

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

DOORDASH, INC.,

Plaintiff,

V.

RYAN BATRA,

Defendant.

Case No.:

## COMPLAINT

DoorDash, Inc. (“DoorDash” or the “Company”), by and through its undersigned counsel,  
files this complaint against Defendant Ryan Batra (“Batra”), and alleges as follows:

## INTRODUCTION

1. This case arises from a deliberate and sweeping theft of DoorDash's highly sensitive confidential and trade secret information by a trusted senior executive recruiter, Batra. In the final days of his employment, Batra stole more than 1,500 files belonging to DoorDash, which contained a vast amount of proprietary and trade secret information. He did so through multiple different avenues, including by uploading these files from his Company device (e.g., his DoorDash laptop) to his personal Google account and forwarding at least forty-four additional emails and attachments containing confidential company information to his personal email address.

2. The stolen materials constitute the strategic blueprint of DoorDash’s recruiting operations in its most competitive sectors. They include not only the traditional confidential and proprietary materials underlying recruiting – executive offer letters, proprietary compensation models, and candidate lists – but also broader business information and internal strategies for DoorDash to strategically hire and develop talent to propel its artificial intelligence (AI) initiatives. Given the scarcity of engineering talent in the AI space, the importance of these strategies and

details cannot be underestimated . Engineers and executives with deep AI expertise are among the rarest and most valuable employees in the global labor market. DoorDash has invested years and significant resources developing the compensation structures, technical assessments, evaluation frameworks, and recruiting strategies necessary to attract and retain this talent.

3. Batra knew this. He also knew that DoorDash’s confidential recruiting data (including valuable information regarding AI talent being currently recruited by DoorDash), particularly its compensation structures, hiring priorities, and candidate information, would be immensely valuable to any entity competing to hire AI talent.

4. As a trusted senior executive recruiter, Batra had access to many of these documents. He exploited that access to take the materials directly from DoorDash’s secure Google enterprise system and Human Resources Information System (“HRIS”), Greenhouse, which DoorDash uses as an Applicant Tracking System (“ATS”). Certain of these documents were marked “confidential” and/or attorney-client privileged.

5. The unauthorized possession and potential use or disclosure of this information poses an immediate and irreparable threat to DoorDash’s competitive position, as it would allow a competitor to replicate DoorDash’s strategy, target key personnel, undercut DoorDash in compensation negotiations, and exploit confidential business plans and investment opportunities . The harm to DoorDash is not only financial, but also threatens its relationships with candidates, employees, investors, and business partners, and cannot be remedied by monetary damages alone.

6. Upon information and belief, Batra began taking this information while he was being recruited by and after receiving an offer letter from his current employer, Khosla Ventures, LLC (“Khosla”).

7. Khosla is a prominent private equity firm whose portfolio includes several high-

growth AI companies. Although Khosla is not a direct competitor of DoorDash, Batra's new role is focused on recruiting executives and engineers for Khosla's AI-related portfolio companies.

8. These are the exact types of positions for which he previously recruited at DoorDash. Batra therefore had a clear motive: to give himself an immediate and unlawful head start by taking DoorDash's confidential data and using it to accelerate his recruiting efforts at Khosla.

9. DoorDash tried to resolve this matter short of litigation. But Batra gave a false explanation when confronted with undisputable evidence of his misconduct. Batra tried to claim that he only had a few DoorDash materials and that they related solely to his transition from the Company. These bogus explanations were belied by the extensive, unassailable findings generated from DoorDash's internal review of Batra's misconduct.

10. Batra also refused to sign a standard certification of deletion affirming he had not shared the DoorDash files he emailed to himself or uploaded to his personal Google account and had deleted said files. Batra's continued retention and potential dissemination of DoorDash's files remains unresolved and poses a continuing and substantial threat to DoorDash.

11. As of the filing of this Complaint, DoorDash does not know whether Batra still possesses its proprietary and confidential trade secrets, whether they have been accessed by Khosla or its portfolio companies, or whether some portion of DoorDash's proprietary AI-recruiting strategy is already being used to recruit talent away from DoorDash.

12. Batra's conduct violates the Defend Trade Secrets Act, 18 U.S.C. §§ 1836 *et seq.* ("DTSA"), New York common law, his contractual confidentiality obligations, and his duty of loyalty.

13. Unless restrained, Batra's possession and potential use of DoorDash's sensitive

recruiting and compensation data threatens immediate and irreparable harm to DoorDash's competitive position and its ability to attract and retain world-class engineering talent, including those with AI expertise.

14. DoorDash therefore brings this action to protect its trade secrets, prevent dissemination or use of its confidential information, compel forensic inspection and remediation of Batra's personal devices and accounts, obtain a full accounting of Batra's misconduct, and secure the temporary restraining order and preliminary injunctive relief expressly authorized by Batra's employment agreements with DoorDash as well as by federal and state law.

15. DoorDash brings this action solely to obtain a temporary restraining order and preliminary injunction. DoorDash expressly reserves all claims for monetary damages and other relief for resolution in arbitration and does not waive, or intend to waive, its right to pursue such claims in arbitration.

### **PARTIES**

16. Plaintiff DoorDash is a corporation organized under the laws of the State of Delaware, with its principal place of business in California.

17. DoorDash also maintains substantial operations, employees, and business activities within the Southern District of New York. DoorDash's New York corporate office is located at 200 Fifth Ave., 8<sup>th</sup> Floor, New York, NY 10010, which is within this District.

18. As part of its core operations, DoorDash engages in advanced AI research and development, including for the purpose of designing proprietary AI models, systems, and technical innovations.

