

1 John M. Desmarais (SBN 320875)  
DESMARAIS LLP  
2 101 California Street  
San Francisco, CA 94111  
3 (415) 573-1900

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

7 *Attorneys for Plaintiffs*

8  
9  
10 **UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

11  
12 CISCO SYSTEMS, INC., a California  
Corporation, CISCO TECHNOLOGY, INC., a  
California Corporation

13  
14 Plaintiffs,

15 v.

16 WILSON CHUNG, JAMES HE, AND JEDD  
WILLIAMS, individuals

17 Defendants.

Case No. \_\_\_\_\_

**JURY TRIAL DEMANDED**

18  
19 **COMPLAINT FOR TRADE SECRET MISAPPROPRIATION**

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

23 **Introduction**

24 1. This is an action for trade secret misappropriation. Cisco has invested significant  
25 resources to design, build, and sell its robust unified communications platform, which includes video  
26 conferencing software and collaboration endpoints. Cisco’s endpoint hardware includes video  
27 endpoints, telepresence units, all-in-one video collaboration systems, integrated collaboration room  
28

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

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

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

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

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

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

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

9 **The Parties**

10 7. Plaintiff Cisco Systems, Inc., is a company duly organized and existing under the laws  
11 of California, having its principal place of business at 170 West Tasman Drive, San Jose, California  
12 95134.

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

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

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

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

19 **Nature Of The Action**

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

22 **Jurisdiction And Venue**

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

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

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

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

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

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

15 **FACTUAL ALLEGATIONS**

16 **A. Dr. Chung**

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

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

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

28

1 22. Dr. Chung claims that his personal and work laptops were stolen around Thanksgiving  
2 2018.

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

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

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

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

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

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

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

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

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

23 32. On February 3, 2019, Dr. Chung connected a Samsung Flash Drive with serial number  
24 374718110032913 (“Samsung Drive”) to his Lenovo laptop five times.

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

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

28

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.