

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

FEB -3 2010

United States of America

v.

Case No.

5:10mj65

SHALIN JHAVERI

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Jan. 2010 through Feb. 2, 2010 in the county of Onondaga in the Northern District of New York, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 1832

Theft of Trade Secrets

This criminal complaint is based on these facts:

See Affidavit of Special Agent Timothy M. Dwyer, attached hereto and incorporated by reference as if fully set forth herein.

x Continued on the attached sheet.

Timothy M. Dwyer
Complainant's signature

Timothy M. Dwyer, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: Feb 3, 2010

George H. Lowe
Judge's signature

City and state: Syracuse, New York

George H. Lowe, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT OF SPECIAL AGENT TIMOTHY M. DWYER

I, Timothy M. Dwyer, having been first duly sworn, do hereby depose and state as follows:

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since November 21, 1994 and have been assigned to the FBI's Albany Division, Syracuse Resident Agency (SYRA), Syracuse, New York, since March, 1995. Since my assignment to the SYRA, I have been assigned to investigate white collar crime matters, including bank fraud, mail fraud, wire fraud, and health care fraud; violent crime matters, including child pornography and international parental kidnapping; drug matters; civil rights matters; and national security matters, including domestic and international terrorism. Currently, I am assigned the responsibility to investigate counterintelligence matters. I have been in my current assignment since January, 2003. During the course of my duties I have been involved in several search warrants which have included the search of computers and associated media storage.

2. I make this affidavit in support of the annexed criminal Complaint.

3. The statements contained in this affidavit are based upon my investigation, information provided by other FBI personnel, information and reports provided by individuals employed by Bristol-Myers Squibb Company (BMS), SHALIN JHAVERI's ("JHAVERI") employer, other individuals specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a Special Agent of the FBI. As this affidavit is being submitted for the limited purpose of supporting the annexed criminal Complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe

that JHAVERI has engaged in conduct constituting a violation of Title 18, United States Code, Section 1832.

4. On January 25, 2010, in Syracuse, New York, JHAVERI spoke on the telephone at approximately 7:00 p.m. with an individual who he believed to be interested in helping finance a pharmaceutical facility JHAVERI planned to start in India, and who JHAVERI knew was not affiliated or employed by BMS in any capacity. This conversation was lawfully recorded. During the conversation, JHAVERI told the individual that he (JHAVERI) had created a new Gmail account, that the email address for this account was [REDACTED].com, and that the password for this new account was "[REDACTED]". JHAVERI told the individual that there is an email in the account with no words in the subject line and attached to the email are three documents. The individual asked JHAVERI if the attached documents were the ones that JHAVERI previously had described to him and JHAVERI responded that they were. The individual then asked JHAVERI if he had all the "rest of the stuff" also previously described by JHAVERI and JHAVERI responded, "yes, I got it", and that he (JHAVERI) had almost 4 GBs worth of documents. The individual asked JHAVERI if that was everything he needed and JHAVERI told him it was, and that it included all the Standard Operating Procedures ("SOP"s), but that he would check the next day to see if there were any more documents that JHAVERI thought "are required". The individual then asked JHAVERI if JHAVERI would send him a list of the names of the documents he had. JHAVERI said that he had already had an Excel file that listed the names all the BMS documents he had gathered and that JHAVERI would put the list in the newly created email account "tomorrow" [on January 26, 2010].

5. After being told this by JHAVERI on January 25, 2010, the individual then accessed the newly created Gmail account. Upon opening the account, he found an email with three

attachments. The attachments were each identified as "BMS Confidential and Proprietary." The three documents were identified as , "APPP-121, version 00"; "SQA-003, Version 02"; and "LAB-048, Version 01".

6. On January 26, 2010, the individual once again queried, as he had been told to do by JHAVERI, JHAVERI's newly created Gmail account. Attached to an email in this account, as promised the previous day by JHAVERI, was an Excel spreadsheet capturing all the BMS SOPs JHAVERI had told the individual he had taken from the company. This spreadsheet listed the titles of 1,327 BMS SOPs.