19. DoorDash employs highly specialized engineers, executives, and technical personnel whose recruitment, evaluation, and compensation involve significant proprietary

methods, confidential information, and investment.

20. DoorDash maintains secure systems, including Google Drive and Greenhouse, its ATS system, through which confidential and trade secret information is accessed and protected.

21. Defendant Batra is an individual residing in Brooklyn, New York. During his employment with DoorDash, Batra's assigned office was the Company's New York corporate office at 200 Fifth Ave., 8<sup>th</sup> Floor, New York, NY 10010, which is within this District. Batra is currently employed by Khosla and may be working remotely or traveling to this District as part of his recruiting responsibilities.

22. Batra is subject to personal jurisdiction in this District because he engaged in acts of misappropriation directed at DoorDash in this District, accessed DoorDash's confidential systems and data affecting operations in this District, and caused injury to DoorDash within this District.

23. As a condition of his employment, Batra entered into agreements with DoorDash containing strict confidentiality, non-use, and return-of-property obligations, along with an arbitration agreement that includes a carve-out permitting DoorDash to seek temporary and/or preliminary injunctive or equitable relief in court.

24. Batra resigned from DoorDash on or about October 20, 2025. He then joined Khosla, a private equity and venture capital firm whose portfolio includes several companies developing AI and advanced-technology products, as VP, Talent Partner.

25. Batra's new role includes recruiting executives, engineers, and technical leaders for Khosla's portfolio companies. This role directly overlaps with the AI, engineering, and product-related recruiting work he performed for DoorDash.

26. Batra's publicly available LinkedIn account states that his role at Khosla includes,

“[a]dvising founder and building a world-class network across AI, Engineering, Research, Product & Growth.”

### **JURISDICTION**

27. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because DoorDash asserts claims arising under the DTSA.

28. This Court also has jurisdiction under 28 U.S.C. § 1332(a) because the parties are citizens of different states and the amount in controversy exceeds \$75,000, exclusive of interest and costs.

29. The Court has supplemental jurisdiction over DoorDash’s state-law claims, including misappropriation of trade secrets, breach of contract, breach of duty of loyalty, conversion, and related claims, pursuant to 28 U.S.C. § 1367, because those claims form part of the same case or controversy as DoorDash’s federal DTSA claim.

30. Batra executed agreements with DoorDash containing an arbitration clause expressly carving out claims for temporary and/or preliminary injunctive or equitable relief, thereby authorizing DoorDash to seek a preliminary injunction and temporary restraining order in a court of competent jurisdiction, including this Court.

31. This Court has personal jurisdiction over Batra because, among other reasons, Batra purposefully directed activities toward this District, accessed DoorDash’s systems and information from within or through this District, entered into agreements governed by New York law, and committed acts giving rise to the claims asserted herein that caused injury to DoorDash in this District.

32. Additionally, Batra has engaged in acts of misappropriation, retention, and potential dissemination of DoorDash’s trade secrets knowing that the resulting injury would be

felt by DoorDash in New York, where DoorDash conducts substantial business operations.

### **VENUE**

33. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in this District, including Batra's access to DoorDash's confidential and trade secret information, DoorDash's detection of Batra's unauthorized downloads and transfers, and the resulting injury to DoorDash's operations located in or managed from this District.

34. Venue is also proper under 28 U.S.C. § 1391(c) because Batra is subject to personal jurisdiction in this District and is thus deemed to reside in this District for venue purposes.

### **FACTUAL ALLEGATIONS**

#### **Background on DoorDash's Business and AI Initiatives**

35. DoorDash is a technology company that operates a local commerce platform that connects customers with local restaurants, grocery stores, and other retailers, and, in some cases, delivery workers. DoorDash is heavily invested in AI projects and initiatives. To support these strategic efforts, DoorDash actively recruits and retains top-tier engineering and executive talent, particularly in the AI and machine learning fields, recognizing that such talent is critical to its competitive position and the growth of its AI platforms.

#### **Batra's Employment and Access to Confidential Information**

36. Batra started his most recent employment with DoorDash on or about April 8, 2024. Batra previously worked for DoorDash from on or about September 30, 2019 until December 31, 2022, as a Technical Recruiting Manager, Engineering.

37. Batra was re-hired in March 2024 with the business title of Lead Technical Recruiter.

38. As Lead Technical Recruiter, Batra was responsible for recruiting for the engineering client group, including machine learning and AI talent for analytics functions at the director level and above. While his primary focus was on engineering, he also assisted with high-level searches outside the engineering group and partnered with the M&A team to facilitate interview processes for potential corporate development opportunities. Furthermore, as a senior executive recruiter, Batra had access to DoorDash's most sensitive and confidential information, including recruiting strategies, compensation structures, deal memos, hiring plans, candidate evaluations, and strategic documents related to DoorDash's AI initiatives and long-term technical roadmap. He regularly handled high-level offer letters, compensation packages, and other proprietary materials, all of which were stored and managed within DoorDash's secure systems, such as Greenhouse and Google Drive.

#### **Relevant Contractual Agreements**

39. On March 4, 2024, Batra signed an employment offer letter from DoorDash, which included a valid and enforceable Proprietary Information and Inventions Agreement ("PIIA"). A copy of the PIIA is attached as Exhibit A.

