

Reported Criminal Arrests And Convictions Under The Economic Espionage Act of 1996

TABLE OF CONTENTS

1. [United States of America v. Patrick and Daniel Worthing, Criminal No. 97-9 \(W.D. Pa. December 7, 1996\).](#)
2. [United States of America v. Kai-Lo Hsu, et al., Criminal No. 97-CR-323,97- 1965 \(E.D. Pa. July 10, 1997\).](#)
3. [United States of America v. Pin Yen Yang et. al., Criminal No. 97 CR 288 \(N.D. Ohio September 4, 1997\).](#)
4. [United States of America v. Steven Louis Davis, Criminal No. 97-00124 \(M.D. Tenn. 1997\).](#)
5. [United States of America v. Mayra Justine Trujillo-Cohen, Criminal No. H- 97-251S \(S.D. Texas 11/14/97\).](#)
6. [United States of America v. Carroll Lee Campbell, Jr. \("Athena"\), 98-CR- 059 \(N.D. Georgia 2/25/98\).](#)
7. [United States of America v. Huang Dao Pei, Criminal No. 98-CR-4090 \(D. N.J. July 27, 1998\).](#)
8. [United States of America v. David T. Krumrei, 98-80943, 98-00300 \(D. Hawaii 5/14/98\).](#)
9. [United States of America v. Caryn L. Camp and Stephen R. Martin, 98-48-P- H \(D. Maine 9/16/98\).](#)
10. [United States of America v. Steven Hallsted and Brian Pringle, Criminal Case No. 4: 98M37 \(E.D. Texas 2/26/98\).](#)
11. [United States of America v. John Fulton, Criminal Case no. 98-059 \(W.D. Penn. 1998\).](#)
12. [United States v. David Sindelar Criminal Case No. 98-2000-70-01-EEO \(District of Kansas 10/16/98.\)](#)
13. [United States v. David B. Kern 99 CR 15 DFL \(E. D. Calif. 3/5/99\).](#)
14. [United States v. Robin Carl Tampoe H-99-158 \(S. D. Texas 3/24/99\).](#)
15. [United States v. Eon Joong Kim 99-CR-481 \(N. D. Illinois July 1999\).](#)
16. [United States v. Matthew R. Lange \(Eastern District of Wisconsin 9/7/99\).](#)
17. [United States v. Jack Shearer/Tejas et.al. 3:99-CR-43-3-D \(Northern District of Texas 1999\).](#)
18. [United States v. Costello, H-99-623 \(S. D. Texas 1999\).](#)
19. [United States v. Corgnati, CR-99-6268 \(Southern District of Florida 1999\).](#)
20. [United States v. Say Lye Ow, CR-00-21110 \(San Jose California 3/29/00\).](#)
21. [United States v. Mark Everheart, CR-00-56 \(W.D. Pa. 2000\).](#)
22. [United States v. Mikahel Chang and Daniel Park, CR-00-20203 \(N.D. California 2000\).](#)
23. [United States v. Jolene Neat-Rector and Steven Snyder, CR-123-T-24C \(M.D. Fla. 2000\).](#)

24. [United States v. Peter Morch \(N.D. Calif. November 21, 2000\).](#)
25. [United States v. Fausto Estrada \(S.D.N.Y. March 21, 2001\).](#)
26. [United States v. Kurtis Kenneth Cullen and Bruce Zak \(W.D. KY April 18, 2001\).](#)
27. [United States v. Junsheng Wang and Bell Imaging Technology Corp. \(N.D. Calif. April 19, 2001\).](#)
28. [United States v. Hai Lin, Kai Xu, Yong-Qing Cheng \(May 3, 2001\)/United States v. ComTriad et. al. \(D.N.J. May 31, 2001\).](#)
29. [United States v. Takashi Okamoto, Hiroaki Serizwa, \(N.D. Ohio, May 8, 2001\).](#)
30. [United States v. Nicholas Daddona, Case No. 3:01CR122AVC \(D. Conn. June 6, 2001\).](#)
31. [United States v. Xingkun Wu, Case No. _____ \(Rochester, NY July 31, 2001\).](#)
32. [United States v. Thomas Kissane, Case No. _____ \(SDNY February, 2002\).](#)
33. [United States of America v. Tse Thow Sun, Case No. _____ \(Monterey, California, April 11, 2002\).](#)
34. [United States of America v. Jeffrey A. Forques, Case No. _____ \(Boston April 25, 2002\).](#)
35. [United States v. Jeffrey W. Dorn \(District of Kansas May 2, 2002\).](#)
36. [United States v. Zhu, Case No. 02-M-0421 \(June 19, 2002\).](#)
37. [United States v. Kissane, \(S.D.N.Y. October 15, 2002\).](#)
38. [United States v. Morris \(D. Delaware October 17, 2002\).](#)
39. [United States v. Ye \(N.D. California December 4, 2002\).](#)
40. [United States v. Serebryany \(January 16, 2003\).](#)

1. [United States of America v. Patrick and Daniel Worthing, Criminal No. 97-9 \(W.D. Pa. December 7, 1996\).](#)

Patrick Worthing worked at PPG Industries, Inc. under a contract with Affiliated Building Services as the supervisor of a maintenance crew at one of PPG's research and development facilities. Patrick Worthing, with access to every office, surreptitiously collected diskettes, blueprints and other types of confidential research information from PPG Industries. The indictment was based on an FBI sting operation prompted by a letter Patrick Worthing wrote to Owens-Corning, a PPG rival attempting to sell the proprietary PPG information.

