JOSEPH C. ALM, State Bar No. 294362
Tesla, Inc.
901 Page Avenue
Fremont, CA 94538-734
Email: jalm@tesla.com
Phone: (650) 681-5000

Counsel for Plaintiff
TESLA, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

TESLA, INC., Plaintiff, v. ALEX KHATILOV Defendant.	Case No.: _____ **COMPLAINT** **(1) Violation of the Defend Trade Secrets Act (18 U.S.C. § 1831 *et seq.*)** **(2) Violation of the California Uniform Trade Secrets Act (Cal. Civ. Code § 3426 *et seq.*)** **(3) Breach of Contract** **JURY TRIAL DEMANDED**

Plaintiff Tesla, Inc. ("Tesla" or "Plaintiff"), complains and alleges against Defendant Alex Khatilov ("Khatilov" or "Defendant"), as follows:

NATURE OF THE ACTION

1. This case is about Tesla protecting its trade secrets from premeditated theft by a (now) former employee, and making sure it does not happen again. Within three days of being hired by Tesla, Defendant brazenly stole thousands of trade secret computer scripts that took Tesla years to develop. Then, he lied about it and tried to delete the evidence of his theft when quickly confronted by Tesla's security team, forcing Tesla to bring this complaint.

2. Tesla hired Defendant as a software automation engineer on December 28, 2020. Within three days, he began stealing thousands of highly confidential software files from Tesla's secure internal network, transferring them to his personal cloud storage account on Dropbox, to which Tesla has no access or visibility. The files consist of "scripts" of proprietary software code that Tesla has spent years of engineering time to build. These scripts, when executed, automate a broad range of functions throughout Tesla's business. Only a select few Tesla employees even have access to these files; and as a member of that group, Defendant took advantage of that access to downloaded files unrelated to his job.

3. Tesla's information security personnel detected Defendant's unauthorized download on January 6, 2021 and confronted Defendant that day and interviewed him. During this interview he repeatedly claimed that he had only transferred a couple personal administrative documents. After being prompted, he gave Tesla investigators access to view his Dropbox account, where they discovered Defendant's claims were outright lies: the Tesla investigators found thousands and thousands of Tesla's confidential computer scripts in his Dropbox. Defendant then claimed he somehow "forgot" about the thousands of other files he stole (almost certainly another lie). Even worse, it became apparent that Defendant had brazenly attempted to destroy the evidence by hurriedly deleting the Dropbox client and other files during the beginning of the interview when investigators were attempting to remotely access his computer.

4. Fortunately, the investigators were able to eventually view the Dropbox account and instructed Defendant to delete all Tesla files that still remained. But Tesla's ability to rectify

Defendants' wrongdoing ended there. Tesla does not know whether Defendant took additional files, whether he copied files from the Dropbox account to other locations in the days before he was caught, or whether he sent any of the files to other persons or entities. Indeed, as soon as Defendant uploaded the stolen files to his Dropbox account, he could have shared or retransferred those files to anyone or any other storage media (whether an external thumb drive, another computer, a mobile device, or another cloud-based storage system). And Tesla would have had no way to know that.

5. This action is based on Defendant's: (1) violation of the Defend Trade Secret Act, 18 U.S.C. § 1831, *et seq*.; (2) violation of the California Uniform Trade Secret Act, Cal. Civ. Code § 3426, *et seq*.; and (3) breach of contract.

THE PARTIES

6. Plaintiff Tesla is a corporation organized and existing under the laws of Delaware, with its principal place of business located at 3500 Deer Creek Road, Palo Alto, California 94304. Tesla develops, manufactures, sells, and leases electric vehicles and energy generation and storage systems throughout the United States and abroad.

7. Defendant Alex Khatilov is a former Tesla employee who also goes by the names Alex Tilov or Sabir Khatilov. Upon information and belief, he resides at 556 Chestnut Avenue, San Bruno, California 94066.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 1836(c), as it arises under the federal Defend Trade Secrets Act, 18 U.S.C. § 1831 *et seq.*

9. This Court has supplemental jurisdiction over Plaintiff's state law claims under the California Uniform Trade Secret Act, Cal. Civ. Code § 3426, *et seq*. and for breach of contract pursuant to 28 U.S.C. § 1367(a) because Tesla's state law claims are so closely related to its federal claim that they form part of the same case of controversy under Article III of the United States Constitution.

10. Venue is proper in the United States District Court for the Northern District of California pursuant to 28 U.S.C. § 1391 because Defendant resides in the Northern District of California and a substantial part of the events and omissions giving rise to the claims asserted occurred in this District.