40. Under the PIIA, Confidential Information is defined as:

any information, communication, data, or other materials which are (i) confidential and proprietary to the Company, (ii) not generally known to the public, or (iii) either disclosed to me by the Company directly or indirectly in writing, orally or by drawings or observation, or learned, created or developed by me (solely or jointly), by virtue of my employment with the Company. Without limiting the generality of the foregoing, "Confidential Information" shall include trade secrets, confidential knowledge, proprietary information, processes, know-how, designs, formulas, drawings, developmental or experimental work, computer programs, technology, products, product specifications, services,



techniques, concepts, ideas, inventions, discoveries, improvements, research, test results, databases, other works of authorship, customer and client lists or other information related to customers or clients or prospective customers or clients, information related to competitors or potential competitors of the Company, marketing or sales materials, business plans, strategies, forecasts, market information, budgets, projections, other financial information, consumer information, or information pertaining to any business of the Company or any of its employees, customers, clients, members, joint venturers, vendors, licensees, consultants or third parties with whom it does business.

Ex. A, ¶ 1(A).

41. Batra agreed to extensive protections of DoorDash's Confidential Information:

I agree that I shall not, and shall not permit any other person or entity to, directly or indirectly, without the prior written consent of the Company: (1) use Confidential or Trade Secrets for the benefit of any person or entity other than the Company; (2) remove, copy, duplicate or otherwise reproduce any document or tangible item embodying or pertaining to any of the Confidential Information or Trade Secrets, except as required to perform responsibilities for the Company; (3) load, install, copy, store or otherwise retain any Confidential Information on any non-Company computer or other device; and (4) while employed and thereafter, publish, release, disclose, deliver or otherwise make available to any third party any Confidential Information or Trade Secrets by any communication, including oral, documentary, electronic, or magnetic information transmittal device or media.

Ex. A, ¶ 1(A).

42. Further, in the PIIA, Batra agreed to return all Company information upon leaving his employment and promised to cooperate with DoorDash to remove or delete all Company information from his personal devices:

I agree that when I leave the Company's employment, I will deliver to the Company (and will not keep, copy, recreate or give any other person, firm or corporation) any and all Company Documents. To the extent any Company Documents ... resides on my personal computer ... or any other personal device of storage location ("Employee Devices"), I shall cooperate with the Company to remove or delete such information from my Employee Devices, including, if applicable, providing access and passwords to the Employee Devices to the Company's third-party forensic provider.

Ex. A, ¶ 4.

43. Batra's offer letter also included an arbitration agreement, which Batra signed on March 4, 2024. The arbitration agreement provides that it "does not affect the parties' rights to pursue ... claims in court for temporary and/or preliminary injunctive or equitable relief but only until such time that an arbitrator may be appointed." A copy of the arbitration agreement is attached hereto as Exhibit B.

#### **DoorDash's Security Measures and Batra's Misappropriation of DoorDash's Information**

44. DoorDash's ATS, Greenhouse, contained non-public information about DoorDash's recruiting strategies, candidate information, compensation structures, and technical requirements for AI-engineer and executive roles. DoorDash invested significant resources developing this information, which provides a substantial competitive advantage.

45. DoorDash maintained this information in secure, access-restricted systems, including its Google Drive environment and its Greenhouse system.

46. In the weeks leading up to his departure, Batra engaged in a sweeping and unauthorized effort to collect and exfiltrate DoorDash's confidential, proprietary, and trade secret information.

47. As described below, Batra uploaded (or emailed to himself) over 1,500 files from his DoorDash device to a personal Google Drive folder and Gmail account. These materials included, among other things:

- offer letters and compensation packages for high-level executives and engineers;
- deal memos for top employees;
- communications with and concerning high-level candidates for employment;
- salary signoffs and spreadsheets reflecting detailed compensation structures;
- strategic recruiting plans and proprietary analyses for AI business vertical strategies;
- internal engineering and leadership recruitment strategy documents; and
- confidential records pulled directly from DoorDash's Greenhouse system.

48. Certain of these materials were plainly marked as confidential or "ACP" (attorney-client privileged) and were accessible only to employees with a demonstrated need for access.

49. Batra had no legitimate business justification to download or retain these materials for personal use, and certainly not for use after he left DoorDash.

#### **Investigation of Batra's Misappropriation of DoorDash's Information**

50. Batra's last day with DoorDash was October 20, 2025.

51. On October 24, 2025, as part of routine operations, DoorDash conducted an off-boarding security review for Batra.

52. The security review's purpose was to determine whether, before his departure, Batra accessed, copied, transmitted, or retained confidential, proprietary, or otherwise protected Company information without authorization.

53. For Batra's security review, DoorDash reviewed his recent account activity using Google's security and administrative tools. Where that activity indicated potential data movement, DoorDash reviewed the underlying Google Workspace Admin Console logs, audit logs, and message trace data to determine whether Company files were moved, shared externally, or transmitted to non-Company destinations.

54. DoorDash also reviewed relevant metadata (including item IDs, file titles where available, timestamps, and sender/recipient, and hash values) to verify if the transfers involved Company materials and to determine the scope of any potential exfiltration.

55. This security review revealed that between September 15, 2025 and October 19, 2025, Batra engaged in extensive exfiltration of sensitive and highly confidential DoorDash files and trade secret information.

56. Batra stole this highly proprietary and confidential trade secret information by uploading materials from his Company device to a personal Google account and forwarding emails to his personal Gmail account.

57. Batra started his nefarious actions on or about September 9, 2025. DoorDash believes, and therefore avers, that Batra was already in discussions with Khosla at that time, and planning to leave his employment at DoorDash.

58. On September 9, 2025, Batra downloaded from DoorDash's ATS, Greenhouse, the January 2025 offer letter for a top executive at the Company who was hired several months earlier in March 2025. This offer letter contained highly confidential and sensitive information about this individual's compensation and employment with the Company. This offer letter was later uploaded, along with other files, to Batra's personal Google Drive.

59. There was no legitimate business reason for Batra to upload this document to his personal Google account. And because this executive was hired six months earlier, there was no reason for Batra to access this document as part of his normal and legitimate business activities for DoorDash.