7. Through my investigation I have learned that JHAVERI was employed at BMS as a Technical Operations Associate. I have also communicated with Michael Hausladen, Associate Director of Manufacturing Support and Pilot Plant, BMS, and JHAVERI's immediate supervisor at BMS. Mr. Hausladen has advised me that JHAVERI was employed at BMS in a management training program at BMS, which had called for him to be rotated through various segments and departments within BMS and thus had given him access to some of the most sensitive areas within the company.

8. On January 27, 2010, after having reviewed the three documents JHAVERI had stolen from BMS and attached to an email in the Gmail account he had created for this purpose (and that he had told the individual to check for proof of his having taken proprietary and confidential BMS documents to be used to launch his planned pharmaceutical company in India), Mr. Hausladen prepared a final report describing the significance of each of the three attachments provided to the individual by JHAVERI. In his report, Mr. Hausladen generally described the significance of each attachment as follows:

a. Document 1: "APPP-121, version 00". This document is a Standard Operating Procedure (SOP) that provides instructions for manufacturing staff to complete one of the manufacturing steps for our drugs. The manufacturing step instructions described in this SOP are for the "Viral Filtration Step" - which utilizes a Planova brand nanometer filter. The instructions in this SOP are for a specific clinical drug substance, Anti-Human CD137 Monoclonal Antibody, identified in the SOP as BMS-663513. These instructions will be similar for other commercial and clinical drugs manufactured in the East Syracuse BMS site.

The manufacturing processes for Biologic compounds are highly confidential, as the "process is the product" for biologic drug products. While certain aspects of utilizing a Planova brand viral filter are available from the manufacturer, the actual implementation is BMS confidential information.

b. Document 2: "SQA-003, Version 02."

This SOP provides instructions for the East Syracuse BMS site for handling an inspection from a regulatory agency, such as the FDA. This SOP provides specific instructions for handling different requests from the inspecting agencies, describes how the inspection team is to be configured, lists roles and responsibilities for the inspection team, lists the key documents that should be available to the inspector as well as the documents that will not be provided to the inspector. It also provides directions for how verbal and written communications with the inspector, the regulatory agency and within BMS are to be handled.

c. Document 3: "LAB-048, Version 01."

This SOP provides instructions to personnel, working in the laboratory where testing of products and manufacturing samples are analyzed, for how to manage a result that fails a specification. An example would be an impurity in process sample that exceeds the allowable limit. When this occurs, a "Laboratory Investigation" (LI) is initiated. The main purpose of a LI is to understand if an error occurred in the laboratory or if there truly is something wrong with the sample. There is an extensive series of investigative questions that are addressed in a logical manner (captured in the flowchart in Appendix B, page 26 of the SOP) to identify the root cause of the laboratory out of tolerance/specification result.

9. Mr. Hausladen also shared with me his opinion about JHAVERI's possession of these documents from his view as his manager. Mr. Hausladen told me that there is no conceivable or legitimate purpose for viewing, copying or sending these SOP documents to anyone outside of the BMS organization within the current work scope assigned to JHAVERI. According to Mr. Hausladen, the copying and sending of these types of documents to anyone outside of BMS is clearly a violation of company policy.

JHAVERI's activity in acquiring and disclosing to an individual outside BMS these three attachments, consisting of proprietary and confidential BMS documents, also appears to me to be in direct violation of a BMS "Employee Confidential Information Agreement", which JHAVERI signed on November 19, 2007.

