. Mr. Shevelenko falsely asserted that Comet was not "agentic," contradicting Perplexity's public marketing materials touting Comet's agentic AI functions, including the ability to "actively conduct[] entire browsing sessions," "book[ing] a meeting or send[ing] an email," "buy[ing] something you forgot," and "execut[ing] complete workflows while keeping perfect context." Ex. 5, Perplexity Team, *Introducing Comet*, Perplexity (July 9, 2025), https://www.perplexity.ai/hub/blog/introducing-comet.

38. Following Defendant's covert and unauthorized access, numerous Amazon software engineers and other highly skilled employees spent significant time conducting a forensic analysis of network traffic and browser data to isolate the Comet AI agent's browser fingerprint from ordinary customer activities. On August 19, 2025, after dedicating substantial resources to tracking and identifying the activities of Defendant's covert AI agent in the Amazon Store and in Amazon's servers, Amazon implemented a technological barrier to restrict the Comet AI agent's ability to access Amazon's private customer accounts.

39. Within 24 hours of Amazon implementing a technological barrier to protect Amazon's private customer accounts from Defendant's unauthorized access, Defendant released an updated version of Comet designed to evade the barrier by altering Comet's behavior so that the Comet AI agent no longer matched the digital fingerprint Amazon had developed to identify it. This software update allowed Defendant to again obtain unauthorized agentic access to Amazon's private customer accounts. Comet's bypassing of Amazon's technological barrier also independently violates the Conditions of Use, which are published and available to everyone accessing the Amazon Store.

E. Amazon Again Informs Defendant that Comet's Agentic Access Is Unauthorized, and Defendant Again Continued to Access Private Customer Accounts in the Amazon Store Without Authorization

40. After Defendant's swift evasion of Amazon's technological barrier, Amazon twice confronted Defendant about its unauthorized access into the Amazon Store.

41. On September 12, 2025, Amazon contacted Defendant's CEO, Mr. Srinivas, and explained that the Comet AI agent is not authorized to access the Amazon Store. Amazon made it clear that if Defendant continues to access the Amazon Store by not identifying the Comet AI agent, legal action would likely follow. Mr. Srinivas did not deny that Comet AI was accessing the Amazon Store without identifying itself.

42. And on September 29, 2025, Amazon contacted Defendant's CEO, Mr. Srinivas, as well as its CBO, Mr. Shevelenko, and explained that the Comet AI agent is not authorized to access the Amazon Store without transparently identifying itself. Mr. Srinivas and Mr. Shevelenko offered no legitimate justification for Defendant's unauthorized conduct. After this call, Defendant's Comet AI agent continued to impersonate Google Chrome and fail to identify itself when accessing the Amazon Store through private customer accounts.

43. On October 2, 2025, Defendant made Comet widely available to the public for free.[5]

F. Amazon Sends a Cease-and-Desist Letter to Defendant, but Defendant Refuses to Change Course

44. On October 31, 2025, Amazon sent Defendant a cease-and-desist letter, reaffirming that Defendant is not authorized to covertly deploy AI agents in the Amazon Store and that Amazon would seek all available legal and equitable remedies if this conduct did not stop.[6]

V. Defendant's Conduct Has Caused Irreparable Harm to Amazon

45. Amazon is entitled to control access to the Amazon Store's private user accounts and private customer data. Defendant's continual covert and unauthorized access into the Amazon Store through private customer accounts irreparably harms Amazon.

46. Under Amazon's Conditions of Use, the License and Access Terms prohibit the downloading, copying, or use of account information for a third party's—like Perplexity's—benefit and the use of data mining, robots, or similar data gathering and extraction tools; the Amazon Software Terms prohibit bypassing any technological measures associated with Amazon Software; and the Agent Terms expressly require AI agents to transparently identify themselves when they

[5] Ex. 6, *The Internet is Better on Comet*, Perplexity (Oct. 2, 2025), https://www.perplexity.ai/hub/blog/comet-is-now-available-to-everyone-worldwide.
[6] Ex. 7, Amazon's Cease and Desist Letter to Perplexity (Oct. 31, 2025).

operate within the Amazon Store and to comply with any request by Amazon that they refrain from accessing the Store. The Agent Terms also prohibit AI agents from circumventing any measure intended to block, limit, or control whether and how they access the Store. Amazon has expressly and repeatedly put Defendant on notice of all these Conditions of Use.