Patrick Worthing and his brother, Daniel Worthing, were indicted under the Economic Espionage Act, 18 U.S.C. Sections 1832(a)(1), (3) and (5). Patrick Worthing pled guilty on 2/27/97 to theft of trade secrets and was sentenced on June 5, 1997 to 15 months in jail, 36 months supervised release.

Daniel Worthing, who reportedly agreed to help his brother the night before for \$100,000 pled guilty on 1/31/97 to conspiracy to possess and deliver trade secrets and was sentenced on 4/18/97 to 60 months probation and 6 months home confinement.

2. [United States of America v. Kai-Lo Hsu, et al., Criminal No. 97-CR-323,97-1997](#). 1965 (E.D. Pa. July 10, 1997).

This case involved the alleged theft of trade secrets relating to Bristol-Myers' anti-cancer drug Taxol. Specifically, the trade secrets related to a new process for the production of Taxol by genetic engineering. According to published reports, Kai-Lo Hsu (a technical director for Taiwan's Yuen Foong Paper Co.) and Chester S. Ho (a biochemist and professor at a Taiwan university) were arrested on June 14 during an FBI sting operation at the posh Four Seasons Hotel in Philadelphia. The secret meeting was arranged by a "technology information broker" who was accompanied by a person posing as a corrupt Bristol-Myers' scientist.

The indictment alleged that Kai-Lo Hsu and Jessica Chou agreed to initially pay \$400,000 for the Taxol technology. Chester S. Ho was apparently at the June 14 secret meeting to verify the value of the secret Taxol technology. According to published reports, Jessica Chou is believed to be in Taiwan which does not have an extradition treaty with the United States. Yuen Foong Paper Co. reportedly called the charges "completely groundless and untrue" and the company is still under investigation for possible indictment under the Economic Espionage Act of 1996.

According to the U.S. Attorney's Office in Philadelphia, the case originated with an FBI sting operation set up in 1994 to act as a "technological information broker."

The indictment involves 18 U.S.C. Section 1832(a)(4) (attempted theft of trade secrets) and 18 U.S.C. Section 1832(a)(5) (conspiracy to steal trade secrets). On July 10, 1997, FBI Director Louis J. Freeh issued a press release after the indictments were returned in Philadelphia commending Bristol-Myers Squibb for their commitment to work with the FBI and the U.S. Attorney's Office to successfully thwart attempts by foreign business interests to steal these extraordinarily valuable trade secrets:

"Economic espionage is estimated to be a multi-billion dollar threat to American business and industry, costing significant losses of jobs and competitiveness as a result of sophisticated efforts to steal trade secrets and other proprietary information. Congress wisely created a powerful new statute that allows the FBI and industry to form strong alliances against economic theft and international economic espionage. This Act, enacted last year by Congress, significantly strengthens our ability to work with industry to safeguard valuable information and prosecute those, either domestic or foreign, who steal valuable trade secrets."

"The unflinching pursuit of this investigation by the U.S. Attorney's Office and the Philadelphia FBI signals FBI's commitment to use this new law to help industry protect against ruthless predators, both domestic and foreign, who steal trade secrets to the great detriment of American businesses and jobs." On March 31, 1999, Kai-Lo Hsu pled guilty to one count of conspiracy to commit trade secret theft; sentenced 7/13/99 (Time served plus probation; \$10,000 fine). All other counts against him were dismissed. The government dropped all charges against Chester S. Ho.

3. [United States of America v. Pin Yen Yang et. al.](#), Criminal No. 97 CR 288 (N.D. Ohio September 4, 1997).

Pin Yen (P.Y.) "Pat" Yang, 70, and his daughter, Hwei Chen "Sally" Yang, 39, were arrested by FBI agents on September 4, 1997 at Cleveland Hopkins International Airport. They were traveling to New York to see the U.S. Open tennis championship. According to published reports, hours earlier, closed-circuit television recorded Pin Yen Yang taking out a small pocket knife and cutting off a portion of the cover page marked "confidential" and "Property of Avery Dennison Corp." from documents he had just been given at the Westlake Holiday Inn.

Both defendants are charged with mail and wire fraud, conspiracy to steal trade secrets, money laundering and receipt of stolen goods from the Avery Dennison Corporation facility in Concord, Ohio. 18 U.S.C. Section 1832. Also 18 U.S.C. Sections 1341, 1343, 1956, 2315. P.Y. Yang is the president of Four Pillars Enterprise Company, LTD, of Taiwan which has more than 900 employees and annual revenues of more than \$150 million. Four Pillars manufactures and sells pressure-sensitive products mainly in Taiwan, Malaysia, Singapore, the United States and the Peoples Republic of China.

Hwei Chen Yang is a corporate officer involved with research and development at Four Pillars. She is believed to hold dual citizenship in the United States and Taiwan.

Avery Dennison, based in Pasadena, California, is one of the nation's largest manufacturers of adhesive products which include postage stamps and mailing labels. The company employs some 16,000 people world-wide.

According to published reports, Ten Hong Lee, an Avery Denison researcher at Avery's manufacturing complex in Concord Township, Ohio confessed to giving Four Pillars "highly sensitive and valuable proprietary manufacturing information and research data" since 1989 and reportedly was paid over \$150,000 (over eight years) by Four Pillars as a "consultant." To conceal the scheme, arrangements for payment were made through Lee family members in Taiwan.