60. Between September 15, 2025 and September 25, 2025, Batra uploaded over one hundred DoorDash files from his DoorDash device to a personal Google account. These materials

included highly confidential and non-public information concerning the Company's strategic initiatives to identify, recruit, and integrate senior executives and early-stage companies in the AI sector.

61. These Company files also contained detailed internal analyses and planning materials reflecting DoorDash's strategies, priorities, and timing for these initiatives. This included information regarding prospective targets, existing relationships, recruitment approaches, succession considerations, and project-specific planning related to potential transactions and integrations. The information related to a critical area of the Company's future business and technological development in the emerging field of AI and was closely guarded by DoorDash.

62. Also, certain of these files and emails were designated and clearly marked confidential or "ACP" (attorney-client privileged).

63. There was absolutely no legitimate reason for Batra to upload or forward this information to his personal accounts.

64. On September 25, 2025, Batra sent twenty-two emails from his DoorDash email account to his personal Gmail address. These emails included employment offers and approvals for several high-level Company positions.

65. Again, there was no legitimate reason for Batra to access or forward these files at the time.

66. On September 25, 2025, Batra downloaded to his DoorDash device and then, on September 26, 2025, uploaded from the device to his personal Google Drive, background check documents from Khosla.

67. That same day, Batra forwarded two emails from his DoorDash email account to his personal Gmail account. One of the emails involved communications with a potential candidate

for a highly confidential, high-level role that would report to DoorDash's co-founder.

68. Just a few days later, on September 29, 2025, among other documents, Batra uploaded to his Google Drive what appears to be an employment offer letter from Khosla with the file name of "KV Offer Letter - Ryan Batra (2025.09.23).doc.pdf".

69. On September 30, 2025, Batra downloaded to his DoorDash device spreadsheets containing highly confidential and private offer, equity, and other compensation information for thousands of DoorDash employees or candidates. It is DoorDash's belief that these spreadsheets were created by Batra in his DoorDash Google Drive through a business intelligence and analytics application called Sigma.

70. Also on September 30, 2025, Batra uploaded over fifty Company files from his DoorDash device to a personal Google Mail account, including the highly sensitive offer spreadsheets. These Company files Batra uploaded to his personal Google account also contained complete offer letters for some high-level individuals, including the offer letter for a key Company executive downloaded from Greenhouse on September 9, 2025.

71. On this same date, September 30, 2025, Batra verbally resigned from DoorDash. Batra subsequently submitted his written resignation via email to his supervisor on October 2, 2025.

72. Between October 3, 2025 and October 19, 2025, Batra sent about eighteen emails from his DoorDash email account to his personal Gmail account and uploaded over 1,500 files with unique hash values to his personal Google Drive.

73. Notably, on October 18, 2025, two days before his last day of employment, Batra moved over 180 files in his DoorDash Google Drive to the trash, including the spreadsheets uploaded on September 30, 2025. The files included sensitive documents that had previously been

uploaded to his personal Google account. In Google Drive, trashing files functions similarly to placing items in a recycle bin where they are scheduled for automatic deletion after a retention period unless manually removed. That same day, Batra permanently deleted those files from the trash. Batra trashed and deleted additional sensitive files on October 19, 2025. This activity is anomalous as between May 30, 2025 and September 30, 2025, Batra had only trashed seven files from his DoorDash Google Drive and had not permanently deleted any files.

### **Nature and Sensitivity of the Stolen Information**

74. All of the uploaded and emailed materials included critical, highly confidential and trade secret information files covering these areas:

- executive compensation and employment matters, as well as sensitive materials relating to the Company's AI initiatives;
- internal planning and analysis of the Company's AI strategy;
- senior AI leadership and recruiting efforts;
- prospective and current AI engineering personnel;
- internal research and development work and planning relating to AI initiatives;
- cyber and data security strategy and plans;
- high level executive employment offers and approvals;
- high level executive interview and evaluation materials;
- succession planning involving key executives; and
- strategic planning documents covering critical areas of the business like AI.

75. These stolen materials also contained highly confidential and sensitive information concerning potential business opportunities involving early-stage companies and specialized talent in the AI space.

76. These files also included several spreadsheets containing compensation and private employment information for thousands of Company employees.

77. All the materials described above were maintained in restricted-access systems and were not publicly available.

78. Certain of these uploaded files and emails were marked confidential or "ACP"

(attorney-client privileged).

79. There was no legitimate reason for Batra to take and certainly no legitimate reason for him to retain any of these highly confidential and trade secret files.

80. This information was developed at significant expense, was closely guarded by the Company, and relates to a critical area of DoorDash's future business and technological development in the emerging field of AI.

81. At no time did Batra have authorization to access, copy, upload, retain, or transfer DoorDash's confidential and proprietary materials for use outside the Company. And Batra did not seek or receive permission to do so.

82. Batra's actions were taken without the Company's knowledge or consent and in direct contravention of the Company's policies, his own confidentiality obligations, and common-sense restrictions governing sensitive business information.

#### **DoorDash's Outreach to Batra and His Deficient Response**

83. Upon discovering anomalies during the off-boarding security review, Kiran Lopez ("Lopez"), Senior Counsel on DoorDash's Employment Litigation team, made several attempts to contact Batra by telephone to speak to him about his conduct and determine whether he had retained any of the Company's materials.

84. After Lopez was unable to reach Batra by telephone, she emailed him on November 20, 2025.

85. After receiving this email, Batra spoke with Lopez by telephone.

86. During their call, Batra denied sending any DoorDash emails or files to his personal email address.

87. On November 21, 2025, Batra emailed Lopez and asserted that he had "double-



check[ed]” his personal email account and claimed that he had only unintentionally sent or saved “a small number of items” while preparing onboarding materials and documentation before he departed.