47. Amazon has directly asked Defendant on at least four separate occasions—on November 19, 2024, August 4, 2025, September 12, 2025, and September 29, 2025—to stop its covert and unauthorized access into Amazon's Store. Yet Defendant has not ceased its illegal conduct.

48. In response to Defendant's refusal to comply with Amazon's requests that it not trespass into Amazon's protected computers, Amazon implemented a technological barrier on August 19, 2025 to restrict Comet's agentic access to the Amazon Store through private customer accounts. But Defendant evaded Amazon's technological barrier to continue accessing the Amazon Store through private customer accounts without identifying its browser or agentic activity.

49. Amazon also sent a cease-and-desist letter on October 31, 2025, unequivocally revoking Defendant's access to the Amazon Store when using covert AI agents, and threatening legal action.

50. To date, Defendant has not heeded any of Amazon's attempts to maintain control of the Amazon Store and its private customer accounts. Rather, Defendant has continually and without authorization obtained access to all data available in the private Amazon Store accounts of Amazon customers who use the Comet AI agent in the Amazon Store, including those users' account details, shopping history, billing information, and other personal and financial data. Defendant's continuous bad-faith conduct indicates that its violations will stop only when a Court intervenes and enjoins Defendant from further unauthorized access to the Amazon Store through private customer accounts.

51. Amazon's harms are increased by Comet's well-documented security vulnerabilities and the danger those vulnerabilities create for Amazon customers who use the Comet AI agent to access their private accounts in the Amazon Store. Defendant's Terms of Use and Privacy Notice grant it sweeping rights to collect passwords, security keys, payment methods, shopping histories,

and other sensitive data from customers when they use Comet to access the Amazon Store or other third-party websites, while at the same time disclaiming any responsibility for data security.[7]

52. This is troubling because Comet is reported to be uniquely vulnerable to security attacks, including the ability for malicious attackers to use the Comet AI agent to "siphon sensitive data . . . from connected services" like the Amazon Store.[8] Indeed, Defendant's Comet browser is vulnerable to "even the oldest tricks in the scammer's playbook," including "scan[ning] an obvious phishing email, visit[ing] the malicious website, and prompt[ing] its user for their banking account credentials without any indication that something might be amiss."[9]

53. Defendant's unauthorized access and illegal conduct increase the risk that the private account data of Amazon customers who use the Comet AI agent to access the Amazon Store will be targeted for data theft and stolen by cyber criminals. This is particularly concerning because Defendant is intentionally evading Amazon's identification of the Comet AI agent when it accesses the Amazon Store through private customer accounts, and thereby directly interfering with Amazon's ability to protect the data of Amazon's customers who use the Comet AI agent to access the Amazon Store.

54. After an Amazon customer experiences fraud or a takeover issue with their account, it is too late. Amazon will also suffer great reputational harm, a loss of customers as well as customer trust, and a loss of goodwill regardless of the fact that any such customer harm will be entirely attributable to the illegal conduct of Defendant and its refusal to heed Amazon's repeated requests that it conduct agentic AI activities with transparency.

55. Lastly, Defendant's misconduct further harms Amazon's reputation and goodwill

[7] *See* Ex. 8, *Comet Privacy Notice*, Perplexity (Jul. 8, 2025), https://www.perplexity.ai/hub/legal/comet-privacy-notice; Ex. 9, *Perplexity's Privacy Policy*, Perplexity (Feb. 2, 2025), https://www.perplexity.ai/hub/legal/privacy-policy.

[8] Ex. 1, Ravie Lakshmanan, *CometJacking: One Click Can Turn Perplexity's Comet AI Browser Into a Data Thief*, The Hacker News (Oct. 4, 2025), https://thehackernews.com/2025/10/cometjacking-one-click-can-turn.html.

[9] Ex. 10, Nathaniel Mott, *Perplexity's AI-Powered Comet Browser Leaves Users Vulnerable to Phishing Scams and Malicious Code Injection — Brave and Guardio's Security Audits Call Out Paid AI Browser*, Tom's Hardware (Aug. 25, 2025), https://www.tomshardware.com/tech-industry/cyber-security/perplexitys-ai-powered-comet-browser-leaves-users-vulnerable-to-phishing-scams-and-malicious-code-injection-brave-and-guardios-security-audits-call-out-paid-ai-browser.

by misappropriating Amazon's services, degrading the shopping experience on the Amazon Store, and disrupting Amazon's customer relationships. Amazon has invested decades of time and resources into creating a curated, individualized shopping experience on the Amazon Store. The Comet AI agent prevents Amazon from controlling access to the Amazon Store and, therefore, the quality of the Amazon shopping experience for its customers. When the Comet AI agent shops and makes purchases from the Amazon Store through private customer accounts, it may not select the best price, delivery method, or product for the customer. The Comet AI agent also may not add products to existing deliveries to meet minimum free-shipping thresholds, which, if done, could result in cheaper and/or faster delivery options for customers. Thus, Defendant's agentic activity within the Amazon Store harms Amazon's business reputation and customer goodwill.