INTRADISTRICT ASSIGNMENT

11. A substantial part of the events and omissions which gave rise to the claims asserted took place in Santa Clara County, California. Thus, pursuant to Civil L.R. 3-2(c) and (e), this action should be assigned to the San Jose Division of this District.

FACTUAL ALLEGATIONS

Tesla's Trade Secrets and Confidential Information

12. Among Tesla's numerous innovations is its development of automated, "Quality Assurance" processes that run a broad range of business functions without human effort, including procurement, materials planning and processing, payables, and purchasing (collectively, the "Tesla Trade Secrets"). For example, much of the manufacturing cycle of Tesla vehicles is managed by these automated processes – from ordering parts to delivering cars.

13. Tesla employs a team of Quality Assurance Engineers who help identify business tasks to be automated based on input from Tesla's business leaders. The engineers write computer scripts in Python (a computer programming language) to automate those tasks, and test the automated processes to ensure they function properly. These scripts are unique to Tesla and run on WARP Drive, the backend software for much of Tesla's business.

14. Developing this complex system is expensive and time-consuming. Tesla has spent roughly 200 man-years of work to develop the Quality Assurance scripts – the cumulative hours spent by the Quality Assurance Engineering team over the past twelve years. The engineers' work is also guided by the business leaders in Tesla, who identify what tasks need to be automated – another large and valuable investment of its time.

15. The Tesla Trade Secrets are extremely valuable to Tesla, and would be to a competitor. Access to the scripts would enable engineers at other companies to reverse engineer Tesla's automated processes to create a similar automated system in a fraction of the time and with

a fraction of the expense it took Tesla to build it. Third-party engineers could not compose these scripts based on public information, especially with such minimal time and effort. The scripts also would inform competitors of which systems Tesla believes are important and valuable to automate and how to automate them – providing a roadmap to copy Tesla's innovation.

16. For these reasons, Tesla takes extensive measures to ensure that the Tesla Trade Secrets remain strictly confidential and are never shared externally. Even within Tesla, access to the scripts is limited to members of the Quality Assurance Engineering team, which is approximately 40 people out of Tesla's roughly 50,000 employees. Who can grant access rights to the Trade Secrets is even more narrowly controlled, with only eight people having the ability to grant access. The engineers who do have access to the scripts are not permitted to download them to personal devices or cloud storage.

17. Tesla's engineers also sign a comprehensive set of agreements and policies as a condition of their employment which require them to protect Tesla's confidential information and not to disclose or misuse that information, including the Tesla Trade Secrets. These include: an Employee Nondisclosure And Inventions Assignment Agreement ("NDA"), which requires employees to hold Tesla's information "in strictest confidence" and prohibits them from using or disclosing any Tesla "Proprietary Information," including "technical data, trade secrets, know-how, … plans, designs, … methods, processes, … data, programs, … and other business information"; and an Internet Usage Policy that prohibits "transmitting, copying, downloading, or removing trade secret, proprietary, or confidential business information of Tesla without written authorization."

18. The NDA also requires employees, upon termination, to "immediately return to the Company all originals and copies of all hard copy and electronic documents, files and other property of the Company in [their] possession or control or to which [they] have access … regardless of the storage medium (e.g., internal or external hard drives, solid-state drives, USB flash drives, flash memory cards, and cloud storage)."

19. Tesla secures its physical facilities by restricting access to authorized personnel, and then monitoring actual access with security guards and cameras. Visitors to Tesla's facilities

must check in with a receptionist or security, sign a nondisclosure agreement, and submit to a photograph. Visitors must also always be escorted by a Tesla employee while at the facilities.

20. Tesla further protects its confidential, trade secret, and proprietary information by using password-protected and firewall-protected networks and servers that are only accessible to current Tesla employees with proper credentials.

21. Tesla also has an Information Security team that monitors its systems for suspicious activity, including unauthorized downloading of confidential information.

Defendant Alex Khatilov Promises to Protect Tesla's Trade Secrets and Confidential Information as a Condition of His Employment at Tesla

22. On December 28, 2020, Tesla hired Defendant Alex Khatilov as a Senior Software Quality Assurance Engineer.

23. Defendant's role and responsibility was to prepare and revise computer scripts to help automate Environmental Health and Safety ("EHS") systems.