The Cleveland Plain Dealer reported on October 12, 1997, that in an earlier FBI sting operation, Ten Hong "Victor" Lee attended a meeting at Avery Denison in January, 1997 where he and others were told of a binder containing confidential information on Avery's plans for the Far East. Closed-circuit TV later showed Lee three times gaining access to the file drawer where the binder was kept, once wearing gloves when he removed it from the office for a few minutes. Confronted by FBI agents in March 1997, Lee admitted he had been providing confidential information to Four Pillars. Thereafter, Lee pleaded guilty to wire fraud, turned over to the FBI a "trove" of Avery Denison documents, and cooperated in an undercover capacity with the FBI leading to the arrest of the Yangs on September 4, 1997.

Federal prosecutors estimate that the research and development costs expended by Avery Dennison to develop the information obtained by the defendants could exceed between \$50 million and \$60 million.

The case has been tried to a jury in Federal District Court in Cleveland. Closing arguments were had on Friday, April 23, 1999. U. S. Assistant Attorney Marc Zwillinger argued to the

jury in closing arguments that P.Y. Yang, chief executive of Taiwan-based Four Pillars Ltd. and his daughter, Hwei Chang "Sally" Yang "knew Avery Dennison was a world leader in the adhesive industry" and paid an Avery Dennison Corp. employee (Ten Hong "Victor" Lee) to steal Avery Dennison's confidential and proprietary information.

According to the Plain Dealer (Saturday April 24, 1999), to bolster arguments that the Yangs and their company intentionally stole Avery Dennison's proprietary information, prosecutors replayed portions of a tape showing the Yangs clipping confidential stamps and Avery Dennison logos off papers delivered by Lee to the hotel room in September 1997.

The Yangs did not testify at the trial and the Yangs' lawyers argued that their clients never asked Lee to steal his employer's trade secrets and that the engineer took them on his own.

Deliberations in the case were scheduled to begin on Monday, April 26, 1999. Jurors in Federal court in Youngstown deliberated for about 18 hours over three days before finding P. Y. Yang, chief executive of the Taiwan-based Four Pillars Ltd., and his daughter, Hwei Chang Yang, guilty of economic espionage. Four Pillars itself was also convicted on the espionage charges. The Yangs were acquitted of mail fraud charges.

According to Asianet (April 29, 1999), Avery Dennison issued a statement after the guilty verdict: "There was never any doubt in our minds that the evidence of illegal activity by Four Pillars was overwhelming."

U.S. District Judge Peter C. Economus fined Four Pillars Enterprises Ltd. \$5 million and sentenced Pin Yen Yang, 73, the company's former chief executive, to six months of home confinement and a \$250,000 fine. His daughter, Hwei-Chen "Sally" Yang, 41, a former Four Pillars executive, was fined \$5,000 and received one year of probation.

Pin Yen Yang apologized at his sentencing and said it was not his intention to steal trade secrets. "I'm deeply sorry for what I've done," Yang said. Federal prosecutors objected that no prison time was imposed. "Is the message, If you steal information from your competitor, you'll be given a probationary term?" Assistant U.S. Attorney David Green said.

Attorneys for both companies declined to comment because Avery Dennison's civil lawsuit against Four Pillars is scheduled for trial Monday (January 10, 2000) in U.S. District Court in Cleveland.

According to published reports, on February 4, 2000, a Cleveland jury in the civil trial returned a verdict awarding Avery Dennison \$10 million for trade secret misappropriation, \$10 million for RICO violations, \$10 million for conversion, and \$30 million in punitive damages. The Sixth Circuit Court of Appeals on Wednesday, February 20, 2002, ruled that Judge Peter C. Economus failed to explain why he gave the two executives (Pin Yen Yang, former chief executive of Four Pillars and his daughter, Hwai-Chen "Sally" Yang) relatively light sentences while fining the company (Four Pillars Enterprises Co. Ltd.) the maximum amount allowed by law (\$5 million). The case was remanded for resentencing.

Steven L. Davis was a process control engineer for Wright Industries, Inc. in Nashville, Tennessee. In the summer of 1996, the Gillette Company retained Wright Industries, Inc. to assist in the development of Gillette's next generation of razor systems. Davis was assigned to be the lead process control engineer on the Gillette Project and he executed a Confidentiality Agreement. According to the grand jury indictment, Wright Industries, Inc., at Gillette's request, removed Davis as the lead process control design engineer in late September, 1996.

Thereafter, according to the grand jury indictment, Davis sent highly confidential engineering drawings relating to the Gillette Project to Gillette's competitors, including Bic Corporation, American Safety Razor, and Warner Lambert, in violation of 18 U.S.C. Sections 1832 (a)(2) and (3).

Davis contacted Gillette's competitors by facsimile and E-Mail using anonymous names "Melinda Ivy" and "Carl Brown" and the computer handles "PSDUMC" and "carl.brown." Davis also represented, in soliciting further interest, that he had 600 "megs" of Gillette's product drawings, equipment drawings and assembly drawings relating to Gillette's next generation of razor systems. In addition to violation of the EEA, Davis was also charged with wire fraud pursuant to 18 U.S.C. Section 1343.

Davis pled guilty on January 26, 1998 to all five counts and was sentenced on April 17, 1998 to 27 months imprisonment, 3 years supervised release. In addition, David was ordered to pay restitution of \$508,575 to Gillette and \$726,576 to Wright Industries.

5. [United States of America v. Mayra Justine Trujillo-Cohen, Criminal No. H- 97-251S \(S.D. Texas 11/14/97\).](#)

The U. S. Attorney's Office in Houston, Texas brought a two-count indictment under the EEA alleging the theft of trade secrets against Mayra Justine Trujillo-Cohen, a former employee of Deloitte & Touche. Ms. Trujillo-Cohen was a former consultant for Deloitte & Touche.