88. Batra explained that the process included forwarding emails to DoorDash teammates as “templates for handoff.”

89. Finally, Batra wrote that he sent himself messages related to non-DoorDash events that he had registered for using his DoorDash email address.

90. Batra stated that he had permanently deleted anything that could “even remotely” be interpreted as proprietary or confidential to the Company.

91. Batra’s assertion that he unintentionally sent or saved a small number of Company files is inconsistent with, and flatly contradicted by, DoorDash’s internal review, which revealed that Batra had uploaded and transmitted to himself hundreds of unique files containing highly confidential and sensitive Company information relating to the Company’s top AI employees and recruitment targets, AI-related initiatives, and other highly sensitive business information.

92. Further, DoorDash’s investigation did not support Batra’s claim that his conduct involved forwarding emails to teammates, as the emails at issue were sent only to his personal Gmail account.

93. Still, DoorDash tried to resolve the matter without resorting to litigation.

94. On November 21, 2025, DoorDash sent Batra a letter summarizing the issue, reminding him of his continuing confidentiality obligations, and detailing his violation of those obligations. DoorDash also attached a copy of Batra’s executed PIIA as well as a sample of his network activity that the Company’s investigation had uncovered.

95. DoorDash asked Batra to execute a written Certificate of Compliance confirming

that:

- he had returned and permanently deleted all Company materials in his possession;
- he had not disclosed, shared, or made available any Company files to any third party; and
- no Company information remained on any of his personal accounts or devices and sought Batra's cooperation in verifying compliance through reasonable means.

96. DoorDash also requested that Batra agree to have a third-party vendor conduct a forensic examination of his personal devices to ensure that they no longer contained any proprietary or confidential information belonging to DoorDash.

97. To date, Batra has refused to execute the Certificate of Compliance or agree to submit to a forensic review of his personal devices.

#### **Ongoing Risk and Need for Injunctive Relief**

98. As a result of Batra's refusal to cooperate, failure to provide credible assurances, and believed continued possession and control of the Company's confidential information, DoorDash has been left with no adequate remedy other than to seek relief from this Court.

99. Batra is now employed by a private equity firm that maintains multiple AI portfolio companies. Although Khosla itself is not a direct competitor, DoorDash and Khosla's AI portfolio companies compete for the same pool of AI talent. And Batra's new responsibilities include recruiting executives, engineers, and technical leaders for Khosla's portfolio companies, several of which compete in the AI and advanced-technology sectors.

100. As a result, there is an ongoing and imminent risk that DoorDash's most sensitive information will be used, disclosed, or exploited in ways that cannot be undone.

101. Once this information is disclosed or used, the resulting competitive harm, loss of strategic advantage, and erosion of confidentiality cannot be adequately remedied through monetary damages alone. This renders a preliminary injunction and temporary restraining order

necessary to prevent irreparable harm.

102. At DoorDash, Batra was heavily involved in recruiting AI engineers and senior technical leaders. These individuals are in extremely short supply and in exceptionally high demand. Successful placement of such individuals typically results in substantial compensation for a recruiter like Batra in his role at Khosla.

103. Batra therefore had a clear economic motive to take DoorDash's confidential recruiting, compensation, and AI strategy materials: to gain a head start at Khosla by leveraging DoorDash's work, insights, and data to identify, target, and recruit top talent, including top AI talent.

104. The nature and volume of the materials Batra took (including AI-focused compensation structures, evaluation strategies, and proprietary hiring analyses) are consistent with an effort to accelerate recruiting pipelines at his new role.

105. In a continued effort to resolve this matter without court intervention and to mitigate potential harm, DoorDash also notified Khosla of the issues identified through DoorDash's internal investigation.

106. Khosla said that it would cooperate and agreed to engage an independent team to search for and remediate any DoorDash proprietary or confidential information existing on its networks and computer systems. Cooperation between DoorDash and Khosla is ongoing as of the filing of this Complaint.

107. While DoorDash appreciates Khosla's willingness to cooperate, that cooperation does not eliminate the serious and ongoing concerns created by Batra's conduct. Batra, not Khosla, controlled the initial access to, transfer of, and retention of DoorDash's confidential information. Batra remains the only individual who can fully account for what information was taken, where it

was stored, whether it was copied, and whether it was shared or otherwise made available to third parties.

108. Batra has refused to provide even the most basic, verifiable assurances required to address these concerns. As a result, DoorDash has no reliable means to confirm that its proprietary and confidential trade secret information has been fully returned, permanently deleted, or not further disseminated.

109. Compounding these concerns, Batra has offered explanations for his conduct that are contradicted by the objective findings of DoorDash's internal review, which documented the access, transfer, and retention of a far greater volume and scope of confidential materials than Batra claimed. Further, DoorDash's investigation shows that in permanently deleting some of the information he stole from his DoorDash Google Drive, he attempted to conceal his conduct. As a result, DoorDash has no reliable basis to credit Batra's representations or to confirm that its proprietary and confidential trade secret information has been fully returned, permanently deleted, or not disseminated.

110. Batra's lack of candor reinforces the need for a preliminary injunction and temporary restraining order notwithstanding any cooperation by third parties.

111. Batra did not merely retain routine recruiting materials or documents related to his former role as a Lead Technical Recruiter. Rather, he accessed and transferred some of the Company's most sensitive and closely guarded information.

112. Batra taking materials related to recruiting activities is already a serious breach. But taking numerous high-level materials about DoorDash's internal AI strategy, research priorities, equity distributions, investment details, and long-term plans for developing and expanding its AI capabilities is even more egregious. These materials are among the most sensitive information

maintained by DoorDash and are far removed from any legitimate recruiting function.