24. As part of his employment, Tesla provided Defendant a laptop to perform his work.

25. As a condition of his employment, Defendant signed and agreed to abide by the terms of the NDA.

Defendant's Theft of Tesla's Trade Secrets, and Attempts to Conceal His Misconduct

26. On December 31, 2020 – just three days after being hired by Tesla – Defendant began downloading thousands of files from Tesla's networks and transmitted those files to his personal Dropbox account. The downloading was completed on January 4, 2021. He also downloaded some additional files on January 6.

27. Tesla's Information Security team detected the downloading of up to approximately 26,000 files on January 6 through its monitoring software. The team immediately reviewed the activity and concluded that it was not an authorized transfer. Tesla also discovered that the files contained a complete set of all automation scripts produced by the Quality Assurance Engineering team for WARP Drive over the last twelve years.

28. The scripts downloaded by Defendant had nothing to do with his responsibilities for developing scripts on the EHS system, which runs on a separate system from WARP Drive.

29. Shortly after the Tesla Information Security team discovered Defendant's theft, Tesla personnel confronted Defendant by initiating a videoconference call via Microsoft Teams that same day. Defendant had been working remotely due to COVID-19.

30. During the call, Defendant confirmed that he had signed the NDA. He also confirmed that he installed a Dropbox desktop application on his Tesla-issued laptop, which enabled him to upload files to a personal cloud-based account to which Tesla has no access or visibility. Defendant claimed, however, that he had only uploaded personal administrative documents to his Dropbox, such as his scanned passport and a copy of his W-4. When asked to clarify, he reiterated again that he uploaded only personal administrative documents to his Dropbox account, not anything confidential to Tesla.

31. Tesla personnel prompted Defendant to share his laptop screen to confirm that his Dropbox account did not contain any confidential Tesla files, as he twice claimed. Defendant delayed accepting the screen share request for over a minute, thus preventing Tesla personnel from viewing his screen or Dropbox files. During this time, he could be seen on videochat hurriedly deleting information from his computer.

32. Once Defendant finally shared his screen, he claimed that he had already deleted the Dropbox desktop application during the interview, confirming that Defendant was destroying evidence to try to prevent Tesla from inspecting what he had done.

33. Although Defendant had deleted the Dropbox desktop application from his laptop, such deletion only disabled the functionality that uploads files to the Dropbox cloud, and did not necessarily delete files uploaded to the account itself. Tesla personnel thus instructed Defendant to display all files that had already been transferred to Dropbox, which revealed folders containing a large amount of non-administrative material, including many of the Quality Assurance scripts that were detected by Tesla's monitoring software.

34. Tesla personnel also instructed Defendant to login to the Dropbox website so they could see whether the files he downloaded remained available in his Dropbox account. This revealed that the same confidential Tesla files seen on his laptop were still available through his cloud storage account. Defendant agreed to delete the remainder of those files – or at least, the

ones that Tesla personnel were able to see during the call. The investigators, however, were only able to view Defendant's screen – they could not actually control his mouse or keyboard in order to delete the files themselves.

35. Tesla personnel then informed Defendant that, despite his claims to the contrary, the Information Security team detected that he removed over 26,000 highly confidential, non-administrative files from the Tesla network over the course of several days. Defendant claimed that he "forgot" he had downloaded them. Defendant was also unable to articulate a business reason for his downloads.

36. Defendant was terse and evasive throughout the interview, providing mostly one-word answers and feigning ignorance. Defendant repeatedly lied to Tesla, claiming (twice) that he had only downloaded and transferred personal administrative files, and then claiming that he "forgot" about downloading thousands of other non-administrative, highly confidential software scripts. He also attempted to destroy evidence of his theft while obstructing Tesla's efforts to access his laptop screen and see what he had taken.

37. After discovering Defendant's theft of the Tesla Trade Secrets, and due to his repeated lying and obfuscation during the investigation, Tesla fired Defendant that day.

38. Although investigators were able to watch Defendant delete the information they found on Defendant's laptop and in his Dropbox account, Tesla could not confirm whether he took additional files, whether the information he downloaded was further transferred from Dropbox to other locations in the days before he was caught, or whether he shared the information with anyone else.

39. As soon as Defendant uploaded the files to his Dropbox account, he had the ability to instantly share or retransfer those files from Dropbox to any other person or location at any time – including loading them onto a thumb drive, emailing them, syncing them to another computer, transferring them to an entirely different cloud-based account, or even printing them. Tesla would have had no way to monitor that activity, which Defendant could have done at any time before he purportedly deleted the files from Dropbox.

40. Moreover, because of COVID-19, this interview had to be conducted remotely, rather than in person. This remote process necessarily hindered Tesla's ability to ensure complete deletion of the Trade Secrets, since Tesla could not directly control Defendant's devices, perform immediate forensic analysis of the devices, or acquire full access to Defendant's Dropbox.