According to the grand jury charges, when she left Deloitte & Touche, Ms. Trujillo-Cohen took a proprietary software program called the "AFRONT for SAP" program. Apparently, Ms. Trujillo-Cohen thereafter allegedly deleted references to Deloitte & Touche and resold the program (or portions of the program) to a third-party company for profit. The third-party company was not indicted. Mayra Justine Trujillo-Cohen pled guilty to one count of theft of trade secrets and one count of wire fraud on July 30, 1998.

Ms. Trujillo-Cohen was sentenced on 10/26/98 to 48 months imprisonment, 3 years supervised release, \$337,000.00 in restitution and a \$200.00 special assessment.

6. [United States of America v. Carroll Lee Campbell, Jr. \("Athena"\), 98-CR- 059 \(N.D. Georgia 2/25/98\).](#)

Carroll Lee Campbell, Jr., former Circulation Manager of the Gwinette Daily Post, his wife Susan Campbell, and Paul Edward Soucy, former District Circulation Manager of its sister

paper, The Rockdale Citizen, were arrested by FBI agents on February 6, 1998 after they allegedly offered to sell marketing plans and subscription lists to the Atlanta Journal-Constitution for the sum of \$150,000.

In September 1997, there was ongoing litigation between the Atlanta Journal-Constitution and the Gwinnett Daily Post newspaper relating to a dispute involving the legality of 34,000 paid newspaper subscriptions relating to a contract between the Gwinnett Daily Post newspaper and a cable TV operator. Carroll Lee Campbell, Jr. was a circulation manager for the Gwinnett Daily Post newspaper. Using the alias -- "Athena" -- Campbell sent a letter to the attorneys representing the Atlanta Journal-Constitution (and to business representatives of the Atlanta Journal-Constitution) in September, 1997 offering to provide the Cable Equities Agreement and other proprietary financial and business information to the Atlanta Journal-Constitution's lawyers to assist them in the lawsuit against the Gwinnett Daily Post newspaper. The offering price for this information was \$150,000.

If the Atlanta Journal-Constitution was interested, "Athena" instructed the newspaper to place an ad in the "Personals" section of the newspaper. The FBI was contacted and a sting operation was set up. In December, 1997 the Atlanta Journal-Constitution's lawyers, in cooperation with the FBI, placed an ad in the "Personals" section entitled "Message to Athena." Thereafter, there were further communications with "Athena" who demanded that the Atlanta Journal-Constitution's lawyers "show me the money." Arrangements were made with an undercover FBI agent to meet "Athena" at a local shopping center to exchange an initial payment of \$5000 (delivered in \$100 bills) in exchange for an initial sample of the proprietary information. The rest of the money would then be paid later in exchange for the rest of the proprietary information.

After Carroll Lee Campbell obtained the \$5000, Susan Campbell allegedly gave \$1500 of the money in \$100 bills to Paul Edward Soucy (a circulation manager for the sister Rockwell Citizen newspaper). Carroll Lee Campbell also allegedly attempted to obtain additional trade secret information including a circulation list that he offered another employee \$300 to obtain. Published reports also indicate that Soucy was acting as a "lookout" for "Athena" at the local shopping center meetings.

Mr. Campbell pled guilty on 5/27/98 to conspiracy to steal trade secrets and was sentenced on 8/25/98 to 3 months imprisonment, home confinement for 4 months with electronic monitoring detention, 3 years supervised release, \$2800 restitution, \$100 special assessment. Apparently, the charges against Susan Campbell were dismissed.

Prologue: (The following E-mail was received from Carroll Lee Campbell, Jr. on April 30, 2002.

"Although my ex wife Susan Campbell was indeed indicted on conspiracy charges (mainly to get myself to cooperate with the Feds) those charges were eventually dropped because Susan did not know the source of the \$1500 she gave to Paul Soucey. She thought it was a personal loan from me to Paul for "home improvements". Paul Soucey (becoming a federal witness) had only told the FBI that he was paid \$1500 by Susan. Therefore implicating her. She was an innocent party. Also... as a final follow up I was sentenced to 3 months (90 days) in the Federal Penitentiary in Atlanta and 4 months on "in house" electronic monitored arrest with 3

years supervised probation in which I was released early after serving only 2 years. While the federal judge was mandated by sentencing guidelines... I won most of my presentencing motions as the judge saw that my reason for "theft of trade" secrets was not motivated by greed as the government tried to indicate but rather it was to hire professional help for my autistic twins (re: Speech therapists, occupational therapists etc.) I found Federal Judge Orinda Evans an island of reason after dealing with the tumultuous sea of FBI and prosecutors, and Judge Evans was sympathetic while following the mandatory sentencing guidelines. Since my release from prison, Susan and I have divorced, I have become a publisher of a newspaper in Oklahoma and own my own newspaper consulting company specializing in 3rd party paid newspaper circulation. I have raised thousands of dollars for the Oklahoma National Memorial on behalf of the Oklahoma Press Association and sat next to then President Bill Clinton at its dedication in 2000, and I received the Habitat For Humanity Award in Atlanta for getting large corporate sponsors to support inner city reading programs through Project Read, and raised thousands of dollars for the victims of the May 3rd tornado that ravaged Oklahoma City in 1999. The irony of the whole incident is that had I not asked for money... I would have been a hero for exposing the Gwinnett Daily News' fraudulent "paid" circulation. But since I asked for remuneration...(for whatever reason)...I became a "corporate spy". It is my understanding that Gray Inc., (parent company of the Gwinnett Daily News) had to purchase the cable company or else they would've been prosecuted of defrauding advertisers. In conclusion... A mistake does not define me as a human being. It was just a mistake. Thank you for allowing me to sound off. C. Lee Campbell II."