113. The volume, scope, and subject matter of the materials Batra took cannot be explained as inadvertent or incidental to his former role at DoorDash.

114. Batra's continued possession of these materials, coupled with his refusal to certify their deletion, his refusal to submit to forensic verification, and the inconsistencies between his explanations and the objective investigative findings, creates an ongoing and substantial risk for DoorDash. That risk supports the need for a preliminary injunction and temporary restraining order.

115. The materials taken by Batra include trade secrets under the DTSA and New York common law because they contain non-public, proprietary, and competitively valuable information relating to:

- compensation structures and strategies used to attract and retain AI engineers and executives;
- internal employee data, compensation modeling, and organizational strategy;
- AI-focused hiring needs, technical competencies, and research priorities;
- proprietary AI-focused workforce strategy documents;
- confidential Greenhouse recruiting data, including candidate information and hiring plans; and
- confidential information about DoorDash investments, equity allocations, and strategic plans.

116. DoorDash derives substantial independent economic value from the secrecy of this information. It reflects years of investment in identifying, cultivating, and compensating world-class AI talent and contains proprietary methods and strategies unavailable to competitors or third parties.

117. If Batra uses or discloses this information at Khosla or at any other company, particularly those engaged in AI development, those companies could instantly benefit from DoorDash's confidential recruiting strategies, compensation structures, and AI strategies and

plans.

118. DoorDash has reason to believe that Batra remains in possession of some or all of the stolen materials and that these materials may already exist on Khosla's systems or devices used by Batra in his new role.

119. Batra executed agreements with DoorDash containing strict confidentiality obligations and an arbitration clause with a carve-out for temporary and/or preliminary injunctive or equitable relief, expressly permitting DoorDash to seek court intervention to prevent misuse of confidential information. *See* Exs. A-B.

120. Batra's unauthorized taking, disclosing, and/or using DoorDash's trade secrets without DoorDash's consent both prior to and after leaving the Company constitute a violation of his PIIA, as well as misappropriation in violation of state and federal law.

121. Similarly, Batra's conduct gives rise to an unfair competition claim because of the unlawful advantage provided through his unauthorized taking, disclosing, and/or using DoorDash's confidential information and trade secrets without DoorDash's consent.

122. Batra's conduct also violated his duty of loyalty to DoorDash. Rather than return DoorDash's information at the end of employment, Batra covertly transferred hundreds of confidential files to personal storage locations in the days immediately preceding his departure.

123. Batra further converted DoorDash's property by exercising unauthorized dominion and control over the Company's confidential and trade secret files, thereby substantially interfering with DoorDash's rights over the same.

124. Batra has been unjustly enriched his wrongful acquisition and retention of DoorDash's confidential and trade secret information, conferring value and a competitive advantage at DoorDash's expense.

**COUNT I**  
**Breach of Contract**

125. DoorDash re-alleges and incorporates by reference all allegations of Paragraphs 1 through 124 as if fully set forth herein.

126. Batra voluntarily entered into a valid and enforceable contract, the PIIA, with DoorDash as a condition of employment under which he agreed to maintain the confidentiality of DoorDash's Confidential Information, to use said information only within the scope of his employment, and to return all such information upon separation.

127. The PIIA further required Batra not to load, store, copy, or retain DoorDash's Confidential Information on non-Company devices, and to cooperate in post-employment remediation, including providing access to a third-party forensic provider if applicable.

128. The PIIA was supported by adequate consideration.

129. DoorDash fully performed its obligations under the PIIA.

130. Batra materially breached the PIIA by: (a) uploading more than 1,500 confidential and trade secret files from DoorDash's systems to his personal Google account; (b) forwarding DoorDash emails and attachments to his personal email; (c) retaining DoorDash information post-employment; and (d) refusing to return, certify deletion of, or cooperate in forensic remediation of DoorDash's information.

131. As a direct and proximate result, DoorDash has suffered and will continue to suffer irreparable harm warranting a preliminary injunction and temporary restraining order, including specific performance of the PIIA's return/deletion and cooperation obligations.

**COUNT II**  
**Misappropriation of Trade Secrets Under The Defend Trade Secrets Act**  
**18 U.S.C. §§ 1836 *et seq.***

132. DoorDash re-alleges and incorporates by reference all allegations of Paragraphs 1

through 131 as if fully set forth herein.

133. DoorDash is the owner of certain valuable trade secrets and confidential information in and relating to its business including its compensation information, recruiting targets, recruiting methods, acquisition targets, investments, AI strategic planning, and other strategy information.

134. These confidential and proprietary trade secrets are of substantial economic value and their possession provides competitive advantages for DoorDash, who has spent significant time and money developing them.

135. These trade secrets and confidential information, as described above, constitute “trade secrets” within the meaning of 18 U.S.C. § 1839(3).

136. DoorDash’s confidential and trade secret information derives independent economic value from not being generally known or readily ascertainable.

137. The Trade Secrets relate to products or services used in, or intended for use in, interstate and/or foreign commerce, including DoorDash’s nationwide and international operations, recruiting, and AI research and development initiatives. DoorDash’s confidential and trade secret information relates to products or services used, sold, or purchased, or intended for use, sale, or purchase, across the United States and throughout the world.

138. DoorDash has taken reasonable measures to maintain the secrecy of its confidential, proprietary and trade secret information, including those trade secrets misappropriated by Batra as described herein, by among other things utilizing role-based access controls, employing multi-factor authentication, designating materials as confidential, and restricting data and device logging.

