

UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF WISCONSIN

---

EPIC SYSTEMS CORPORATION, a  
Wisconsin Corporation,

Plaintiff,

Case No. 14-CV-748

v.

**DEMAND FOR JURY TRIAL**

TATA CONSULTANCY SERVICES  
LIMITED, an Indian Corporation; and TATA  
AMERICA INTERNATIONAL  
CORPORATION (dba TCS AMERICA), a  
New York Corporation,

Defendants.

---

**COMPLAINT**

---

Plaintiff Epic Systems Corporation (“Epic”) complains against Defendants Tata Consultancy Services Limited (“TCS India”), and Tata America International Corporation (dba “TCS America”), as follows:

**NATURE OF THE CASE**

1. Epic seeks damages and injunctive relief to prevent TCS India and TCS America (cumulatively “TCS”), and potentially other Tata-related entities such as Tata Group (India) and Tata Sons Limited, from disclosing or misusing documents, data, confidential information, trade secrets, and other valuable information and intellectual property stolen from Epic. The misuse and disclosure of valuable Epic property flows from a series of computer fraud and computer theft violations by TCS personnel in the United States and India.

2. Epic makes software for mid-size and large medical groups, hospitals, and integrated healthcare organizations. Epic works with customers that include community

hospitals, academic facilities, children's organizations, safety net providers, and multi-hospital systems. Epic's integrated software spans clinical, access, revenue and managed care plan functionality. Epic's software manages the collection and storage of patient data and care process data into a common database, including records of patient admissions and discharges, pharmacy, specialty care, billing, insurance benefits, and referral information. Epic's software is used by an estimated 281,000 physicians worldwide to manage the care and records of an estimated 169 million patients. The company and its high quality, integrated software products are recognized leaders in the healthcare software industry.

3. Epic is a privately held company. It has internally developed, installed, and supported its applications since its inception in 1979. The know-how and development of Epic's software is the result of careful, hard work by its employees at a tremendous monetary cost and expenditure of man-hours over a period of decades.

4. Epic's intellectual property, confidential information, documents, and trade secrets are of the utmost importance to Epic and the company takes reasonable means to protect those assets. Epic shares its confidential information and trade secrets on a need-to-know basis with its employees and certain customers subject to confidentiality obligations designed to protect Epic's computer network, software, documents, confidential information, and trade secrets. Epic regularly requires parties with which it does business to execute non-disclosure agreements. Epic utilizes processes and tools to monitor whether its materials are publicly disclosed, and has processes in place to review materials before publication from its customers.

5. Epic maintains its confidential business information on its computer systems that can be accessed only by authorized users. Epic does allow third parties (such as customers and consultants working for customers) to access some information through Epic's UserWeb web

portal if necessary to further implementation, integration, or testing of Epic's software at a customer facility. To gain access credentials to enter into Epic's UserWeb web portal, a person must contact and register with Epic, agree to strictly protect Epic's confidential information, and agree not to use the Epic information in a manner harmful to Epic. Those outside Epic are not able to access Epic's UserWeb to access or download data unless they have registered with Epic as a customer or a consultant who is supporting an Epic customer.

6. Despite Epic's precautions, and promises from TCS not to wrongfully disclose or misuse Epic's confidential information but only to use it for the purpose of supporting Epic's customer, TCS personnel wrongfully accessed Epic's UserWeb and downloaded a substantial amount of data containing Epic documents, confidential information, trade secrets, and other valuable assets owned by Epic. The vast majority of the stolen data was not required for TCS to provide consulting services to Epic's customer. To the contrary, much of the data wrongfully taken from Epic, if used improperly, would provide an unfair development and design advantage for TCS's competing medical management software called Med Mantra.

7. Rather than compete lawfully with Epic, TCS has engaged in an apparently elaborate campaign of deception to steal documents, confidential information, trade secrets, and other information and data from Epic, for the purpose of realizing technical expertise developed by Epic over years of hard work and investment. TCS's misconduct appears designed to allow TCS and perhaps other Tata entities to unfairly compete with Epic in the marketplace. The unlawful conduct of TCS and potentially other Tata entities must be stopped and an appropriate remedy fashioned for the benefit of Epic.

## **THE PARTIES**

8. Plaintiff Epic is a Wisconsin corporation with its principal place of business located at 1979 Milky Way in Verona, Wisconsin. Epic is a leading developer and distributor of software products for the healthcare industry. Epic markets and licenses software products for use in the healthcare industry throughout the United States and the world.