7. [United States of America v. Huang Dao Pei, Criminal No. 98-CR-4090 \(D. N.J. July 27, 1998\).](#)

The FBI arrested a former scientist at Roche Diagnostics in August, 1998 in New Jersey on charges he tried to steal trade secrets for a hepatitis monitoring kit he hoped to sell in China.

Huang Dao Pei, a Chinese-born naturalized U.S. citizen living in Piscataway, N.J., allegedly tried to buy information from a scientist who worked for Roche. The scientist was cooperating with the FBI in a sting operation and secretly tape-recorded Huang.

Huang told the Roche scientist that he needed to get information about Roche's hepatitis C diagnostic testing kit so his firm, LCC Enterprises, could develop a similar kit and sell it in China, prosecutors say. Huang worked for Roche from 1992 to 1995.

Huang Dao Pei was released on a \$100,000 bond pending trial.

8. [United States of America v. David T. Krumrei, 98-80943, 98-00300 \(D. Hawaii 5/14/98\).](#)

Indictment filed on May 14, 1998. Wilsonart International, Inc., located in Temple, Texas, produces laminates used to manufacture furniture, kitchen and bathroom countertops, residential floors and other items used in the construction of residential and commercial buildings throughout the world. In 1995, Wilsonart retained the services of Vactec Coatings, Inc/Robert Amis to use a planar magnetron sputter coating machine to conduct certain R&D tests for Wilsonart. In turn, Vactec retained another Michigan company (Federal Industrial Services, Inc.) to assist Mr. Amis with the planar magnetron sputter coating machine tests. David Krumrei was hired by Federal Industrial Services and in this position obtained access

to Wilsonart's trade secret technology. Wilsonart then worked with the FBI to set up a sting operation by arranging a meeting with Krumrei in Hawaii to exchange he information and money. Krumrei was arrested at that meeting and charged under the EEA. The case has since been transferred to the U.S. District Court for the Eastern District of Michigan.

Thereafter, David Krumrei telephoned a Wilsonart competitor in Australia (CSR Limited)--apparently from Hawaii--and advised CSR Limited that-- in return for employment in Australia--that he could provide CSR Limited with the unique formula for surface coating that Wilsonart had developed. Thereafter, CSR Limited (Henry Pens--Executive General Manager) contacted Wilsonart and offered to do everything possible to assist Wilsonart in protecting their trade secrets. David Krumrei pled guilty on July 27, 1999. The Rule 11 Plea Agreement provided that any sentence of incarceration would not exceed 30 months. On November 18, 1999, David Krumrei was sentenced to two years imprisonment, \$10,000 restitution, \$100 special assessment.

9. [United States of America v. Caryn L. Camp and Stephen R. Martin, 98-48-P- H \(D. Maine 9/16/98\).](#)

Caryn L. Camp, 31, of Portland, Maine developed a relationship on the Internet with Stephen R. Martin of Sonoma, California according to published reports. An E-mail note from Camp to Martin was inadvertently misdirected to a Idexx co-worker and stated as follows: "They know I've been stealing, so-to-speak, from the company and sending information to someone. Can I go to jail for this? I am so scared." According to prosecutors, Camp used E-mail, the postal service and commercial carriers to send proprietary Idexx documents, including laboratory notebooks, customer lists, sales reports, and other information to Stephen Martin.

The two initially became acquainted when Martin applied to Camp for a job via the Internet. Thereafter, an Internet relationship developed, and according to published reports, Martin told Camp she was the type of person he would like to hire, that her efforts would be "richly rewarded" and that "you may become CEO yourself."

Martin wrote further to Camp that if his company were successful in marketing a veterinary diagnostic test similar to the one marketed by Idexx that "we'll give you enough bonus money to buy your own house in cash. Maybe on a lake." Both have been indicted and pled innocent. Martin's two companies, Dna Vaccine and Maverck Technologies, had no employees or assets. No Idexx trade secrets ever reached Idexx competitors. According to published reports, Caryn was "a very lonely and isolated person." Apparently the two met just shortly before they were arrested in Denver, Colorado. Camp allegedly realized then that Martin was not a successful businessman -- but a dreamer -- when he showed up with a long beard, in tied-died clothes, driving a VW van.

Caryn L. Camp, 33, pled guilty to 15 counts on July 22, 1999 and agreed to testify on behalf of the government against Martin. Camp was sentenced on 12/17/99 to 3 years probation, \$7,500 restitution, \$1,500 special assessment. On August 16, 1999, after a day and a half of deliberations, the jury returned a guilty verdict on 8 of 15 counts, including mail fraud, wire fraud, conspiracy to steal trade secrets and conspiracy to transport stolen property.

Stephen Martin of stealing trade secrets from Idexx Laboratories. The Associated Press (8/17/99) reported that the panel of eight women and four men found Martin guilty of four

counts of wire fraud, two counts of mail fraud, and one count each of conspiracy to steal trade secrets and conspiracy to transport stolen goods. (Martin was acquitted of six counts of wire fraud and one count of interstate transportation of stolen goods). Martin, 52, said he was shocked by the verdict but would not elaborate.

