John M. Desmarais (SBN 320875)
DESMARAIS LLP
101 California Street
San Francisco, CA 94111
(415) 573-1900

Tamir Packin (SBN 317249)
Carson Olsheski (*pro hac vice* pending)
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
212-351-3400

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CISCO SYSTEMS, INC., a California Corporation, CISCO TECHNOLOGY, INC., a California Corporation

Plaintiffs,

v.

WILSON CHUNG, JAMES HE, AND JEDD WILLIAMS, individuals

Defendants.

Case No. _____

JURY TRIAL DEMANDED

COMPLAINT FOR TRADE SECRET MISAPPROPRIATION

Plaintiffs Cisco Systems, Inc. and Cisco Technology, Inc. (collectively "Cisco"), for their Complaint against Defendants Wilson Chung ("Dr. Chung"), James He ("Mr. He"), and Jedd Williams ("Mr. Williams") hereby alleges as follows:

Introduction

1. This is an action for trade secret misappropriation. Cisco has invested significant resources to design, build, and sell its robust unified communications platform, which includes video conferencing software and collaboration endpoints. Cisco's endpoint hardware includes video endpoints, telepresence units, all-in-one video collaboration systems, integrated collaboration room

systems, VoIP and video phones, microphones, cameras, speakers, and headsets. The field of unified communications is highly competitive and characterized by rapid innovation.

2. Cisco also has made substantial and significant investments in developing its routes to market for its collaboration products and services, through extensive engagement of partner, customer, and industry connections by its global sales force. Cisco's global sales force relies upon proprietary information, such as customer lists, pricing models, and forecasts to develop Cisco's go-to-market and business development strategies.

3. Cisco has uncovered evidence that Dr. Chung and Mr. He, two former high-level engineers in Cisco's Unified Communications Technology Group, downloaded thousands of Cisco's highly confidential and proprietary documents ("Cisco Confidential Materials") relating to the design, manufacture, pricing, and market opportunities for both current and unreleased products immediately preceding their departure for a competitor of Cisco. Dr. Chung undertook efforts over a period of weeks preceding his departure to exfiltrate Cisco Confidential Materials to removable hard drives, personal email, cloud storage, and to the competitor's internal intranet, and then used Cisco Confidential Materials while at the competitor. When confronted with evidence of his misappropriation, Dr. Chung destroyed evidence to conceal his actions.

4. Mr. He joined the same competitor after being recruited by Mr. Chung. Prior to his departure, Mr. He copied thousands of files containing Cisco Confidential Materials to an external hard drive. These documents also related to the design, manufacture, pricing, and market opportunities for both current and unreleased products. Cisco has recovered Mr. He's hard drive, and learned that Mr. He accessed a number of these documents while at the same competitor, and, when the misappropriation was uncovered, deleted the files to avoid detection.

5. Cisco also has uncovered evidence that Mr. Williams misappropriated Cisco Confidential Materials relating to Cisco's sales forecasts and business development opportunities, including spending commitments and potential upsides, by exfiltrating these documents from Cisco immediately before his resignation from Cisco to join the same competitor, and by storing a backup of his Cisco laptop on a home server and, on information and belief, maintaining Cisco Confidential Materials on that server after leaving Cisco and starting work at that competitor. Cisco also has

uncovered evidence suggesting that Mr. Williams was offered employment at the same competitor after proposing a go-to-market strategy he dubbed "Project X," which had been developed and refined at Cisco.

6. Defendants' conduct threatens to cause Cisco irreparable harm, potentially depriving Cisco of the opportunity to obtain a first-mover advantage in product development and go-to-market strategies, and depriving Cisco of business opportunities. There is also the threat that Cisco Confidential Materials will be disclosed by Defendants, which will destroy the value of Cisco's trade secret technology and business processes.

The Parties

7. Plaintiff Cisco Systems, Inc., is a company duly organized and existing under the laws of California, having its principal place of business at 170 West Tasman Drive, San Jose, California 95134.

8. Plaintiff Cisco Technology, Inc. is a wholly owned subsidiary of Cisco Systems, Inc., and is a company duly organized and existing under the laws of California, having its principal place of business at 170 West Tasman Drive, San Jose, California 95134.

9. Dr. Chung is an individual residing in this jurisdiction.

10. Mr. He in an individual residing in this jurisdiction.

11. Mr. Williams is an individual residing outside this jurisdiction.

Nature Of The Action

12. This is a civil action for violation of the Defend Trade Secrets Act ("DTSA") under 18 U.S.C. § 1836 *et seq.*, and violation of Cal. Civ. Code § 3426 *et seq*.

Jurisdiction And Venue

13. This Court has subject matter jurisdiction over Cisco's claims for violation of the Defend Trade Secrets Act ("DTSA") pursuant to 28 U.S.C. §§ 1331 because they present a Federal Question.

14. This Court has supplemental subject matter jurisdiction of the pendent state law claims pursuant to 28 U.S.C. § 1367 because they are so related to the DTSA claims that they form part of the same case or controversy.