9. Defendant Tata Consultancy Services Limited (“TCS India”) is an Indian Corporation with its principal place of business located in Mumbai, India. The company specializes in information technology services, consulting, and business solutions, and does over half of its business in the Americas. TCS India also develops and markets software products, including the hospital management system Med Mantra, which is discussed in detail at the TCS website: [http://www.tcs.com/SiteCollectionDocuments/Brochures/Healthcare\\_Brochure\\_Med-Mantra-Healthcare-Solution\\_0612-1.pdf](http://www.tcs.com/SiteCollectionDocuments/Brochures/Healthcare_Brochure_Med-Mantra-Healthcare-Solution_0612-1.pdf). Med Mantra is being designed by TCS, and perhaps other Tata entities, to directly compete with Epic software products.

10. Defendant Tata America International Corporation (dba “TCS America”) is a New York corporation with its principal place of business located at 101 Park Avenue, Suite 2603, New York, New York 10178. TCS America appears to be a wholly-owned subsidiary of TCS India and is registered to do business in Wisconsin.

11. At all times mentioned herein, TCS India and TCS America were the agents of one another, acting in the full course and scope of said agency. In addition, on information and belief, at all times mentioned herein, TCS India and TCS America were the alter egos of one another. A unity of interest in ownership and other interests between TCS India and TCS America existed such that any separateness ceased to exist between them, and each was the mere instrumentality of the other. For example, TCS India and TCS America operate under the same

name (both regularly do business as “TCS”); use the same logo for their businesses; maintain interconnected websites that link to each other, with the TCS India website including a separate page for TCS America; and use the same email protocol. The companies appear to also use the same computer network and other shared services. Both TCS entities have the same principal executive office in the United States, have the same registered agents in the states in which they are both registered to do business, and have overlapping leadership. Furthermore, they offer the same services and products, with TCS America merely acting as the North America operation of TCS India.

### **JURISDICTION AND VENUE**

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1367(a) and 18 U.S.C. § 1030. This action involves the Defendants’ violations of the Computer Fraud and Abuse Act, and related misconduct.

13. This Court alternatively has jurisdiction pursuant to 28 U.S.C. § 1332(a). The dispute arises between citizens of different states and a citizen of a foreign state is an additional party—Epic is a citizen of Wisconsin, TCS America is a citizen of New York, and TCS India is a citizen of India—and the amount in controversy far exceeds the sum of \$75,000, exclusive of interests and costs.

14. TCS America and TCS India are subject to personal jurisdiction in Wisconsin. TCS America is registered in and authorized to conduct business in Wisconsin, and has a registered agent located in Madison, Wisconsin. TCS India and TCS America also directed their tortious and illegal conduct at Wisconsin, stealing documents and information from Wisconsin; wrongfully accessed servers physically located in Wisconsin; and knowingly caused related injuries to Epic in Wisconsin. The Defendants are engaged in substantial business activities

within Wisconsin. They are, and were at the time of the injury, engaged in solicitation and service activities in Wisconsin, and materials and things manufactured, serviced, and processed by the Defendants are used and consumed in Wisconsin. TCS America also entered into a Standard Consultant Agreement with Epic, under which TCS America consented to personal jurisdiction of the state and federal courts located in Wisconsin.

15. Venue is proper in the United States District Court for the Western District of Wisconsin pursuant to 28 U.S.C. §§ 1391 and 1400 because TCS America or its agent may be found in this judicial district, TCS India and TCS America are subject to personal jurisdiction in this judicial district, and a substantial portion of the events giving rise to this action occurred within this district. The servers wrongfully accessed and from which information and documents were stolen are physically present in this district. Furthermore, the intellectual property and confidential and proprietary information that is the subject of these allegations was created in and is situated in this judicial district.

### **FACTUAL BACKGROUND**

#### **Epic's Licensing Agreement With Kaiser**

16. Kaiser Foundation Hospitals ("Kaiser") is a substantial customer and user of Epic software. On February 4, 2003, Epic entered into a written agreement with Kaiser (the "Kaiser Agreement") under which Epic agreed to license certain computer software to Kaiser to support patient care delivery activities at all of Kaiser's venues.

17. Pursuant to the Kaiser Agreement, Epic has provided Kaiser with access to Epic's UserWeb, a protected electronic workspace through which Epic provides training and other user materials, such as program manuals, to assist customers with their implementation and maintenance of Epic products. The Kaiser Agreement also contains provisions protecting Epic's

confidential information by only allowing dissemination of information to persons with a need to know. It also contains restrictions on the use the Epic confidential information, limiting the uses to those needed to fulfill the purpose of the Kaiser Agreement.