139. Batra received access to DoorDash’s trade secret information as a result of his acceptance of the obligations and terms of the PIIA. The terms of the PIIA included an obligation



on Batra to maintain the confidentiality of DoorDash's proprietary information, including DoorDash's trade secret information.

140. Having acquired DoorDash's trade secrets under circumstances giving rise to a duty to maintain the secrecy of DoorDash's trade secrets, Batra unlawfully misappropriated DoorDash's trade secrets by taking, disclosing, and/or using DoorDash's trade secrets without DoorDash's consent both prior to and after leaving the Company.

141. Batra acquired, accessed, disclosed, and used DoorDash's trade secret and confidential information by improper means, without DoorDash's express or implied consent, and in violation of the PIIA, as discussed above.

142. Batra acquired DoorDash's trade secrets through improper means in order to benefit himself, and to unfairly compete against and harm DoorDash.

143. Batra knew or had reason to know at the time he acquired, disclosed, and used DoorDash's trade secret and confidential information that the trade secrets and the material containing the trade secrets was confidential and proprietary to DoorDash and was acquired and maintained by improper means and/or under circumstances creating a duty to maintain confidentiality or limit use including by and through the PIIA.

144. Batra further knew and understood that the information contained in DoorDash's trade secrets was information that was not generally known or available in the public domain and was information that would provide a significant and unfair competitive advantage to those in competition with DoorDash, especially in the highly competitive market for AI engineering talent.

145. Khosla hired Batra to recruit AI talent for their portfolio companies. Although Khosla and DoorDash are not direct competitors, Khosla's portfolio companies and DoorDash both compete for AI employee talent. Like DoorDash, Khosla's portfolio AI companies need to

hire AI talent in a highly competitive market.

146. The trade secret and other confidential information taken by Batra from DoorDash would help him to compete against DoorDash when recruiting AI talent. It would also give him a massive head start in his recruiting efforts for Khosla.

147. DoorDash has never, directly, or indirectly, consented to Batra's use, acquisition, or disclosure of its trade secrets.

148. Batra has engaged in the actual or threatened misappropriation of DoorDash's confidential and trade secret information in violation of the DTSA.

149. Batra's actions, as alleged herein, constitute "misappropriation" within the meaning of 18 U.S.C. § 1839(5).

150. Batra's actions, as alleged herein, entitle DoorDash to preliminary and permanent injunctive relief, including by enjoining Batra from using or retaining DoorDash's confidential and trade secret information, enjoining the destruction, altering, or deletion of any trade secret information or material or information derived from DoorDash's trade secret information, and requiring a return of all material concerning, referring, related to or embodying in whole or in part any of DoorDash's confidential and trade secret information.

**COUNT III**  
**Misappropriation of Trade Secrets Under New York Common Law**

151. DoorDash re-alleges and incorporates by reference all allegations of Paragraphs 1 through 150 as if fully set forth herein.

152. DoorDash possesses protectable trade secrets under New York law, including its compensation information, recruiting targets, recruiting methods, investments, acquisition targets, AI strategic planning, and other strategy information, which derive independent economic value from their secrecy and are subject to reasonable secrecy measures, including *inter alia* employing

role-based access controls, multi-factor authentication, designation of materials as confidential, and restricting data and device logging.

153. Batra misappropriated DoorDash's trade secrets by acquiring, copying, removing, and retaining them on personal devices and accounts without authorization, refusing to return or certify deletion, and acting in breach of his duties and in breach of the PIIA, and Batra accomplished his misappropriation through improper means.

154. As a result, DoorDash has suffered, and will continue to suffer, irreparable harm and is entitled to a preliminary injunction and temporary restraining order, return and deletion, and forensic remediation.

**COUNT IV**  
**Breach of Duty of Loyalty**

155. DoorDash re-alleges and incorporates by reference all allegations of Paragraphs 1 through 154 as if fully set forth herein.

156. As a Lead Technical Recruiter entrusted with highly sensitive information, Batra owed DoorDash a duty of loyalty to act in DoorDash's best interests and to refrain from misusing DoorDash's confidential and trade secret information for personal or third-party benefit.

157. While still employed by DoorDash and after receiving an offer from Khosla, Batra deliberately collected and transferred DoorDash's confidential and trade secret materials for his own use and to benefit his transition, in direct violation of his duty of loyalty. He also attempted to conceal his misconduct by deleting some of the information he stole from his DoorDash Google Drive. This conduct demonstrates not only a clear awareness of wrongdoing, but also an intent to evade detection and accountability.

158. As a result, DoorDash suffered irreparable harm and is entitled to relief.

**COUNT V**  
**Conversion**

159. DoorDash re-alleges and incorporates by reference all allegations of Paragraphs 1 through 158 as if fully set forth herein.

160. DoorDash owns and has the right to possess the confidential and trade secret files, confidential information, records, and data at issue.

161. Batra intentionally and without authorization exercised dominion and control over DoorDash's property by copying, removing, uploading, retaining, and refusing to return it upon demand, thereby substantially interfering with DoorDash's rights.

162. As a direct and proximate result, DoorDash has suffered and will continue to suffer irreparable harm, and DoorDash is entitled to return and delivery up of all such materials and forensic remediation.

**COUNT VI**  
**Unfair Competition by Misappropriation**

163. DoorDash re-alleges and incorporates by reference all allegations of Paragraphs 1 through 162 as if fully set forth herein.

164. Batra misappropriated DoorDash's labor, skill, and expenditures by taking DoorDash's confidential and trade secret information to gain an unfair head start for himself and for the companies within Khosla's portfolio's recruiting efforts in the AI talent market, acting in bad faith.