15. This Court has personal jurisdiction over Dr. Chung because he resides in this district.

16. This Court has personal jurisdiction over Mr. He because he resides in this district.

17. This Court has personal jurisdiction over Mr. Williams because he has purposefully directed his activities to this forum by committing intentional acts within California causing harm to Cisco (a California corporation). Specifically, as outlined in the detailed factual allegations below, Mr. Williams uploaded to cloud storage Cisco Confidential Materials while he was in California immediately preceding his resignation from Cisco. Furthermore, Mr. Williams revealed details of a sales strategy developed at Cisco and for Cisco to the competitor. Mr. Williams himself created the contacts with the competitor in California, at least through his frequent travels and regular visits to its headquarters in California while seeking employment with the competitor. Further still, upon his resignation, Mr. Williams returned his Cisco issued laptop to Cisco's California headquarters in-person, but failed to return the backup of his laptop that he stored on a home server.

18. Venue is proper within this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to these claims occurred within this District.

FACTUAL ALLEGATIONS

A. Dr. Chung

19. Dr. Chung was employed at Cisco as Principal Engineer in Cisco's Unified Communications Technology Group ("UCTG"). Dr. Chung was involved in developing Cisco's collaboration products, including IP telephony solutions and audio headsets. Incumbent with this role was access to some of Cisco's most confidential trade secrets used within the UCTG, including design specifications, schematics, source code, product market analyses, and vendor contract details. Dr. Chung left Cisco in February 2019 to join a competitor. Before doing so, Dr. Chung, without authorization, willfully and maliciously misappropriated Cisco Confidential Materials to use for his own benefit at the competitor, and to the detriment of Cisco. Subsequently, Dr. Chung recruited his former Cisco colleague, James He, to join the competitor.

20. Dr. Chung began working for Cisco as a Technical Leader in March 2007.

21. On May 7, 2012, Dr. Chung became Principal Engineer of Cisco's UCTG.

22. Dr. Chung claims that his personal and work laptops were stolen around Thanksgiving 2018.

23. Subsequent to the alleged theft, Dr. Chung used a Lenovo ThinkPad X1 with serial number PF0Z3DLE ("Lenovo laptop") issued by Cisco as his primary work computer.

24. On November 14, 2018, Cisco leased a MacBook Pro from IBM Global Finance which was assigned to Dr. Chung to use as a secondary work computer. Dr. Chung's department incurred the cost for this MacBook Pro. This MacBook Pro (serial number C02W186W186HV2M) ("MacBook") was shipped to Cisco and later delivered to Dr. Chung.

25. Dr. Chung does not own, and has never owned, the MacBook.

26. Dr. Chung is not the lessee, and has never been the lessee, of the MacBook.

27. Cisco did not authorize Dr. Chung's retention of the MacBook when his employment with Cisco ended.

28. Dr. Chung has no right to possess the MacBook after his employment with Cisco terminated, and also had no right to possess the MacBook when he began to work at the competitor.

29. On February 3, 2019, Dr. Chung downloaded over 3000 files from Cisco's internal document repositories. These documents are Cisco Confidential Materials and relate to, among other things, Cisco's contributions to 5G technology (such as its market opportunities), and design specifications of a pre-release video conferencing display prototype.

30. On February 3, 2019, Dr. Chung connected a Seagate Expansion Drive with serial number NAA77962 ("First Seagate drive") to his Lenovo Laptop.

31. Dr. Chung has not made this Seagate Expansion Drive available for inspection by either Cisco or the competitor.

32. On February 3, 2019, Dr. Chung connected a Samsung Flash Drive with serial number 374718110032913 ("Samsung Drive") to his Lenovo laptop five times.

33. Dr. Chung copied Cisco Confidential Materials to the Samsung Drive.

34. On February 3, 2019, Dr. Chung uploaded files from the MacBook to his personal iCloud account, including Cisco's source code for debugging a user interface.

35. On February 6, 2019, Dr. Chung copied 129 files containing Cisco Confidential Materials that relate to vendor product roadmaps and a pre-release video conferencing display prototype to a Seagate Expansion SCSI Disk Device with serial number 26977AAN ("Second Seagate drive"). The pre-release video conferencing display prototype documents included user experience design documentation, user interview feedback, artwork prototypes, and schematics.

36. On February 6, 2019, Dr. Chung connected the Samsung Drive to the Lenovo laptop four times.

37. On February 6, 2019, Dr. Chung connected a Sandisk UltraFit storage drive with serial number 4C50001291121118332 ("Sandisk drive") to his Lenovo laptop two times.

38. On information and belief, on February 6, 2019, Dr. Chung uploaded a folder entitled "Toyshop" from his Lenovo laptop to cloud storage. This folder included Cisco Confidential Materials such as design details and specifications relating to Cisco's collaboration endpoints, including Cisco's sound bar products.

39. Dr. Chung's misappropriation of Cisco's Confidential Materials was organized, premeditated, and intentional.

40. On February 6, 2019, Dr. Chung created various folders on the Samsung drive named after an internal Cisco project codename.

41. On February 6, 7, and 8, 2019, Dr. Chung created various folders on the Second Seagate drive named after numerous additional Cisco project codenames.