10. I also asked Mr. Hausladen to share with me the steps that BMS employs to prevent documents like these from being removed from the company or shared with BMS'

competitors, or other outsiders. According to Mr. Hausladen, there are a number of controls that are in place to prevent such from happening. Some of the steps are listed below.

a. The SOPs are stored electronically, with each SOP an individual file. These files are not accessible from outside of BMS.

b. The SOPs for the BMS East Syracuse site are currently located on network drives that are accessible only if one is logged into a BMS computer that is connected to the BMS intranet and logged into the BMS East Syracuse server.

c. East Syracuse BMS employees have access to these SOP files. BMS employees are expected to follow the SOPs that apply to them and the work they do.

d. BMS employees outside of the East Syracuse site cannot access these SOP files.

e. All SOPs that are stored electronically are clearly marked within the files that the SOPs are "BMS Confidential and Proprietary."

f. BMS employees are trained on the appropriate handling of confidential and proprietary information and sign employee confidentiality agreements as a condition of their employment.

11. On January 29, 2010, Mr. Hausladen told me that at a minimum, the value of each individual SOP that JHAVERI has told the individual he has obtained from BMS is significant. This minimum value represents only the time and effort it would take to

prepare each of these documents and did not include each SOPs market value. Given Mr. Hausladen's initial analysis, and that JHAVERI has told the individual that he has obtained 1,327 of these SOPs from BMS, I have concluded that JHAVERI has taken confidential and proprietary documents from BMS that have substantial value.

12. On January 29, 2010, and February 1, 2010, Sheri Cipriano, Principal Analyst, Forensic Security Investigations, Information Security Department, BMS, told me that she and her colleague, Sean Conover, Principal Analyst, Forensic Security Investigations, Information Security Department, BMS, were notified by BMS Corporate Security on December 22, 2009 that JHAVERI was misappropriating BMS confidential and proprietary information. In response, Ms. Cipriano and Mr. Conover made an image of JHAVERI's BMS work laptop using computer forensic software. I have been informed that all BMS company computers display a banner each Wednesday morning when employees log on to their BMS computers setting forth BMS company policy that:

Information is a key competitive asset for our organization. Ensuring the privacy of our confidential proprietary information is extremely important to securing our success. Employees must not disclose such information to those who do not have a legitimate business need to know. This includes, but is not limited to postings in internet message boards and chat rooms. Employees who violate this standard are subject to not only disciplinary action, including termination, for violating company policies, but also criminal and civil prosecution for violating federal securities laws and civil liability for violating applicable confidentiality agreements.

The E-mail, Internet and Computer-based Information Policy clearly informs employees that the company monitors computer use by employees, including Internet use and, in certain cases, e-mail use. Monitoring is conducted in order to manage the company's computer network, assurance of system security, and verification that employees are in compliance with company policy, among other reasons. No system user can have any expectation of privacy as to the contents of any e-mail communications, the nature of the system user's Internet usage or any

other use by any individual of company systems. Violation of company policy regarding the use of computer resources may result in restriction or termination of access to the company's computing resources and other disciplinary action, up to and including termination of employment.

13. On December 29, 2009, Mr. Conover reviewed an image of JHAVERI's BMS work laptop and discovered information that JHAVERI had planned and was taking steps to start a bio-pharmaceutical company named Cherish Bio Sciences in India with his father. Some of the documents observed by Mr. Conover included an application to the government of India to start the company, a Biologics Contract Manufacturing Survey, a company profile, and an Internet domain registration for [REDACTED].

14. On January 11, 2010, Ms. Cipriano connected to JHAVERI's work station using computer forensic software and determined that JHAVERI had attached an external drive of at least 600 GB to his business laptop. Ms. Cipriano also determined that JHAVERI had downloaded at least 45 GBs of information to the 600+ GB external drive.

15. On January 15, 2010, Ms. Cipriano, utilizing additional computer forensic software that includes key stroke monitoring, determined that JHAVERI had received an e-mail from an individual in India on his Gmail account with an attachment concerning a business plan model that appeared to her to be for cell culture products.