The evidence at trial portrayed Martin manipulating Caryn Camp to send him secrets about Ivexx to start a competing company and Caryn Camp would be rewarded for her spying. In separate E-Mails, he promised her a position in the new company...and later wrote "you may become the CEO yourself." In contrast, defense lawyer William Schaffer portrayed Stephen Martin and Caryn Camp as "two lonely people" alleging that no real trade secrets ever changed hands.

Assistant U.S. Attorney Toby Dilworth showed jurors a notebook with 250 e-mails most of which passed between Camp and Martin. In one E-Mail, Martin wrote: "I never had a spy before. We are going to be in the veterinary business big time." The relationship between Camp and Martin ended after Camp accidentally sent an E-Mail intended for Martin to a co-worker. She was fired shortly afterward. Later she learned that Martin was not a successful entrepreneur but a dreamer who lived with his mother and drove a VW van.

According to the Associated Press (July 23, 1999), Camp wrote in a July, 1998 e-mail to Martin: "Aren't I awful? I like this spying business way too much." "They know I have been stealing, so to speak, from the company and sending info to someone. Can I go to jail for this? I'm so scared" reads the e-mail that was mis-directed to a co-worker the day Camp was planning to resign from Idexx. Camp had worked there three years as a chemist and technical service representative. Camp first came in contact with Martin when she e-mailed her resume to the website of Wyoming Dna Vaccine, a fledging business in which Martin had no ownership interest.

Court records show that Martin asked about Idexx's prices, the nature of Idexx's test kits and other questions about the proprietary aspects of Idexx's business. Camp's attorney, Thomas Connolly, stated that Camp decided to change her plea to guilty based upon more than 200 e-mail messages found in her computer. Martin's attorney argued that Martin and Camp were "pen-pals" and the e-mails were taken out of context. For example, Martin's attorney argued that the e-mail ("I never had a spy before") should not be taken literally and "merely reflects the playful hyperbolic communication style of both Camp and Martin."

Martin had been living with his mother at a mobile home retirement community when he was arrested and all of his "research" was impounded last year. "I didn't think about the use of certain terms in my e-mail...we were pen-pals." Martin said. However, the Associated Press reports that box loads of documents and e-mails changed hands including pages from laboratory notebooks, an internal Idexx product study, customer lists, and documents about Idexx's competitors in the business of making diagnostic equipment for veterinarians.

The Associated Press (December 22, 1999) reports that Martin had five college degrees including a doctorate in immunology from the University of California at Berkeley but has earned his living with occasional logging, roofing and woodworking jobs. He has applied for several patents but has not come up with the cash necessary for clinical tests on his theories. "I'm a bio-nerd," Martin says. "I am not a freak, I am not crazy, my heart is in the right place." Martin must report to prison on January 20, 2000, according to Assistant U.S. Attorney Toby Dilworth.

On December 20, 1999, Martin was sentenced to 366 days imprisonment, 3 years supervised release, \$7,500 restitution, \$800 special assessment.

On March 18, 2002, the San Francisco Chronicle reported that Stephen Martin is not angry about being only the second person brought to trial under the Economic Espionage Act of 1996 and he is not pleased about the year he spent in federal prison as a convicted industrial spy. However, the thing that "gets Martin's bacon sizzling" is that people still have a totally cavalier attitude about E-mail. "They think they can say anything in an e-mail," he told (reporter David Lazurus). "People don't realize the horrible things that can happen."

10. [United States of America v. Steven Hallsted and Brian Pringle, Criminal Texas 2/26/98](#).

Case No. 4: 98M37 (E.D.

Using an Internet ad, Pringle and Hallstead allegedly advertised the availability of these five prototype Intel CPUs. Working with the FBI, Cyrix and Intel arranged for Pringle and Hallstead to bring the CPUs to the Cyrix location in Texas for Cyrix personnel to inspect and hopefully purchase. One of the CPUs were identified as the five stolen from Intel in California, Hallstead and Pringle were arrested.

Pringle pled guilty on 6/2/98 to conspiracy to commit theft of trade secrets. On July 15, 1998, Hallsted pled guilty to conspiracy to commit theft of trade secrets.

On December 4, 1998, U.S. District Judge Paul Brown sentenced Steven Craig Hallstead, 29, to 77 months imprisonment and \$10,000 restitution. Brian Russell Pringle, 34, was sentenced to 60 months imprisonment and \$50,000 restitution.

11. [United States of America v. John Fulton, Criminal Case no. 98-059 \(W.D. Penn. 1998\)](#).

John Fulton, a former employee of Joy Mining Machinery Inc., was charged with attempting to buy proprietary schematic designs for an MS-14 model of a chock interface unit, an electronic switchbox that operates of a coal mining machine known as a longwall shearer, produced by Joy Mining.

Fulton pled guilty on 4/17/98 to theft of trade secrets. Before sentencing Fulton on November 13, 1998, U.S. District Judge Donetta W. Ambrose noted that Fulton had tried to recruit a Joy employee as an industrial spy. In his guilty plea, Fulton admitted to offering the worker \$1500 for proprietary information. Fulton was sentenced to 12 months home detention and 5 years probation.

12. [United States v. David Sindelar Criminal Case No. 98-2000-70-01-EEO \(District of Kansas 10/16/98.\)](#)

Theft of proprietary information from employer (Preco). Information filed on 10/16/98. The Defendant pled guilty on 10/16/98 to one count of theft of international trade secrets and was sentenced on March 1, 1999 to 5 years probation; \$16,618.35 restitution, \$10,000 fine, \$100 special assessment.

13. [United States v. David B. Kern 99 CR 15 DFL \(E. D. Calif. 3/5/99\)](#).