18. Healthcare organizations regularly hire third party software analysts, software test engineers, and other technology consultants to support their computer networks and their employees' ability to use the networks. These consultants assist in the installation, configuration, operation, and support of Epic's electronic medical records systems at various Epic customers. In some cases these consultants are engaged to alter customer systems to improve system compatibility and train employees of Epic's customers.

19. Access to the Epic UserWeb is limited to those who require access to Epic information in order to facilitate installation, maintenance, or support of Epic software in use by a particular customer of Epic. Each user who attempts to access the Epic UserWeb must complete an online registration form. The registration includes a UserWeb log-in and password.

20. The UserWeb registration form requires each registrant to provide his or her employer information, including whether the registrant is an "employee of an Epic customer," or a "consultant" for an Epic customer. Employees of Epic customers are granted access to the Epic UserWeb without additional restrictions because the customer has already contractually promised not to wrongfully use or disclose Epic documents or information (ordinarily in a detailed written agreement governing the entire relationship between Epic, its products, and the customer).

21. Consultants who have been hired by customers, on the other hand, are required to complete a UserWeb Access Agreement before their account can be considered for approval and authorization for access granted by Epic. The agreement is designed to provide a layer of

protection for Epic before the consultants, some of whom work for companies that compete with Epic, may access Epic's UserWeb. In addition, under the UserWeb Access Agreement, consultants are not eligible to obtain access to the UserWeb until their consulting firm has entered a Consultant Access Agreement with Epic for the applicable customer. The specifics of the Consultant Access Agreement are designed to limit the Consultant's use of information and protect Epic from any improper use or disclosure of its software, documents, confidential information, intellectual property, or the other valuable information on the Epic UserWeb.

22. Even if a consultant is granted access to the UserWeb, that access is more limited than the access enjoyed by Epic's customers. Epic purposefully circumscribes consultants' access to a limited area that is necessary for the consultant to support Epic's customer. The UserWeb Access Agreement obligates the "User" who agrees to the agreement to accept access to UserWeb only for purposes of performing the specific services for or on behalf of the Epic customer. Each consultant User agrees that he or she will not share the login password with any other person, or grant access for any other person to login to UserWeb. The User further agrees that he or she will not use the Epic confidential information for any other purpose other than performance of the Customer project that the consultant is supporting.

23. Epic requires the UserWeb Access Agreement and agreements with consulting firms to protect its documents, confidential information, trade secrets, and other intellectual property and information, and to take reasonable steps to prevent unauthorized disclosure or use of the intellectual property assets of Epic. Consultants are not authorized to access the Epic UserWeb without agreeing to the UserWeb Access Agreement. Their authorization is expressly limited by the terms of that agreement.



### **Epic's Standard Consultant Agreement with TCS**

24. TCS is not an Epic customer. It provides consulting services to Epic's customers. It is also a competitor of Epic in that it is offering competing software systems and services.

25. In August 2005, in connection with Epic's ongoing provision of computer software services to Kaiser, several individuals claiming to be Kaiser employees registered with Epic to receive certain software training classes. When Epic personnel realized that the registering individuals' email addresses were from TCS, not Kaiser, they immediately contacted Kaiser regarding the discrepancy. Kaiser responded that the individuals were in fact TCS employees consulting for Kaiser, apparently working with Kaiser in support of its complex computer networks and software systems. Epic physically removed the TCS employees from the Epic training course and informed them that they could not take the course until Epic received an executed non-disclosure agreement from TCS.

26. Shortly thereafter, on August 10, 2005, Epic and TCS America entered a Standard Consultant Agreement (the "TCS America Agreement") whereby Epic agreed to allow certain TCS employees access to Epic training programs for purposes of providing consulting services to Epic's customers related to the implementation of "Epic Program Property."

27. The TCS America Agreement defines Epic Program Property to be the "computer program object and source code and the Documentation for all of Epic's computer programs." In the TCS America Agreement, TCS agreed that Epic's Program Property "contains trade secrets of Epic protected by operation of law and this Agreement."