42. On February 7, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop.

43. On February 8, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop twice.

44. On information and belief, on February 8, 2019, Dr. Chung uploaded Cisco Confidential Materials to cloud storage, including a presentation detailing go-to-market strategy, design details, cost modeling, and pricing information for a pre-release video conferencing display product.

45. On February 9, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop twice.

46. On February 10, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop.

47. On February 11, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop twice.

48. On February 12, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop five times.

49. On February 13, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop twice.

50. On February 13, 2019, the MacBook was physically connected to Cisco's corporate network.

51. On February 13, 2019, Dr. Chung informed his manager that he was leaving Cisco.

52. During that February 13, 2019 conversation between Dr. Chung and his manager, Dr. Chung told his manager that he was not sure where he would be working, but that he was considering joining Apple.

53. On February 14, 2019, Dr. Chung connected the Second Seagate drive to the Lenovo laptop four times.

54. On February 21, 2019, Dr. Chung told a vendor representative that his last day at Cisco would be February 22, 2019.

55. Dr. Chung told the competitor that his last day at Cisco was February 22, 2019.

56. Dr. Chung's last day at Cisco was, in fact, February 28, 2019.

57. On February 24, 2019, Dr. Chung forwarded an email and attachment from his Cisco email account to his personal Gmail account. The attached document, clearly marked Cisco confidential, related to Cisco's prospective market positioning.

58. On February 25, 2019, Dr. Chung downloaded more than 100 recordings of Webex presentations to his Lenovo laptop. On information and belief, these recordings related to the design,

manufacture, pricing, and market opportunities for Cisco's Unified Communications product portfolio.

59. On February 25, 2019, Dr. Chung connected the Second Seagate drive to his Lenovo laptop six times.

60. On February 25, 2019, Dr. Chung created a folder entitled "Webex_Recordings" on the Second Seagate drive.

61. From February 26, 2019 through February 28, 2019, Dr. Chung was an employee of both Cisco and the competitor.

62. On February 26, 2019, Dr. Chung began work at the competitor.

63. On February 26, 2019, Dr. Chung logged into the MacBook.

64. On February 26, 2019, Dr. Chung emailed vendor representatives from his Cisco email account to inform them that his last day at Cisco would be February 28, 2019.

65. On February 26, 2019, Dr. Chung forwarded an email from his Cisco email account to his personal Gmail account. This email thread included "minutes" from a Cisco meeting.

66. On February 26, 2019, Dr. Chung logged into the competitor's "Sharepoint" site from the Lenovo laptop. Dr. Chung uploaded to the competitor's Sharepoint, among other things, a spreadsheet entitled Endpoints and Accessories ("EA document").

67. The EA document contains Cisco Confidential Materials, including component specifications and competitive differentiators for Cisco's current and not yet released endpoint products.

68. On February 27, 2019, Dr. Chung forwarded an email from his Cisco email account to his personal Gmail account with details about a vendor contract, which also included a payment terms.

69. On February 27, 2019, Dr. Chung accessed his Google drive from the Lenovo laptop.

70. On February 27, 2019, Dr. Chung went to Cisco's office and returned his badge and the Lenovo laptop to Cisco. Dr. Chung arrived at approximately 3:00pm, had coffee with a Cisco colleague, and posed for a group photo with members of Cisco's UCTG. Dr. Chung did not turn in the MacBook, First Seagate drive, Second Seagate drive, SanDisk drive, or Samsung drive.

71. On February 28, 2019, Dr. Chung forwarded an email from his Cisco email account to his personal Gmail account with details about sensor requirements for Cisco products.

72. On March 8, 2019, Dr. Chung emailed the EA document from his personal Gmail account to his new business email account.

73. On March 8, 2019, Dr. Chung emailed a file marked as Cisco Confidential and entitled "Webex Workplace Vision and Strategy – Compete" from his personal Gmail account to his new business email account.

74. By March 9, 2019, Dr. Chung began recruiting James He to join the competitor.

75. As of March 28, 2019, the MacBook had not been returned to Cisco. Cisco contacted Dr. Chung to secure return of the MacBook.

76. On March 29, 2019, Cisco contacted Dr. Chung and requested return of the MacBook. Dr. Chung insisted that he owned the MacBook and asked Cisco to check with Cisco's IT department.

77. On April 9, 2019, after checking with Cisco's IT department, Cisco notified Dr. Chung that the MacBook was Cisco property and must be returned. Dr. Chung subsequently confirmed that he possessed the MacBook. Cisco followed up with Dr. Chung on April 10, April 11, April 14, April 15, and April 18, but Dr. Chung refused to return the MacBook.

78. Dr. Chung accessed Cisco's confidential and proprietary business information while employed at the competitor.

79. After being notified of Cisco's concerns that Dr. Chung had misappropriated Cisco's trade secrets, on September 26, 2019, the competitor informed Cisco that it had found five documents on Dr. Chung's devices, including the EA document that Dr. Chung had previously uploaded to the competitor's Sharepoint, which potentially included Cisco's confidential and proprietary business information.

80. Dr. Chung downloaded the EA document from the competitor's Sharepoint to his new work computer issued by the competitor.