16. On January 26, 2010, Ms. Cipriano determined that on the evening of January 25, 2010, between 6:00 p.m. and 7:45 p.m., JHAVERI made additional downloads to unauthorized external drives from his BMS business laptop. It appeared to Ms. Cipriano

that JHAVERI was copying documents from a BMS file server to the "My Documents" folder on his business laptop, and then from there to the unauthorized external drives. After he had copied the documents to these unauthorized external drives, JHAVERI deleted his "My Documents" folder and emptied the recycling bin on his BMS laptop computer that he had just finished using to transfer the BMS data to these unauthorized removable hard drives.

17. On January 27, 2010, Ms. Cipriano observed, again using computer forensic software, JHAVERI downloading BMS SOPs to unauthorized external hard drives between 6:00 p.m. and 10:00 p.m.

18. On February 1, 2010, Ms. Cipriano further advised me that, based on her further use of computer forensic software, she has determined that there is no evidence of JHAVERI using his BMS laptop computer to create the [REDACTED].com Gmail account, nor of JHAVERI attaching the three BMS SOPs (that he provided to the UCE) to an email in that account, thus confirming that he had access to and apparently used another computer under his control outside of the BMS computer network.

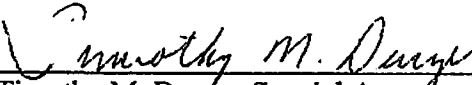
19. On February 2, 2010, the individual traveled to Syracuse and met JHAVERI at the Renaissance Hotel, as they previously had discussed and agreed. The individual and JHAVERI met at the hotel at approximately 6:15 p.m. The individual had told JHAVERI that he (the individual) had discussed this investment opportunity with his (the individual's) father and that his father wanted him to meet with JHAVERI to review additional items JHAVERI had already obtained from BMS.

20. On the evening of February 2, 2010, I observed JHAVERI meeting with the individual in a room at the Renaissance Hotel in Syracuse. During that meeting, JHAVERI showed the individual, using JHAVERI's personal laptop computer, BMS confidential and proprietary files that he had taken from BMS without authorization and downloaded onto his own personal, non-BMS laptop computer. My understanding is that JHAVERI showed these documents to the individual for the purpose of demonstrating to him that he was prepared to launch a biopharmaceutical venture in India and to obtain from the individual financing and/or an investment to fund that venture. JHAVERI showed the individual a directory of computerized files from his laptop during this meeting that he described to the individual as substantially all of the SOPs maintained at BMS Syracuse. JHAVERI arrived at the meeting in the hotel room with a large backpack and other items, which together included JHAVERI's personal laptop computer, what was described to me as a 250GB hard drive, and a business plan related to the launching of JHAVERI's planned pharmaceutical venture in India.

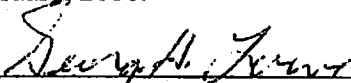
21. After observing the meeting, I interviewed JHAVERI. He admitted during this interview that (a) he had taken 1327 SOPs from BMS without authorization and (b) that he previously had made available to the individual three BMS SOPs that he had taken from BMS and placed into an email in a Gmail account he had recently created specifically for that purpose. Later, JHAVERI confirmed to me in a signed written statement that he had taken these three BMS SOPs and made them available to the individual using the Gmail account and that he "understood that the documents were proprietary and confidential and that he should not have shared them with unauthorized persons."

Conclusion

22. Based upon the above information, I believe that probable cause exists to believe that in or about January of 2010 and continuing until February 2, 2010, in the Northern District of New York and elsewhere, the defendant, SHALIN JHAVERI, with the intent to convert trade secrets that are related to or included in products that are produced for or placed in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secrets, and knowing and intending that the offense would injure any owner of the trade secrets, knowingly did steal and without authorization appropriate, take, carry away and conceal, and by fraud, artifice and deception obtain such information, in violation of Title 18, United States Code, Section 1832(a).

  
Timothy M. Dwyer, Special Agent  
Federal Bureau of Investigation

Sworn to me this 3d day of  
February, 2010.

  
Honorable George H. Lowe  
United States Magistrate Judge