28. The TCS America Agreement included confidentiality provisions and use restrictions whereby TCS agreed that it, its employees, and its agents would do the following, among other things, to protect Epic's rights:

- a. TCS will “limit access to the Program Property to those [TCS employees] who must have access to the Program Property in order to implement the Program Property on Epic’s or its customer’s behalf” (i.e., Kaiser);
- b. TCS will not “use the Program Property ... for any other purpose other than in-house training of [TCS] employees to assist Epic customers in the implementation of the Program Property licensed by that Epic customer”;
- c. TCS will “require any [TCS] employees who are given access to the Confidential information to execute a written agreement ... requiring non-disclosure of the Confidential Information and limiting the use of the Confidential Information to uses within the scope of the employee’s duties conduct pursuant to this Agreement” or “inform all such employees that [TCS is] obligated to keep Confidential Information confidential...”;
- d. TCS will “use Confidential Information only for the purpose of implementing the Program Property on an Epic customer’s behalf”;
- e. TCS will “notify Epic promptly and fully in writing of any person, corporation or other entity that You know has copied or obtained possession of or access to any of the Program Property without authorization from Epic”; and
- f. TCS will not permit any employee who has had access to the Program Property to participate in any “development, enhancement or design of, or to consult, directly or indirectly, with any person concerning any development, enhancement or design of, any software that competes with or is being developed to compete with Epic Program Property....”

29. The TCS America Agreement remains in effect today. It is understood by all parties that the agreement covers the work of TCS consultants at Kaiser.

30. On information and belief, since 2005 the Defendants have continued to provide consulting services to Kaiser related to the implementation and maintenance of Epic Program Property.

31. TCS India and/or TCS America are currently performing a Testing Center of Excellence contract with Kaiser, under which TCS personnel develop and implement processes, tools, and best practices for testing and improving certain Epic Program Property licensed to Kaiser under the Kaiser Agreement.

**TCS's Unauthorized Access, Fraud, and Theft of Epic Information**

32. Epic recently learned from an informant that TCS personnel have been fraudulently accessing Epic's UserWeb computer network, and that the information obtained through the unauthorized access into UserWeb was being used to benefit TCS's competing Med Mantra software.

33. According to the informant, TCS leaders in the U.S. and India appear to be aware of and complicit in TCS's scheme to gain unauthorized access to Epic's UserWeb and information and misuse them for the benefit of TCS. The unauthorized access by TCS began as early as 2012.

34. The informant further described that an access credential for the UserWeb has been used in India to access Epic's UserWeb without authorization to download information from Epic's UserWeb, and that the purpose of the misconduct was to use information and documents related to Epic's leading software to benefit TCS's creation of and improvements to TCS's competing Med Mantra product.

35. After learning of the unauthorized and illegal downloading of Epic information by TCS personnel, and the apparent purpose of the misconduct, Epic evaluated its protected UserWeb and discovered that an account associated with a TCS employee who worked as a consultant for Kaiser in Portland, Oregon, and who worked on projects related to Epic's provision of software and services to Kaiser, had downloaded from Epic's UserWeb at least **6,477 documents** accounting for **1,687 unique files**.

36. The access credentials of this individual were used to access the Epic UserWeb from an IP address in India during the time when the employee resided in Oregon. The access credentials were also utilized from other IP addresses around the United States, outside of Oregon.

37. Epic is still investigating the specific stolen documents, but the documents downloaded by TCS personnel included, among other things, documents detailing over twenty years of development of Epic's proprietary software and database systems, including programming rules and processes developed to produce optimal functionality of Epic's software; documents that decode the operation of its source code that would otherwise be unusable to those outside of Epic; and information regarding Epic's system capabilities and functions, including procedures for transferring data between customer environments, rules related to information collection, methods for limiting access to patient records, and processes for converting customer data, all of which reveal decades of work with its customers to determine the functionality desirable or required for Epic to provide successful products to those customers. The majority of these downloaded Epic documents were not required for TCS employees to perform job functions in support of Kaiser.

38. In addition to the enormous number of downloads accomplished through the misuse of a TCS employee's credentials, it was discovered that the credentials had been obtained in a fraudulent manner. When the employee who had been assigned the abused credentials registered for his credentials, he represented that he was a "customer employee" instead of a "consultant." He also used his kp.org email address, which Kaiser provides to its consultants for use while consulting for Kaiser, to mislead Epic into believing that he was an employee of Kaiser rather than an employee of TCS. The TCS employee appears to have intentionally misrepresented himself as a Kaiser employee when he knew that was a false representation for the purpose of gaining customer-level access authorization to Epic's UserWeb.

39. Upon discovery of the fraudulent access to and excessive downloading from the Epic UserWeb by the TCS employee, Epic suspended the TCS employee's User ID so no further access or downloading could occur.