81. On information and belief, Dr. Chung accessed this file, and others, for his own benefit, and for the benefit of the competitor, to Cisco's detriment.

82. On September 19, 2019, counsel for Cisco wrote Dr. Chung a letter putting Dr. Chung on notice to preserve all documents and things related to the potential misappropriation of Cisco's confidential and proprietary business information.

83. After receiving this preservation notice, Dr. Chung took steps to conceal his misappropriation. For example, after receiving the preservation notice, Dr. Chung:

a. permanently deleted iCloud backups;

b. permanently deleted Cisco Confidential Materials from the MacBook;

c. deleted Cisco Confidential Materials from the Sandisk drive;

d. deleted Cisco Confidential Materials from the Samsung drive; and

e. propounded a demonstrably false explanation for failing to return the Second Seagate drive to Cisco.

84. After receiving this preservation notice, and before delivering the MacBook, Sandisk drive, his personal iPad, and Samsung drive to his attorney to eventually return to Cisco, Dr. Chung performed internet searches such as "how to permanently delete icloud backup," and "how to see what is [sic] the thumb drive without detection."

85. The Cisco competitor is in the IP telephony, headset, video, and collaboration space.

86. Dr. Chung understood that his employment by Cisco created a relationship of confidence and trust with respect to confidential and proprietary information. Dr. Chung's Proprietary Information and Inventions Agreement ("Chung PIIA") prohibited Dr. Chung during his employment with Cisco from becoming an employee of any other firm engaged in a business in any way competitive with the Company or involved in the design, development, marketing, sale, or distribution of any networking or software products without first informing Cisco and obtaining its consent.

87. By the terms of the Chung PIIA, Dr. Chung agreed that he would "not remove any Company Documents and Materials from the business premises of the Company or deliver any Company Documents and Materials to any person or entity outside of the Company, except as [] required to do in connection with performing the duties of [his] employment." Dr. Chung also agreed that "immediately upon the termination of [his] employment," he would "return all Company

Documents and Materials, apparatus, equipment and other physical property, or any reproductions of such property . . . ."

B. Mr. He

88. Mr. He was an engineer with Cisco, who played an integral role in developing many of Cisco's successful products. Incumbent with Mr. He's responsibilities was access to some of Cisco's most confidential trade secrets used within the UCTG, including design specifications, schematics, source code, product market analyses, and vendor contract details. Mr. He was slated to be promoted to Principal Engineer. Mr. He left Cisco in June 2019 to join the same competitor.

89. Before leaving Cisco, Mr. He, without authorization, willfully and maliciously misappropriated Cisco's confidential and proprietary business information to use for his own benefit at the same competitor, and to the detriment of Cisco.

90. On March 1, 2019, Dr. Chung communicated details of his new position at the same competitor to Mr. He.

91. On March 9, 2019, Dr. Chung told Mr. He that the same competitor was interested in having Mr. He work there.

92. Mr. He regularly took photographs of Cisco Confidential Materials on his iPhone Max.

93. For example, on May 13, 2019, Mr. He took a photograph of a financial presentation containing Cisco Confidential Materials, which included Cisco's Q3 financial highlights, largest deals, and comparative revenue by category.

94. On May 30, 2019, Mr. He copied Cisco Confidential Materials, including architectural design documents relating to Cisco's unreleased headset concepts to a Lacie external Hard Drive with serial number 0000NL37HDBX ("Lacie drive").

95. On June 1, 2019, Mr. He was notified that he was being promoted to Principal Engineer.

96. On June 1, 2019, Mr. He traveled from his home in China to California. Mr. He told his manager that this was a personal trip. Mr. He remained in California until June 9, 2019.

97. On June 3, 2019, Mr. He took a photo from his iPhone Max of a hardware diagram for a Cisco headset prototype.

98. On June 5, 2019, Mr. He took photographs from his iPhone Max of Cisco Confidential Materials that discussed Cisco's emerging business opportunities in the collaboration space. On this date, Mr. He also downloaded a headset test report containing Cisco Confidential Materials.

99. On June 6, 2019, Mr. He informed his manager that he was resigning from Cisco.

100. On June 6, 2019, Mr. He connected to Cisco's Virtual Private Network from a Comcast IP address in the United States.

101. On June 6, 2019, Mr. He copied over 100 documents to the Lacie drive. These documents included Cisco Confidential Materials, such as design and configuration documents relating to Cisco's unreleased headset prototypes. Also included in these files was information relating to vendor roadmaps for Cisco's products.

102. On June 10, 2019, Mr. He had an in-person meeting with his manager in China. In this meeting, Mr. He discussed his resignation with his manager. Mr. He stated that he was not going to the same competitor, but that he was moving to Guangzhou for family reasons.

103. On June 11, 2019, Mr. He copied an email archive from his Cisco email account to the Lacie drive. On June 14, 2019, Mr. He copied two additional archives from his Cisco email account to the Lacie drive. These archives contain Cisco Confidential Materials. Discussions over email contained in the archive reflect Cisco's strategic product development decisions. The email archives also include, as email attachments, technical design documents and presentations containing Cisco's trade secrets.