The indictment was filed on March 5, 1999. The indictment alleges that David Kern copied proprietary information from a laptop computer inadvertently left by a service technician for Varian Medical Systems, Inc. at a hospital where Mr. Kern serviced the million-dollar cancer treatment Varian machines for a competitor (Sacramento-based Radiological Associates). "In the course of misappropriating Varian's trade secret, the defendant copied files from the Varian service technician's laptop after hooking it up to his own desktop computer using a Laplink program." David Kern commenced a wrongful termination suit against Radiological Associates after he was fired (June 1995) and then Varian entered its appearance and filed a cross-complaint against Kern for trade secret misappropriation (which occurred in October 1996).

Further details of the case were provided by Russ Atkinson (now Senior Manager for Netscape, AOL West) at the recent High Technology Crime Investigation Association (HTCIA) International Conference in Chicago.

David Kern's deposition was taken in the civil action. During the deposition, Kern admitted that the Varian files which he copied to his desktop computer were proprietary. When then asked whether he had permission to copy the files, his lawyer in the civil case advised Kern to "take the Fifth Amendment." and he refused to answer the question. The civil deposition was videotaped under oath and the transcript was subsequently turned over to the FBI. Apparently, Kern had also obstructed civil discovery by refusing to turn over his computer files for inspection and copying.

The FBI then commenced an investigation and grand jury subpoenas were issued for David Kern's computer. Thereafter, Varian's technicians, at the request of the FBI, reviewed the contents of the recovered files, identified the theft of proprietary information, and provided original copies to the FBI. Thereafter, in the civil suit, the trial court awarded sanctions barring Kern's testimony and evidence for failure to comply with civil discovery requests and entered summary judgment awarding Varian \$3.5 million in damages. In the criminal action, a pre-indictment plea agreement was worked out, but Kern reneged, his attorney was fired, and Kern was thereafter indicted on March 5, 1999.

On October 25, 1999, the Los Angeles Times quoted Russ Atkinson, a former FBI special agent and legal advisor who was second in command of the FBI's high-tech task force in San Jose, California. Atkinson cited the \$3.5 million civil judgment stating that the man might never have been caught if he hadn't bragged of his deed to associates who notified Varian. The engineer is now awaiting criminal trial which would be the first criminal prosecution under the EEA in California.

Ms. Kathy Dunlap, a Radiological director, has acknowledged in the press that "We did contact Varian because we had questions about the information we had." On January 13, 2000, David Kern pled guilty to one count of theft of trade secrets. On April 4, 2000, David Kern was sentenced to 1 year imprisonment and 3 years supervised release.

14. [United States v. Robin Carl Tampoe H-99-158 \(S. D. Texas 3/24/99\)](#).

Indictment filed 3/24/99. The alleged EEA violations involved an employee (Tampoe) and IBM proprietary technology. The case was assigned to Judge David Hittner.

The Defendant pled guilty to Count 2 (attempted theft of trade secrets) and Count 3 (forfeiture) of the superseding indictment. Count 1 (theft of trade secrets) of the superseding indictment and both counts of the original indictment were dismissed at sentencing.

Tampoe was sentenced on 10/25/99 to 15 months imprisonment followed by 2 years' supervised release. Judge Hittner made a finding of no ability to pay and did not assess a fine. Defendant ordered to forfeit \$5000 in cash and special assessment of \$100.

15. [United States v. Eon Joong Kim 99-CR-481 \(N. D. Illinois July 1999\).](#)

Complaint filed July 1999. Alleged EEA violation involved a 3COM employee (Kim). Complaint dismissed without prejudice on October 1, 1999.

16. [United States v. Matthew R. Lange \(Eastern District of Wisconsin 9/7/99\).](#)

The indictment filed 9/7/99 alleges that Matthew Lange, 24, tried selling engineering drawings of aircraft parts belonging to Replacement Aircraft Part Co. Inc. (RAPCO) to a RAPCO competitor. According to published reports, prosecutors assert that Lange (a draftsman) altered proprietary warnings on the RAPCO drawings making them look like his own. Using an alias and dummy e-mail account, Lange then contacted an executive at the RAPCO competitor saying "you must admit it is nice to have an \$8 million company handed to you (I see a smile on your face)."

The executive at the RAPCO competitor called RAPCO and told them about the security breach. "The cooperating informant took the high road" and is not a co-defendant reported U.S. Assistant Attorney Eric Klumb who filed the case in the U.S. District Court in Milwaukee.

Matthew Lange was convicted on December 12, 1999 of violating the EEA, copyright infringement and wire fraud. Lange was sentenced on 3/2/00 to 30 months imprisonment, 3 years supervised release, \$2500 fine and \$525 special assessment.

17. [United States v. Jack Shearer/Tejas et.al. 3:99-CR-43-3-D \(Northern District of Texas 1999\).](#)

Jack Shearer, 53, the owner of two Conroe, Texas energy parts companies, has admitted to corporate spying and has pled guilty under the Economic Espionage Act. Conroy admitted that he built an \$8 million business using information stolen from Caterpillar, Inc. From 1995 to 1998, Jack Shearer paid more than \$100,000 to three employees at Caterpillar's Solar Turbines subsidiary in San Diego, California to steal plans used to make parts for oil field and pipeline machinery, said Paul E. Coggins, U.S. Attorney for the Northern District of Texas.