41. On information and belief, Tesla did not uncover all of Defendant's theft. Defendant's proven track record of dishonesty and evidence destruction raises grave concerns that he continues to misappropriate Tesla's Trade Secrets. On information and belief, Defendant has indeed further used and/or disseminated that information.

First Cause of Action

(Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1831 *et seq.*)

42. Tesla re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 38 of this Complaint.

43. As set forth above, Defendant misappropriated thousands of Quality Assurance automation software scripts constituting "trade secrets" under the Defend Trade Secrets Act, 18 U.S.C. § 1831 *et seq.* Tesla is the owner of these Tesla Trade Secrets.

44. The Tesla Trade Secrets automate business processes underlying the development, manufacturing, sale, and leasing of products and services used in, and intended for use in, interstate and foreign commerce.

45. The Tesla Trade Secrets derive independent economic value from not being generally known to the public, to Tesla's competitors, or to other persons who can obtain economic value from the disclosure or use of the information.

46. The Tesla Trade Secrets are not readily ascertainable through proper means or from generally available, public sources.

47. At all relevant times, Tesla has made reasonable efforts to protect and preserve the secrecy of the Tesla Trade Secrets.

48. Defendant misappropriated the Tesla Trade Secrets within the meaning of 18 U.S.C. § 1839(5) by, *inter alia*, knowingly acquiring the Tesla Trade Secrets through improper

means, and disclosing and/or using the Tesla Trade secrets without Tesla's express or implied consent.

49. Defendant knew or had reason to know that, at the time he accessed, downloaded and used the Tesla Trade Secrets, this information was acquired and obtained by improper means and/or under circumstances giving rise to a duty to maintain secrecy or limit use, and that he did not have Tesla's express or implied consent to do so.

50. Defendant acquired the Tesla Trade Secrets by virtue of his employment with Tesla, not through his own independent research and efforts, in direct violation of his legal obligations to Tesla.

51. On information and belief, Defendant failed to fully delete or return the Tesla Trade Secrets that he misappropriated, and continues to use or disclose the Tesla Trade Secrets without Tesla's consent.

52. On information and belief, Defendant has gained, or will gain, substantial benefit from his misappropriation of the Tesla Trade Secrets, to Tesla's substantial detriment.

53. As a result of Defendant's unlawful conduct, the Tesla Trade Secrets have been compromised, and Tesla is substantially threatened by Defendant's further use and/or dissemination of that information.

54. As a direct, proximate, and foreseeable result of Defendant's misappropriation of the Tesla Trade Secrets, Tesla has been damaged in an amount not yet ascertained.

55. Defendant's unlawful actions were willful and malicious, and with the deliberate intent to injure Tesla's business, thereby entitling Tesla to exemplary damages and/or attorneys' fees in an amount to be proven at trial pursuant to 18 U.S.C. § 1836(b)(3)(D).

56. Tesla is entitled to an order requiring Defendant, his agents, and all persons acting in concert with him, from using or disclosing, or threatening to use or disclose, the Tesla Trade Secrets, and restraining Defendant from obtaining any benefit from his wrongful possession and use of the Tesla Trade Secrets. Unless enjoined by this Court, said misappropriation of the Tesla Trade Secrets, actual or threatened, will cause great and irreparable injury to Tesla. Tesla has no adequate or other remedy at law for such acts and threatened acts.

Second Cause of Action

(Violation of California's Uniform Trade Secrets Act, Cal. Civ. Code § 3426 *et seq.*)

57. Tesla re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 53 of this Complaint.

58. As set forth above, Defendant misappropriated thousands of Quality Assurance automation software scripts constituting "trade secrets" under the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426, *et seq.* Tesla is the owner of these Tesla Trade Secrets.

59. The Tesla Trade Secrets derive independent economic value from not being generally known to the public, to Tesla's competitors, or to other persons who can obtain economic value from disclosure or use of the information.

60. At all relevant times, Tesla has made reasonable efforts to protect and preserve the secrecy of the Tesla Trade Secrets.

61. Defendant misappropriated the Tesla Trade Secrets within the meaning of Cal. Civ. Code § 3426.1(b) by, *inter alia*, knowingly acquiring the Tesla Trade Secrets through improper means, and disclosing and/or using the Tesla Trade secrets without Tesla's express or implied consent.