104. On June 17, 2019, Mr. He copied approximately 200 emails from his Cisco email trash folder to the Lacie drive. These emails contain Cisco Confidential Materials and relate to design details for a then unreleased IP telephone project.

105. On June 18, 2019, Mr. He copied approximately 1500 files to the Lacie drive. These files contain Cisco Confidential Materials and include internal emails, architectural documents, marketing plans, and cost information.

106. On June 20, 2019, Mr. He copied approximately 90 files to the Lacie drive. These files contain Cisco Confidential Materials and relate to Cisco's headset projects.

107. On June 21, 2019, Mr. He left Cisco. Mr. He retained the Lacie drive.

108. On information and belief, Mr. He joined the same competitor on or around June 24, 2019.

109. On June 27, 2019, Mr. He accessed Cisco Confidential Materials stored on the Lacie drive, including a schematic for an unreleased IP telephone project. Mr. He again accessed this file on July 3, 2019.

110. On July 1, 2019, Mr. He accessed Cisco Confidential Materials stored on the Lacie drive, including a vendor's roadmap update created for Cisco.

111. On July 15, 2019, Mr. He accessed Cisco Confidential Materials stored on the Lacie drive, including a full engineering specification for a next-generation conference room collaboration device. Mr. He had previously copied this file to the Lacie drive on May 30, 2019.

112. On information and belief, Mr. He accessed these Cisco Confidential Materials for his own benefit, and for the benefit of the same competitor, to Cisco's detriment.

113. On August 2, 2019, counsel for Cisco put Mr. He on notice to preserve all documents and things related to the potential misappropriation of Cisco's confidential and proprietary business information.

114. On August 5, 2019, Mr. He deleted thousands of Cisco files containing Cisco's confidential and proprietary business information from the Lacie drive. On information and belief, Mr. He deleted these files because the same competitor had commenced an internal investigation into the misappropriation, and Mr. He was requested to turn the Lacie drive to the same competitor's investigators. In addition to the aforementioned files and file types, Mr. He deleted various source code library stacks from the Lacie drive.

115. Mr. He understood that his employment by Cisco created a relationship of confidence and trust with respect to confidential and proprietary information.

116. By the terms of Mr. He's Proprietary Information and Inventions Agreement ("He PIIA"), Mr. He agreed that he would "not remove any Company Documents and Materials from the business premises of the Company or deliver any Company Documents and Materials to any person or entity outside the Company, except as [] required to do in connection with performing the duties of [his] employment." Mr. He also agreed that "immediately upon the termination of [his] employment,"

he would "return all Company Documents and Materials, apparatus, equipment and other physical property, or any reproductions of such property . . . ."

C. Mr. Williams

117. Mr. Williams was a Managing Director in Global Collaboration Sales at Cisco until October 2019. In this role, he had global responsibility for developing sales and marketing strategies for bringing Cisco's suite of collaboration products to market. Mr. Williams started at Cisco in 1998 as a Systems Engineer II.

118. On January 27, 2018, Mr. Williams emailed his resume to a former Cisco colleague, whom he worked with at Cisco to collectively execute foundational business development strategies of "Project X" on Cisco's behalf.

119. On January 29, 2019, an Executive Vice President of the same competitor, who was formerly at Cisco, communicated with Mr. Williams over LinkedIn.

120. On information and belief, from January 29, 2019 to October 14, 2019, Mr. Williams met or otherwise corresponded with the same competitor's executives, recruiters, and other employees no fewer than 19 times.

121. On information and belief, on June 10, 2019, Mr. Williams sent himself an email from his phone with prep notes for an interview with the same competitor. These notes say, among other things, "Have to promise not to say anything," "make sure he knows I know channels," "xx% of the business goes through channel today," "I own SPaaCH [Service Provider as a Channel] today," and "you can't be successful at Cisco without understanding how to drive the channel."

122. On June 28, 2019, Mr. Williams traveled to San Francisco to interview with the same competitor.

123. On September 6, 2019, Mr. Williams drafted an email to an Executive Vice President of the same competitor, who was formerly at Cisco, from his Cisco email account to the Executive Vice President's personal Gmail account. Mr. Williams proposed to the Executive Vice President a vision for how he could hit the ground running at the same competitor entitled "Project X." The proposal outlined Mr. Williams vision of how the same competitor could take market share from, among others, Cisco. Mr. Williams explained that "Project X" was a "play I drove VERY successfully

at Cisco … and a play that I'd like to repeat again. I could literally start on this fulltime on Monday . . . and turn this idea into a complete plan that will have a material positive impact on this launch." Mr. Williams indicated that he looked forward to a live discussion with the Executive Vice President.

124. On information and belief, Mr. Williams received an offer to join the same competitor shortly after proposing "Project X" to an Executive Vice President of the same competitor, who was formerly at Cisco.

125. Mr. Williams traveled to Santa Clara, California on October 13, 2019.

126. On October 14, 2019, Mr. Williams uploaded to cloud storage 12 Cisco sales forecasting spreadsheets for Fiscal Year 2020 using Firefox on his Cisco laptop. These files, which contain detailed information about Cisco's sales forecasts and opportunities, including customer names, commitments, and upsides.