56. When customers who use the Comet AI agent cannot trust that their personal account information is secure, or when they suffer from a degraded shopping experience, their confidence in the Amazon brand is diminished. Perplexity's interference with Amazon's ability to offer a secure and positive customer experience, and the corresponding erosion in customer trust, is a quintessential irreparable harm.

VI. Defendant's Covert and Unauthorized Access into the Amazon Store Has Caused Significant Economic and Technological Harm to Amazon

57. Amazon has also suffered economic and technological damages well in excess of $260,000, including expenditure of effort and resources used to investigate and combat Defendant's unauthorized and covert deployment of the Comet AI agent into the Amazon Store.

58. Since July 2025, eight members of Amazon's Traffic Engineering team have spent hundreds of full workdays investigating, monitoring, and remediating Comet's agentic activity within the Amazon Store.

59. These Traffic Engineering team members have also worked to devise a technological barrier to prevent Defendant's Comet AI agent from covertly accessing the Amazon Store through private customer accounts. And Defendant has already evaded that technological barrier within 24 hours of its deployment.

60. The agentic traffic coming from the Comet AI agent has also disrupted and caused

damage to Amazon's technology and automated computer systems in at least two ways.

61. First, traffic from automated agents, such as that from the Comet AI agent, imposes operational burdens and costs on Amazon's advertising systems. Amazon's advertisers pay for their ads to be shown to humans, with billing based on valid ad impressions. When automated agents, such as the Comet AI agent, generate ad traffic, Amazon must invest engineering resources to detect and filter out these non-human impressions before billing advertisers. This requires modifications to Amazon's advertising systems, including developing new detection mechanisms to identify and exclude automated traffic. These system adaptations are necessary to maintain contractual obligations with advertisers who pay only for legitimate human impressions.

62. Second, Perplexity has damaged the Amazon accounts of Amazon customers who also use the Comet AI agent to access the Amazon Store. When Amazon customers access the Amazon Store through Comet's AI agent, Amazon has previously had to block those customers' accounts after Amazon identified Comet's agentic activity. Once this happened, these users could not access the Amazon Store through Comet. As a result, Amazon had to repair and unblock these accounts when these customers wanted to re-access their Amazon accounts through non-agentic browsing. This imposed operational burdens and costs on Amazon that would likely have been unnecessary if the Comet AI agent identified itself through its user-agent string when accessing the Amazon Store because that would allow Amazon to block traffic associated with just the Comet AI agent, instead of blocking a customer account.

63. The economic burden on Amazon to investigate and remediate Defendant's conduct is exacerbated because the Traffic Engineering team members working on this effort have diverted their attention away from their regular tasks of operating and maintaining Amazon's servers to ensure reliable customer satisfaction across Amazon's many services.

COUNT ONE

Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.*

64. Amazon repeats and re-alleges every allegation contained above as if set forth fully herein.

65. Defendant violated 18 U.S.C. § 1030.

66. Amazon's computers are involved in interstate and foreign commerce and communication and are protected computers as defined under 18 U.S.C. § 1030(e)(2)(B).

67. Defendant violated 18 U.S.C. § 1030(a)(2) because it knowingly and intentionally accessed, and continues to access, Amazon's computers without authorization or in excess of authorization, obtaining private customer information from Amazon's protected computers. Defendant obtained information from Amazon's protected computers in transactions involving interstate and foreign commerce that included, among other things, Amazon's customers' private account details, shopping history, billing information, and other sensitive customer personal and financial data.

68. Defendant violated 18 U.S.C. § 1030(a)(4) because it knowingly and with intent to defraud, accessed Amazon's computers without authorization or in excess of authorization, including by hiding its agentic activity and violating Amazon's Conditions of Use, and by means of such conduct furthered the intended fraud and obtained something of value. Defendant's intended fraud included sending concealed commands and requests to Amazon computers that falsely represented themselves as requests from authenticated, logged-in customers, in order to access and obtain data from Amazon, the value of which exceeded $5,000.