165. As a direct and proximate result, DoorDash has suffered and will continue to suffer irreparable harm.

166. DoorDash is entitled to a preliminary injunction and temporary restraining order and other equitable remedies.

**COUNT VII**  
**Unjust Enrichment**

167. DoorDash re-alleges and incorporates by reference all allegations of Paragraphs 1 through 166 as if fully set forth herein.

168. Batra has been unjustly enriched by his wrongful acquisition and retention of DoorDash's confidential and trade secret information, conferring value and a competitive advantage at DoorDash's expense.

169. As a result of Batra's wrongful conduct, DoorDash has sustained, and will continue to sustain, immediate irreparable harm and incalculable monetary loss.

**PRAYER FOR RELIEF**

**WHEREFORE**, DoorDash, Inc. respectfully requests that the Court enter judgment in its favor and against Defendant Ryan Batra and award the following relief:

(a) An order requiring Defendant to turn over to a mutually agreed-upon neutral, independent forensic examiner ("Neutral Forensic Examiner") all devices, accounts, and storage media that have housed, accessed, or touched DoorDash's information, including but not limited to:

- Desktop or laptop computers (personal or work);
- Mobile phones;
- Tablets/iPads;
- External drives/USB devices;
- Personal or business email accounts;
- Cloud-storage accounts (e.g., Dropbox, Google Drive, iCloud, OneDrive); and
- Messaging or collaboration platforms (e.g., WhatsApp, Slack, Teams).

(b) An order requiring Defendant to provide a sworn declaration identifying with specificity:

- All documents, data, files, records, or other information belonging to DoorDash that Defendant downloaded, copied, emailed, uploaded, transferred, retained, or accessed, including any information originating from DoorDash's Greenhouse recruiting system, Google systems, or related databases;
- All methods and means by which DoorDash's information was obtained, transmitted, or accessed, including, but not limited to, personal or business email accounts, cloud-storage accounts, external drives, messaging platforms, or file-transfer tools;
- All devices, accounts, storage media, and locations (physical or digital) where

DoorDash's information was or is presently stored, retained, backed up, or accessible;

- Every person or entity to whom Defendant provided access to DoorDash's information, directly or indirectly, along with the nature, extent, and dates of such access; and
- All actions taken by Defendant with respect to DoorDash's information, including any access, review, copying, transfer, forwarding, uploading, editing, deletion, or use.

(c) An order requiring the parties and the Neutral Forensic Examiner to meet and confer to develop a Forensic Examination and Remediation Protocol (the "Protocol") that will:

- Identify all DoorDash information on any device or account accessed by Defendant at any time since the end of his employment with DoorDash;
- Determine whether any information was accessed, used, or disseminated, and if so, by whom, to whom, and when;
- Identify all residual or derivative copies;
- Provide for the secure removal and full remediation of DoorDash's information from Defendant's devices, storage media, and accounts;
- Ensure preservation of evidence in accordance with the Federal Rules of Civil Procedure.

(d) An order that the Neutral Forensic Examiner shall maintain all devices and data in escrow pending examination and remediation under the Protocol under the Court's supervision.

(e) An order that the Neutral Forensic Examiner shall prepare a written report detailing findings, chain of custody, and all recovered materials, with disclosure of DoorDash's information restricted under the parties' Protocol or, if necessary, a protective order approved by the Court.

(f) An order requiring Defendant to provide all required passwords, authentication credentials, two-factor codes, security tokens, and other information necessary for full access to the above devices and accounts (paragraph (a)).

(g) An order enjoining Defendant, and anyone in concert with Defendant, from accessing, altering, deleting, destroying, wiping, encrypting, transferring, or modifying any device, files, account, or other information subject to examination.

(h) Pending further order of the Court, an order restraining and enjoining Defendant and anyone in concert with Defendant, from:

- Using, accessing, retaining, disclosing, sharing, copying, transferring, relying upon, or referencing any of DoorDash's confidential, proprietary, or trade secret information, including all information obtained from DoorDash's Greenhouse and Google systems;
- Providing access to any person or entity (other than DoorDash, the Neutral Forensic Examiner, and attorneys of record) to any such information;
- Altering, destroying, deleting, wiping, encrypting, concealing, or modifying any document, device, file, account, or metadata relating to DoorDash's information or the

forensic examination ordered herein.

- (i) An order requiring Defendant to appear for a deposition limited solely to:
- What information Defendant took or accessed;
  - How the information was obtained, transmitted, or used;
  - All devices/accounts that touched DoorDash's information;
  - All persons or entities who received or were exposed to the information; and
  - The current or former existence of any copies.

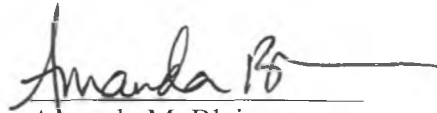
Without restricting additional discovery allowed under the Federal Rules of Civil Procedure or as part of any arbitration.

(j) An order requiring Defendant to preserve all documents, devices, accounts, and electronically stored information ("ESI") potentially relevant to the claims in this action, consistent with this Court's Local Civil Rules and applicable Federal Rules of Civil Procedure.

(k) Attorneys' fees and costs to the extent permitted by law or contract.

(l) Such other and further legal and equitable relief as the Court deems just and proper.

Dated: December 19, 2025  
New York, NY



Amanda M. Blair  
David J. Walton, *Pro Hac Vice Forthcoming*  
FISHER & PHILLIPS LLP  
Times Square Tower  
7 Times Square, Suite 4300  
New York, NY 10036  
Tel.: (610) 230-6105  
Tel.: (212) 899-9989  
dwalton@fisherphillips.com  
ablair@fisherphillips.com

*Attorneys for Plaintiff DoorDash, Inc.*