40. Shortly thereafter, the TCS employee sought via email to have his access to the UserWeb reactivated. He sent two emails on June 24, 2014, and June 30, 2014, seeking reactivation of his account. The first email on June 24 included a signature line indicating that his title was "QA Lead, Kaiser Permanente." The second email on June 30 included a different signature line indicating that the TCS employee was actually an "Onshore Test Lead" for TATA Consultancy Service as well a "QA Lead" title for Kaiser. On information and belief, the first email deleted the identification of TATA Consultancy Service so as to mask the fact that the TCS employee was not with Kaiser but rather TCS. The TCS employee also appears to have understood that the access he sought exceeded access that would be granted to a consultant.

41. There appears to be no legitimate reason for the TCS employee who downloaded more than six thousand files from Epic to download so many files, or to download some of the

specific pieces of data he targeted on the Epic system. Much of the information taken would not be needed by the TCS employee for him to perform his limited job function supporting Kaiser.

#### **A TCS Employee Admits To Wrongdoing**

42. When confronted by Kaiser regarding this downloading of Epic data, the TCS employee identified above initially denied the downloading. He claimed that he only viewed Epic information on UserWeb, but did not save or download any Epic materials. After being presented with the download logs associated with his account, however, the TCS employee changed his story and admitted that he had provided his Epic access credentials to two other TCS personnel, in violation of the UserWeb Access Agreement. He also admitted that these other TCS personnel did not need access to the Epic UserWeb to perform job functions in support of Kaiser.

#### **Epic Uncovers More Misconduct By TCS Personnel**

43. On July 29, 2014, Epic suspended the UserWeb access credentials for another TCS consultant working with Kaiser after it was determined that this additional TCS employee had also downloaded Epic documents which have no apparent relationship to his position as a consultant supporting Kaiser.

44. Epic is still investigating the misconduct of TCS personnel and does not yet know the extent of the damage caused by TCS's misconduct. Epic will continue to incur costs and damages as it seeks to uncover how much of its intellectual property, trade secrets, confidential information, internal documents, and other information and data was taken by TCS personnel.

45. The sensitive materials taken by TCS personnel cannot be disclosed in this publicly filed document but will be identified for the Court and the parties in this case, after an

appropriate protective order is entered to protect Epic's valuable information and intellectual property and TCS discloses for the Court and parties the extent of its misconduct.

46. Unless restrained by this Court, TCS's unauthorized access to Epic's intellectual property, trade secrets, confidential information, internal documents, and other information and data, and subsequent theft of Epic's intellectual property, trade secrets, confidential information, internal documents, and other information and data by downloading from the UserWeb, will allow TCS to shortcut years of hard work and investment expended by Epic in developing Epic's industry-leading medical software products.

47. TCS' actions set forth above were malicious and taken with an intentional disregard of the rights of Epic.

### **FIRST CAUSE OF ACTION**

Computer Fraud and Abuse Act under 18 U.S.C. § 1030

(against All Defendants)

48. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 47 above.

49. Epic's computer system is a protected computer as that term is defined by the Computer Fraud & Abuse Act. Defendants accessed Epic's UserWeb, without authorization and by exceeding their authorization, to obtain confidential business information and/or trade secrets belonging to Epic, and to engage in and advance a fraud and theft, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The conduct of TCS described above was knowing and intentional.

50. The actions of Defendants were without Epic's knowledge, permission, or authorization.

51. The actions of the defendants crossed state lines, including conduct from Oregon, Wisconsin, and other states, and involved interstate commerce.

52. As a result of the violation by Defendants of the Computer Fraud and Abuse Act, Epic has suffered damage and loss far in excess of \$5,000, and Epic will continue to be injured irreparably, while Defendants will be unjustly enriched. Epic's damages include, among other things, costs related to identifying TCS's access of Epic's UserWeb and efforts to remedy the breach and prevent further misconduct. The specific amounts of damages suffered by Epic will be set forth at the trial of this matter.

### **SECOND CAUSE OF ACTION**

Computer Crimes Act under Wis. Stat. § 943.70

(against All Defendants)

53. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 52 above.

54. Defendants willfully, knowingly, and without authorization accessed, copied, and took possession of electronic data and information belonging to Epic from Epic's UserWeb, without Epic's consent and without lawful authority.

55. The conduct of Defendants interfered with the right of Epic to possess such property and directly and proximately caused injury to Epic.