127. Mr. Williams negotiated a mutual separation agreement that same day. Even though he was directly asked about his plans after leaving Cisco, he claimed that he was going to work at his church and focus on personal issues. In light of these circumstances and to help Mr. Williams with his family, Cisco offered Mr. Williams two months sales pay, in addition to a lump sum payment to cover two months COBRA health care premiums. Mr. Williams accepted this offer.

128. Also, on October 14, 2019, after uploading the sales forecasts, Mr. Williams returned his laptop to Cisco's San Jose office in person.

129. Mr. Williams' employment with Cisco terminated on October 15, 2019.

130. Mr. Williams joined the same competitor shortly thereafter.

131. During the course of his employment at Cisco, Mr. Williams ran a home server that he used to store a Time Machine backup of his Cisco laptop. This backup contained, and, on information and belief, still contains Cisco's confidential and proprietary documents. Mr. Williams did not return this backup to Cisco upon his termination.

COUNT I

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Dr. Chung

132. Paragraphs 1 through 131 are incorporated by reference as if fully stated herein.

133. Dr. Chung's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

134. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco technical information such as source code, schematics, design details and specifications, user feedback, design documentation, and features relating to Cisco's existing and future products, as well as Cisco business information such as marketing strategy, cost and pricing information, and payment information.

135. Dr. Chung has maintained and continues to maintain in his possession the wrongfully acquired Cisco documents and materials after the termination of his employment with Cisco.

136. Dr. Chung used and continues to use Cisco trade secret contained in these wrongfully acquired Cisco documents by way of providing these documents to a Cisco competitor and/or accessing these documents.

137. Dr. Chung's past (after leaving Cisco) and ongoing possession, acquisition, disclosure, and/or use of Cisco trade secrets is without Cisco's express or implied consent.

138. Cisco trade secrets were developed over time after expenditure of significant effort and resources.

139. Cisco trade secrets are not publicly available, and are kept within the knowledge and know-how of Cisco employees under strict confidentiality obligations, and only shared with parties bound by contractual obligations of confidentiality.

140. Cisco has taken reasonable measures to keep its trade secret information secret.

141. Cisco communicates the importance of maintaining confidentiality to its employees in various means and forms, including but not limited to the Proprietary Information and Inventions Agreements and termination letters.

142. On February 9, 2007, Dr. Chung executed the Chung PIIA in consideration for his employment with Cisco.

143. The Chung PIIA protects Cisco's proprietary information, which was defined in the Chung PIIA as (i) information that was or will be developed, created, or discovered by or on behalf of Cisco, or which became or will become known by, or was or is conveyed to Cisco, which has

commercial value in Cisco's business, or (ii) any other information that Cisco does not want publicly disclosed. The Chung PIIA further states that Cisco proprietary information includes but is not limited to software programs and subroutines, source and object code, algorithms, trade secrets, designs, technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or not), works of authorship, formula, business and product development plans, customer lists, terms of compensation and performance levels of Cisco employees, and other information concerning Cisco's actual or anticipated business, research or development, or which is received in confidence by or for Cisco from any other source, or any document that is marked as "confidential."

144. By signing the Chung PIIA, Dr. Chung agreed that he would "not remove any Company Documents and Materials from the business premises of Cisco or deliver any Company Documents and Materials to any person or entity outside of Cisco, except as [] required to do in connection with performing the duties of [his] employment." Dr. Chung also agreed that "immediately upon the termination of [his] employment," he would "return all Company Documents and Materials, apparatus, equipment and other physical property, or any reproductions of such property . . . ."

145. Dr. Chung took intentional and systematic steps during at least a three and a half week period before the termination of his employment to transfer thousands of documents containing Cisco Confidential Materials out of Cisco.

146. Upon termination of Dr. Chung's employment at Cisco on February 18, 2019, Cisco delivered to Dr. Chung a termination letter, reminding Dr. Chung of his continuing obligations to Cisco, including the duty to maintain confidentiality of Cisco confidential information, the duty of non-solicitation within one year after the termination of Dr. Chung's employment, and the duty to return any Cisco documents as soon as possible.

147. Dr. Chung did not return the Cisco Confidential Materials that he had systematically transferred out of Cisco.

148. Cisco implements security measures such as electronic access points to restrict access to Cisco's confidential and proprietary information.

149. Cisco trade secrets derive independent economic value, actual or potential, from not being generally known to, and/or not being readily ascertainable through proper means by, the public or other persons who can obtain economic value from the disclosure or use of the information.

150. Cisco's trade secrets at issue in this case are related to products that are placed in or are intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. § 1836.

151. Defendant Dr. Chung's misappropriation of Cisco's trade secret information was willful and malicious.

152. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

153. On information and belief, if Defendant Dr. Chung's conduct is not enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to Cisco's detriment Cisco's trade secret information.

154. Because Cisco's remedy at law is inadequate, Cisco seeks preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant Dr. Chung's continued misappropriation of Cisco's trade secret information.