62. Defendant knew or had reason to know that, at the time he accessed, downloaded and used the Tesla Trade Secrets, this information was acquired and obtained by improper means and/or under circumstances giving rise to a duty to maintain secrecy or limit use, and that he did not have Tesla's express or implied consent to do so.

63. Defendant acquired the Tesla Trade Secrets by virtue of his employment with Tesla, not through his own independent research and efforts, in direct violation of his legal obligations to Tesla.

64. On information and belief, Defendant failed to fully delete or return the Tesla Trade Secrets that he misappropriated, and continues to use or disclose the Tesla Trade Secrets without Tesla's consent.

65. On information and belief, Defendant has gained, or will gain, substantial benefit from his misappropriation of the Tesla Trade Secrets, to Tesla's substantial detriment.

66. As a result of Defendant's unlawful conduct, the Tesla Trade Secrets have been compromised, and Tesla is substantially threatened by Defendant's further use and/or dissemination of that information.

67. As a direct, proximate, and foreseeable result of Defendant's misappropriation of the Tesla Trade Secrets, Plaintiff has been damaged in an amount not yet ascertained.

68. Defendant's unlawful actions were willful and malicious, and with the deliberate intent to injure Tesla's business, thereby entitling Tesla to exemplary damages pursuant to Cal. Civ. Code § 3426.3(c) and/or attorneys' fees in an amount to be proven at trial pursuant to Cal. Civ. Code § 3246.4.

69. Tesla is entitled to an order requiring Defendant, his agents, and all persons acting in concert with him, from using or disclosing, or threatening to use or disclose, the Tesla Trade Secrets, and restraining Defendant from obtaining any benefit from his wrongful possession and use of the Tesla Trade Secrets. Unless enjoined by this Court, said misappropriation of the Tesla Trade Secrets, actual or threatened, will cause great and irreparable injury to Tesla. Tesla has no adequate or other remedy at law for such acts and threatened acts.

Third Cause of Action

(Breach of Contract)

70. Tesla re-alleges and incorporates by reference each and every allegation contained in paragraphs 1 through 66 of this Complaint.

71. As a condition of his employment with Tesla, Defendant signed and agreed to abide by 1) the terms of an NDA between himself and Tesla and 2) the terms of an employment agreement contained in the offer letter between Defendant and Tesla. Both the NDA and the employment agreement prohibited Defendant from, among other things, using or disclosing the Tesla Trade Secrets.

72. Tesla fully complied with and fulfilled its obligation under the NDA and employment agreement by, among other things, employing the Defendant.

73. While employed by Tesla, Plaintiff breached the NDA and employment agreement by, without authorization or any business purpose, accessing, downloading, transmitting, and

retaining thousands of Quality Assurance automation software scripts constituting the Tesla Trade Secrets, and storing those scripts on a personal cloud storage account.

74. On information and belief, Plaintiff further breached his NDA and employment agreement by providing the Trade Secret information to other unknown individuals or entities after that information had been exfiltrated to Dropbox.

75. Tesla has sustained and will sustain damages as a direct and proximate result of Defendant's breach of contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Tesla prays for judgment in its favor and against Defendant Alex Khatilov, inclusive as follows:

1. Granting temporary, preliminary, and permanent injunctive relief against Defendant, and any persons in active concert or participation with him: (i) enjoining Defendant from obtaining, retaining, using, transmitting, disseminating, or disclosing the Tesla Trade Secrets; (ii) requiring Defendant to immediately return all Tesla equipment, tangible materials, and information that remain in Defendant's possession, custody, or control; (iii) ordering Defendant to identify, and turn over, any property in his possession, custody, or control containing or reflecting the Tesla Trade Secrets, including hard copy documents or any form of electronic storage media; (iv) ordering Defendant to identify any other persons, entities, or locations not within his possession, custody, or control, to which Defendant has transmitted, disseminated, disclosed, or stored any Tesla Trade Secrets; and (v) any other appropriate injunctive relief;

2. Awarding compensatory damages in an amount to be determined at trial;

3. Awarding exemplary damages in an amount to be determined at trial;

4. Awarding interest at the maximum legal rate on all sums awarded;

5. Awarding reasonable attorneys' fees as permitted by law;

6. Awarding all costs of suit and investigation herein; and

7. Awarding such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff Tesla demands a jury trial on all triable issues.

Dated: January 22, 2021

s/ Joseph Alm
Joseph Alm

Joseph Alm
CA Bar # 294362
jalm@tesla.com
901 Page Ave
Fremont, CA 94538
(650) 681-5000

Counsel for Plaintiff
Tesla, Inc.