56. The actions of Defendants constitute a violation of Wis. Stat. § 943.70.

57. As a direct and proximate result of the violation by Defendants of Wis. Stat. § 943.70, Epic has suffered damages and loss in a manner which will be set forth at the trial of this matter.



### **THIRD CAUSE OF ACTION**

Misappropriation of Trade Secrets under Wis. Stat. § 134.90

(against All Defendants)

58. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 57 above.

59. Certain files that Defendants downloaded without authorization from Epic's UserWeb contain "trade secrets" within the meaning of Wis. Stat. § 134.90(1)(c) and C.R.S. § 7-74-102(2). Specifically, the files contain data from which Epic derives economic value because it is not generally known and not readily ascertainable by proper means to Epic's competitors, and Epic takes significant steps to maintain the secrecy of the information, including by restricting access to Epic customers and requiring others to sign non-disclosure agreements and other use restriction agreements. Epic also uses physical and technological restrictions to protect its valuable trade secret information, as described partially in this Complaint.

60. Upon information and belief, Defendants misappropriated the files for the purpose of utilizing Epic's trade secrets, which the company has developed through decades of work and significant expense, for purposes of developing TCS's formerly elementary Med Mantra software in order to compete directly with Epic.

61. Pursuant to Wis. Stat. § 134.90(3), Epic is entitled to an injunction to prevent the misappropriation and misuse of its trade secrets.

62. While some of the injury being caused by Defendants' actions is irreparable pursuant to Wis. Stat. § 134.90(3), Epic has suffered also damages as a result of Defendants' misappropriation of Epic's trade secrets and it is entitled to recover such damages and/or disgorgement of any profits received by Defendants from their misappropriation of Epic's trade

secrets pursuant to Wis. Stat. § 134.90(4). An award of exemplary and punitive damages is also appropriate in light of the misconduct of TCS outlined herein.

#### **FOURTH CAUSE OF ACTION**

##### Breach of Contract

(against All Defendants)

63. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 62 above.

64. The TCS America Agreement is a valid agreement under which TCS America, acting as the agent and alter ego of TCS India, made certain promises that while consulting for Kaiser to protect Epic's confidential and proprietary information, including by restricting access to the information, limiting its use to training and other consulting activities for Epic customers, and preventing use to design, develop, or enhance a competing software product.

65. Epic has done all of the things required of Epic under the TCS America Agreement.

66. All conditions required under the TCS America Agreement for Defendants' performance were excused or have occurred, as detailed herein.

67. Defendants have breached the Agreement and failed to protect Epic's confidential and proprietary information by, among other things, improperly utilizing UserWeb access credentials by non-registered employees and employees who do not require access to consult for an Epic customer; downloading documents and information not required for any consulting activity for an Epic customer and sending that information to India; and using Epic confidential and proprietary information to develop and enhance software that competes with Epic.

68. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants’ willful and material breaches and willful misconduct in an amount to be proven at trial. All of these damages were foreseeable as the consequences of Defendants’ breaches as alleged herein. The amount of damages will be set forth in detail at the trial of this matter, after the extent of TCS’s misconduct is discovered through this case.

69. If Defendants are allowed to continue breaching the TCS America Agreement as described above, Epic will suffer irreparable harm for which it has no adequate legal remedy.

### **FIFTH CAUSE OF ACTION**

#### Breach of the Covenant of Good Faith and Fair Dealing

(against All Defendants)

70. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 69 above.

71. The TCS America Agreement is a valid agreement under which TCS America, acting as the agent and alter ego of TCS India, made certain promises to protect Epic’s confidential and proprietary information, including by restricting access to the information and limiting its use to training and other non-competitive activities.

72. Defendants owed Epic a duty of good faith and fair dealing implied from the TCS America Agreement. The TCS America Agreement contained an implied covenant of good faith and fair dealing that, among other things, prohibited Defendants from engaging in the misappropriation and misuse described above.

73. Epic has done all of the things required of Epic under the TCS America Agreement.

74. Through the intentional and deceitful conduct alleged above, Defendants breached the covenant of good faith and fair dealing implied in the TCS America Agreement and denied Epic benefits due to Epic under the agreement. Defendants' conduct violated the spirit of the TCS America Agreement, and deprived Epic of the fruits of that contract.

75. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants' willful and material breaches of the implied covenants of good faith and fair dealing, and willful misconduct, in an amount to be proven at trial. All of these damages were foreseeable as the consequences of Defendants' breaches as alleged herein.