69. Defendant's conduct has caused a loss to Amazon as defined by 18 U.S.C. § 1030(e)(11), during a one-year period in excess of $5,000, including the expenditure of resources to investigate and remediate Defendant's conduct.

70. Amazon seeks compensatory damages in amount to be proven at trial and injunctive relief under 18 U.S.C. § 1030(g).

71. Amazon has suffered irreparable and incalculable harm and injuries resulting from Defendant's conduct, and this harm will continue unless Defendant is enjoined from further unauthorized use of Amazon's protected computers. Amazon has no adequate remedy in law.

COUNT TWO
California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502

72. Amazon repeats and re-alleges every allegation contained above as if set forth fully

herein.

73. Defendant violated California Penal Code § 502.

74. Defendant knowingly accessed and without permission took, copied, and/or used data from Amazon's computers, computer systems, and/or computer network in violation of California Penal Code § 502(c)(2).

75. Defendant knowingly and without permission used or caused to be used Amazon's computer services in violation of California Penal Code § 502(c)(3).

76. Defendant knowingly and without permission accessed and added and altered data to Amazon's computer, computer systems, and/or computer network, including by creating browsing and shopping history data while logged into customer accounts, in violation of California Penal Code § 502(c)(4).

77. Defendant knowingly and without permission accessed or caused to be accessed Amazon's computers, computer systems, and/or computer network in violation of California Penal Code § 502(c)(7).

78. Amazon suffered and continues to suffer damages as a result of Defendant's violations of the California Penal Code § 502 identified above.

79. Defendant's conduct also caused irreparable and incalculable harm and injuries to Amazon, and, unless enjoined, will cause further irreparable and incalculable injury, for which Amazon has no adequate remedy at law.

80. Defendant willfully violated California Penal Code § 502 in disregard and derogation of Amazon's rights, and Defendant's actions, as alleged above, were carried out with oppression, fraud, or malice.

81. Pursuant to California Penal Code § 502(e), Amazon is entitled to injunctive relief, compensatory damages, punitive or exemplary damages, attorneys' fees, costs, and other equitable relief.

PRAYER FOR RELIEF

82. Amazon respectfully requests that judgment be entered in its favor and against Defendant on all counts.

83. Amazon requests that the Court issue preliminary, interim, and permanent injunctive relief, enjoining and restraining Defendant and its agents, employees, successors, and assigns, and all other persons acting in concert with or in conspiracy with or affiliated with Defendant, from:

a. Accessing, attempting to access, or assisting, instructing, or providing a means for others to access or attempt to access Amazon's protected computer systems using AI agents;

b. Using any accounts, creating any new accounts, or taking over any existing accounts, on Amazon's websites, for the purpose of allowing Perplexity's AI agents to access Amazon's protected computer systems;

c. Accessing, attempting to access, or assisting, instructing, or providing a means for others to access Amazon's protected computer systems in excess of Amazon's authorization; and

d. Violating or evading any restrictions Amazon puts on the use of AI agents or other agentic activity on Amazon's protected computer systems.

84. Amazon further requests that the Court order the following additional nonmonetary relief:

a. Destruction of all copies of Amazon's data, including customer data, unlawfully obtained by Perplexity, whether in the custody or control of Perplexity or its employees, agents, assigns, or the third-party service providers (including, without limitation, web hosts, proxy servers, privacy services, and domain registrars);

b. Identification of each and every Amazon account ever accessed, used, or controlled through or by Perplexity, or any of its employees, agents, and assigns, to engage in the complained-of conduct; and

c. That Defendant certify and confirm, in writing and under oath, within thirty (30) days of the issuance of any order of the Court providing a remedy to Amazon, that Defendant has complied fully and completely with all requirements of such order.

85. Amazon further requests that the court award to Amazon as permitted by law and in such amounts to be proven at trial:

a. Monetary damages, including but not limited to compensatory, statutory, and punitive damages;

b. Amazon's reasonable costs, including reasonable attorneys' fees; and

c. Pre- and post-judgment interest.

86. Amazon further requests such other relief as the Court may deem just and proper.

JURY DEMAND

87. Plaintiff Amazon.com, Inc. hereby demands a trial by jury on all issues.

Dated: November 4, 2025

Respectfully submitted,

HUESTON HENNIGAN LLP

By: _____

Moez M. Kaba
Christine Woodin
Hagan Scotten (*Pro Hac Vice Pending*)
Billy Joe McLain

Attorneys for Plaintiff
AMAZON.COM SERVICES LLC