COUNT II

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Dr. Chung

155. Paragraphs 1 through 154 are incorporated by reference as if fully stated herein.

156. Dr. Chung's misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 et seq.

157. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

158. Defendant's misappropriation of Cisco's trade secret information was willful and malicious.

159. On information and belief, if Dr. Chung is not enjoined, the Defendant will continue to misappropriate, disclose, and use for his own benefit and the benefit of others and to Cisco's detriment Cisco's trade secret information.

160. Because Cisco's remedy at law is inadequate, Cisco seeks preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

COUNT III

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. He

161. Paragraphs 1 through 160 are incorporated by reference as if fully stated herein.

162. Mr. He's misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

163. Cisco Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco technical information such as design and architectural documents, hardware diagrams, schematics, source code stacks, and engineering specification relating to existing and future Cisco products, as well as business information such as relating to marketing plans, business opportunities, and revenue and cost information.

164. Mr. He maintained in his possession these wrongfully acquired Cisco documents and materials after the termination of his employment with Cisco.

165. Mr. He has used Cisco trade secrets contained in these wrongfully acquired Cisco documents.

166. Mr. He's past (after leaving Cisco) and ongoing possession, acquisition, disclosure, and/or use of Cisco trade secrets is without Cisco's express or implied consent.

167. Cisco trade secrets were developed over time after expenditure of significant effort and resources.

168. Cisco trade secrets are not publicly available, and are kept within the knowledge and know-how of Cisco employees under strict confidentiality obligations, and only shared with parties bound by contractual obligations of confidentiality.

169. Cisco has taken reasonable measures to keep its trade secret information secret.

170. Cisco communicates the importance of maintaining confidentiality to its employees in various means and forms, including but not limited to the Proprietary Information and Inventions Agreements and termination letters.

171. On March 8, 1999, Mr. He executed the He PIIA in consideration for his employment with Cisco.

172. The He PIIA protects Cisco's proprietary information, which was defined in the He PIIA as information that was developed, created, or discovered by or on behalf of Cisco, or which became or will become known by, or was or is conveyed to Cisco, which has commercial value in Cisco's business. The He PIIA further states that Cisco proprietary information includes but is not limited to software programs and subroutines, source and object code, algorithms, trade secrets, designs, technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or not), works of authorship, formula, business and product development plans, customer lists, terms of compensation and performance levels of Cisco employees, and other information concerning Cisco's actual or anticipated business, research or development, or which is received in confidence by or for Cisco from any other person.

173. By signing the He PIIA, Mr. He agreed that he would "not remove any Company Documents and Materials from the business premises of [Cisco] or deliver any Company Documents and Materials to any person or entity outside [Cisco], except as [] required to do in connection with performing the duties of [his] employment." Mr. He also agreed that "immediately upon the termination of [his] employment," he would "return all Company Documents and Materials, apparatus, equipment and other physical property, or any reproductions of such property . . . ."

174. Mr. He took intentional and systematic steps at least during a six week period before the termination of his employment to transfer thousands of documents containing Cisco Confidential Materials out of Cisco.

175. Cisco implements security measures such as electronic access points to restrict access to Cisco's confidential and proprietary information.

176. Cisco trade secrets derive independent economic value, actual or potential, from not being generally known to, and/or not being readily ascertainable through proper means by, the public or other persons who can obtain economic value from the disclosure or use of the information.

177. Cisco's trade secrets at issue in this case are related to products that are placed in or are intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. § 1836.

178. Defendant Mr. He's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. § 1836(b)(3)(C) and its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

179. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

180. On information and belief, if Defendant Mr. He's conduct is not remedied and/or enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to Cisco's detriment Cisco's trade secret information.

181. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Mr. He's continued misappropriation of Cisco's trade secret information.

COUNT IV

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. He

182. Paragraphs 1 through 181 are incorporated by reference as if fully stated herein.

183. Mr. He's misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 et seq.

184. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

185. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

186. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

187. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their own benefit and to Cisco's detriment Cisco's trade secret information.

188. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, preliminary and permanent injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

COUNT V

Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836 by Mr. Williams

189. Paragraphs 1 through 188 are incorporated by reference as if fully stated herein.

190. Mr. Williams' misappropriation of trade secrets is actionable under the Defend Trade Secrets Act, 18 U.S.C. § 1836.

191. Cisco's Confidential Materials contained trade secrets under 18 U.S.C. § 1839(3). For example, these trade secrets include Cisco's customer lists with additional non-public information that is not readily available, such as purchase commitments and "upside." On information and belief, the Cisco documents stored on Mr. Williams' server backup include Cisco's trade secrets such as customer lists, pricing information and strategic business development plans.

192. On information and belief, Mr. Williams maintained possession of Cisco Confidential Materials after the termination of his employment with Cisco.

193. On information and belief, Mr. Williams has used Cisco trade secrets contained in these wrongfully acquired Cisco documents.

194. Mr. Williams' past (after leaving Cisco) and ongoing possession, acquisition, disclosure, and/or use of Cisco trade secrets is without Cisco's express or implied consent.

195. Cisco trade secrets were developed over time after expenditure of significant effort and resources.

196. Cisco trade secrets are not publicly available, and are kept within the knowledge and know-how of Cisco employees under strict confidentiality obligations, and only shared with parties bound by contractual obligations of confidentiality.