76. If Defendants are allowed to continue breaching the covenant of good faith and fair dealing implied in the TCS America Agreement as described above, Epic will suffer irreparable harm for which it has no adequate legal remedy.

### **SIXTH CAUSE OF ACTION**

Fraud

(against All Defendants)

77. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 76 above.

78. When TCS employees registered for limited access to Epic's system, at least one of them falsely claimed to be a Kaiser employee for the purpose of gaining access.

79. Defendants' representation was false, and Defendants knew the representation was false when they made it. It was made intentionally to advance Defendants' apparent scheme to steal confidential information, documents, intellectual property, and other information from Epic.

80. Defendants intended that Epic rely on the representation, and Epic did in fact rely on the representation in granting TCS access to the UserWeb.

81. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants’ intentional misrepresentation. The amount of Epic’s damages will be proven at trial.

82. Defendants’ misconduct as described herein was intentional, malicious and specifically directed at causing harm to Epic, entitling Epic to an award of exemplary and punitive damages.

### **SEVENTH CAUSE OF ACTION**

#### Misrepresentation

(against All Defendants)

83. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 82 above.

84. Defendants represented to Epic on the UserWeb registration form that at least one of their employees was a Kaiser employee.

85. Defendants’ representation was false, and Defendants had no reasonable grounds for believing the representation was true when they made it to Epic.

86. Defendants intended that Epic rely on the representation, and Epic did in fact rely on the representation in granting access to the UserWeb.

87. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants’ intentional misrepresentation. The amount of these damages will be set forth at the trial of this matter.

## **EIGHTH CAUSE OF ACTION**

### Conversion

(against All Defendants)

88. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 87 above.

89. This cause of action does not depend on information that meets the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

90. Epic was the owner of information and documents stored on its UserWeb, which was wrongfully accessed by TCS personnel.

91. Defendants willfully took, controlled, interfered with, and/or deprived Epic of documents and information without Epic's consent and without lawful authority (including information and documents that do not comprise trade secrets). The specific identification of the information wrongfully converted by TCS will be uncovered through the discovery process and as Epic continues its own evaluation of the data stolen from its UserWeb.

92. As a result of the conversion by Defendants of Epic's property, Epic has been and will continue to be injured irreparably and otherwise, while Defendants will be unjustly enriched. Moreover, Defendants' actions with respect to Epic's property have seriously interfered with Epic's right to possess the property, damaging Epic in an amount that will be evidenced at the trial of this matter.

93. Defendants' misconduct as described herein was intentional, malicious and specifically directed at causing harm to Epic, entitling Epic to an award of exemplary and punitive damages.

## **NINTH CAUSE OF ACTION**

### Common Law Unfair Competition

(against All Defendants)

94. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 93 above.

95. This cause of action does not depend on information that meets the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

96. Epic has invested substantial time, labor, and money in the creation and development of its data systems, software, documents, and information.

97. Without Epic's authorization, Defendants intentionally and wrongfully used, and will continue to use, Epic's stolen documents, password credentials, and information in unfair competition with Epic. This use is in direct competition with the services offered by Epic.

98. Defendants have gained an unfair advantage in their competition with Epic because Epic, not Defendants, expended the time, money and energy to create and develop the documents and information stolen from Epic, as detailed above.

99. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants' misconduct described above. The amount of those damages will be set forth at the trial of this matter.

100. Defendants' misconduct as described herein was intentional, malicious and specifically directed at causing harm to Epic, entitling Epic to an award of punitive damages.

## **TENTH CAUSE OF ACTION**

Injury to Business under Wis. Stat. § 134.01

(against All Defendants)

101. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 100 above.

102. This cause of action does not depend on information that meets the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

103. Defendants conspired and acted in concert together to misappropriate and misuse Epic's confidential and proprietary information for the purpose of willfully or maliciously injuring Epic's business via competitive harm to Epic's competing software product, including EpicCare Inpatient and EpicCare Ambulatory.

104. The actions of Defendants constitute a violation of Wis. Stat. § 134.01.

105. As a direct and proximate result of the violation by Defendants of Wis. Stat. § 134.01, Epic has suffered damages and loss in an amount which will be proven at the trial of this matter.

### **ELEVENTH CAUSE OF ACTION**

Wis. Stat. § 895.446

(against All Defendants)

106. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 105 above.

107. This cause of action does not depend on information that meets the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.



108. Without Epic's consent, Defendants intentionally took and all Defendants have used property belonging to Epic, including Epic documents and other property found on Epic's UserWeb, with the intent to deprive Epic permanently of the possession, use, and/or value of such property in violation of Wis. Stat. § 943.20.

109. As a direct and proximate result of Defendants' wrongful actions, Epic has suffered damage and loss. Pursuant to Wis. Stat. § 895.446, Epic is entitled to actual damages, including all costs of investigation and litigation. The amount of these damages will be evidenced at the trial of this matter.

### **TWELFTH CAUSE OF ACTION**

#### Unjust Enrichment

(against All Defendants)

110. Epic pleads this Cause of Action in the alternative to the Fourth Cause of Action for breach of contract.

111. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 109 above.

112. This cause of action does not depend on information that meets the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

113. Epic was, and is, entitled to the benefit of the data, documents, and information that was stored on its UserWeb.

114. With full knowledge of Epic's rights, Defendants unjustly obtained the benefit of Epic's property, as described herein, resulting in inequity and damage to Epic, as described in more detail above.

115. At all relevant times, Defendants appreciated or had full knowledge of the benefit of the data and information, and other things, which they stole from Epic.

116. Defendants have unjustly and wrongfully benefited, and continue to benefit, from their misappropriation and use of the property of Epic, to the detriment of Epic and against the fundamental principles of justice, equity, and good conscience. Under the circumstances described above, it is inequitable for Defendants to accept or retain the benefit of Epic's confidential and proprietary information.

117. Defendants were unjustly enriched and Epic was damaged in an amount to be proven at trial.

#### **PRAYER FOR RELIEF**

WHEREFORE, Epic prays for relief and judgment as follows:

- a. An order from the Court granting the parties immediate and expedited discovery in the matter;
- b. Preliminary and permanent injunctive relief appropriately fashioned by the District Court to prevent further injury to Epic, and to prevent Defendants from further benefiting from their misconduct as alleged herein, including but not limited to injunctive relief:
  - i. requiring Defendants to cease all use of any document, information, or trade secret, taken from Epic in violation of law;
  - ii. requiring Defendants to not disclose to any party any document, information, or trade secret, taken from Epic in violation of law;
  - iii. requiring Defendants to immediately destroy and/or permanently delete (1) all copies of Epic documents and information in any form (electronic

- or hardcopy) including without limitation any trade secret and confidential information acquired from Epic; and (2) all copies of any materials in any form containing any, or derived from any, Epic trade secret or confidential information;
- iv. requiring Defendants to provide a detailed accounting of its search for and destruction of the documents and information described in (iii) above, including providing a list of all documents or information destroyed or deleted.
  - v. preventing Defendants from any further unauthorized access, or access exceeding authorization, of any computer network or system of Epic, including, without limitation, the UserWeb;
  - vi. preventing Defendants from further improper use or disclosure of Epic's trade secrets or confidential information; and
  - vii. preventing Defendants from selling or offering to sell products that utilize, embody, or were developed or enhanced using Epic's trade secrets and/or confidential information;
- c. An award of the actual and consequential damages and loss that Epic has sustained as a result of Defendants' wrongdoing;
  - d. Disgorgement of Defendants' profits arising from the benefits of Defendant's use of Epic's confidential and proprietary information;
  - e. An award of all costs of investigation and litigation related to Epic's theft and misappropriation of Epic trade secrets and/or confidential information;

- f. An award of punitive damages against Defendants in an amount to be determined at trial;
- g. An award of pre- and post-judgment interest to the extent allowed by law; and
- h. An award of such other, further, and different relief as may be just and proper in light of the circumstances of this case.

**DEMAND FOR JURY TRIAL**

Epic respectfully demands a trial by jury on all claims and causes of action properly tried thereto.

Dated: October 31, 2014

/s/ Anthony A. Tomaselli

Brent Caslin  
bcaslin@jenner.com  
Nick G. Saros  
nsaros@jenner.com  
Kate T. Spelman  
kspelman@jenner.com  
JENNER & BLOCK LLP  
633 West 5th Street Suite 2600  
Los Angeles, CA 90066  
Tel: 213-239-5100  
Fax: 213-230-5199

Anthony A. Tomaselli  
aat@quarles.com  
Kristin Graham Noel  
kristin.noel@quarles.com  
Stacy A. Alexejun  
stacy.alexejun@quarles.com  
QUARLES & BRADY LLP  
33 East Main Street, Suite 900  
Madison, WI 53703  
Tel.: 608.251.5000  
Fax: 608.251.9166

*Attorneys for Plaintiff Epic Systems Corporation*