197. Cisco has taken reasonable measures to keep its trade secret information secret.

198. Cisco communicates the importance of maintaining confidentiality to its employees in various means and forms, including but not limited to the Proprietary Information and Inventions Agreements and termination letters.

199. On July 20, 1998, Mr. Williams executed the Williams PIIA in consideration for his employment with Cisco.

200. The Williams PIIA protects Cisco's proprietary information, which was defined in the Williams PIIA as information that was developed, created, or discovered by or on behalf of Cisco, or which became or will become known by, or was or is conveyed to Cisco, which has commercial value in Cisco's business. The Williams PIIA further states that Cisco proprietary information includes but is not limited to software programs and subroutines, source and object code, algorithms, trade secrets, designs, technology, know-how, processes, data, ideas, techniques, inventions (whether patentable or not), works of authorship, formula, business and product development plans, customer lists, terms of compensation and performance levels of Cisco employees, and other information concerning Cisco's actual or anticipated business, research or development, or which is received in confidence by or for Cisco from any other person.

201. By signing the Williams PIIA, Mr. Williams agreed that he would "not remove any Company Documents and Materials from the business premises of [Cisco] or deliver any Company Documents and Materials to any person or entity outside [Cisco], except as [] required to do in connection with performing the duties of [his] employment." Mr. Williams also agreed that "immediately upon the termination of [his] employment," he would "return all Company Documents

and Materials, apparatus, equipment and other physical property, or any reproductions of such property . . . ."

202. Before leaving Cisco, Mr. Williams took intentional steps to transfer Cisco Confidential Materials out of Cisco.

203. Cisco implements security measures such as electronic access points to restrict access to Cisco's confidential and proprietary information.

204. Cisco trade secrets derive independent economic value, actual or potential, from not being generally known to, and/or not being readily ascertainable through proper means by, the public or other persons who can obtain economic value from the disclosure or use of the information.

205. Cisco's trade secrets at issue in this case are related to products that are placed in or are intended to be placed in, interstate or foreign commerce due to the fact that Cisco sells its products around the world. Thus, the trade secrets are covered by the federal trade secrets act, 18 U.S.C. § 1836.

206. Defendant Mr. Williams' misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under 18 U.S.C. § 1836(b)(3)(C) and its attorneys' fees and costs under 18 U.S.C. § 1836(b)(3)(D).

207. Under 18 U.S.C. § 1836(c), this Court has original federal jurisdiction over this claim.

208. On information and belief, if Defendant Mr. Williams' conduct is not remedied and /or enjoined, Defendant will continue to misappropriate, disclose, and use for his own benefit and to Cisco's detriment Cisco's trade secret information.

209. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Mr. Williams' continued misappropriation of Cisco's trade secret information.

COUNT VI

Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426 by Mr. Williams

210. Paragraphs 1 through 209 are incorporated by reference as if fully stated herein.

211. Mr. Williams' misappropriation of trade secrets is independently actionable under California's Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*

212. Under 28 U.S.C. § 1367, this Court has jurisdiction over this claim.

213. Cisco is entitled to recover damages in the form of actual loss, unjust enrichment and/or reasonable royalty. Cal. Civ. Code § 3426.3(a),(b).

214. Defendant's misappropriation of Cisco's trade secret information was willful and malicious, further entitling Cisco to recover exemplary damages under Cal. Civ. Code § 3426.3 and its attorneys' fees and costs under Cal. Civ. Code § 3426.4.

215. On information and belief, if the Defendant's conduct is not remedied, and if the Defendant is not enjoined, the Defendant will continue to misappropriate, disclose, and use for their own benefit and to Cisco's detriment Cisco's trade secret information.

216. Because Cisco's remedy at law is inadequate, Cisco seeks, in addition to damages, injunctive relief to recover and protect its confidential, proprietary, and trade secret information and other legitimate business interests. Injunctive relief is necessary to eliminate the commercial advantage that otherwise would be derived from Defendant's continued misappropriation of Cisco's trade secret information. Cisco is entitled to injunctive relief under Cal. Civ. Code §3426.2.

Prayer For Relief

WHEREFORE, CISCO prays for judgment as follows:

A. Impose preliminary and permanent injunction against Defendants;

B. Award compensatory damages against Messrs. He and Williams according to the proof;

C. Award punitive and exemplary damages to deter similar wrongdoings;

D. Award prejudgment interest at the maximum legal rate as allowed by the law;

E. Award reasonable attorney's fees;

F. Award costs of suit herein incurred; and

G. Such other and further relief as this Court deems just and proper.

Demand For Jury Trial

Plaintiff Cisco hereby demands a trial by jury on all issues so triable.

Dated: November 18, 2019

By: /s/ *John M. Desmarais*

John M. Desmarais (SBN 320875)
DESMARAIS LLP
101 California Street
San Francisco, CA 94111
(415) 573-1900

Tamir Packin (SBN 317249)
Carson Olsheski (*pro hac vice* pending)
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
212-351-3400

Attorneys for Plaintiffs