According to a Press Release by the Justice Department, Shearer admitted that he stole proprietary trade secrets from his former employer, Solar Turbines, Inc. (Solar) headquartered in San Diego, California. Solar designs and manufactures industrial gas turbine engines and turbo machinery systems for the production and transmission of crude oil, petroleum products and natural gas; thermal energy and generating electricity for a wide variety of industrial applications and the fast ferry marine market. Solar, with approximately 5100 employees worldwide, is a wholly owned subsidiary of Caterpillar, Inc., the world's largest manufacturer of construction and mining equipment, diesel and natural gas and industrial gas turbines.

Shearer worked for Solar for 26 years until his employment was terminated in 1992. While he was employed at Shearer, Shearer lived overseas and serviced a sales territory that included Libya, Jordan, Syria, Lebanon, Iraq, Iran and Saudi Arabia. When Shearer was terminated from Solar, he started Tejas Compressor Systems, Inc. and Tejas Procurement Services, Inc., headquartered in Conroe, Texas, in order to compete with his former employer.

Shearer obtained Solar's trade secret information and used that information to manufacture counterfeit Solar parts through Tejas. Shearer obtained this confidential trade secret information through at least three individuals, defendant William Robert Humes and defendant Jack Edward Nafus, as well as a third individual. Tejas, at Shearer's direction, paid each of these Solar employees to provide Solar drawings, plans and schematics that included confidential specifications describing the dimensions and manufacturing details of Solar parts. One of Shearer's main customers was an Iranian businessman who operated an oil and gas parts broker business in Uppsala, Sweden. This businessman placed millions of dollars of orders per year with Tejas and orders he placed were designed for oil field applications.

Tejas and a number of its employees became suspicious that the parts ordered by this Iranian national businessman were going to prohibited countries, such as Iran. One of Tejas's suppliers, in fact, refused to manufacture parts for Tejas because it determined, based on the type of gear sought to be manufactured, that it was a proprietary Solar part of a Solar turbine engine located in Iran. Two Solar employees, William Robert Humes, 59, and Jack Edward Nafus, 50, have also agreed to plead guilty under the Economic Espionage Act to stealing plans for Shearer, United States Attorney Paul Coggins said in a prepared statement. The third employee has not yet been charged.

"This is certainly shocking news for all of the honest and hardworking Solar Turbines employees who are committed to the success of our company," Solar Turbines President, Gary Stoup said. Stoup said his company sought a federal investigation after it found out its plans were being stolen. Company spokesperson, Wendy Swanson, said management received a tip about a year ago from a source she declined to reveal.

Three corporations founded by Shearer also agreed to plead guilty to conspiracy to steal trade secrets: Tejas Procurement Services, Tejas Compression Systems and Procurement Solutions International. Coggins said that Shearer instructed his employees to remove warnings stating the plans were owned by Solar before transferring them to third-party machine shops where counterfeits were made.

All the defendants pled guilty on 12/9/99 to conspiracy to steal trade secrets. The San Diego Union (12/14/99) reports that U. S. Attorney, Paul E. Coggins, stated that this was the first EEA case in which the defendants agreed to plead guilty to taking trade secret information

and actually converting the stolen information into manufactured products that were actually placed in the stream of interstate commerce. On June 15, 2000, United States District Judge Sidney A. Fitzwater sentenced.

Jack Shearer to 54 months imprisonment and ordered him to pay \$7,655,155.00 in restitution. William Robert Humes of Arlington, Texas was sentenced to 27 months imprisonment and ordered to pay \$3.8 million in restitution. Nafus was sentenced to 21 months imprisonment; 3 years supervised release; \$3,800,000.00 in restitution.

The three corporations founded by Jack Shearer--Tejas Procurement Services, Inc., Tejas Compressor Systems, Inc., and Procurement Solutions International, L.L.C.--pled guilty, by their duly appointed representative, and were each sentenced to five years probation and ordered, jointly and severally, to pay \$7,655,155.00 in restitution.

United States Attorney Paul E. Coggins stated: "This is the first EEA case in which the defendants pled guilty to taking trade secret information and actually converting the stolen information into manufactured products that were placed in the stream of commerce. The sentences handed down today (June 15, 2000) are among the longest sentences ever imposed in an Economic Espionage case."

18. [United States v. Costello, H-99-623 \(S. D. Texas 1999\).](#)

Charges filed 10/28/99. One count of theft of trade secrets. This EEA indictment involves an alleged EEA violation by an employee (Costello) relating to proprietary information involving oil and gas logs manufactured by Fina. Defendant pled guilty on 2/25/00 to theft of trade secrets. Defendant was sentenced on 6/5/00 to three years probation.

19. [United States v. Corgnati, CR-99-6268 \(Southern District of Florida 1999\).](#)

This indictment involves an alleged EEA violation relating to the theft and use of proprietary information relating to Motorola systems for 2-way radios. The Defendant pled guilty to one count of economic espionage and was sentenced on 6/12/00 to 5 years probation and \$120,000 in restitution.

20. [United States v. Say Lye Ow, CR-00-21110 \(San Jose California 3/29/00\).](#)

A federal grand jury returned an indictment on 3/29/00 against Say Lye Ow, a 29-year-old Malaysian national and former Intel engineer, who has been accused of stealing Intel trade secrets relating to Intel's upcoming "Itanium" processor before he left the company in 1998. A trial has been set for January 2001.

On December 11, 2001, The United States Attorney's Office for the Northern District of California announced that Say Lye Ow was sentenced today by U.S. District Judge Jeremy

Fogel in San Jose, California, on his guilty plea to a felony charge of copying a trade secret in violation of the Economic Espionage Act of 1996. Judge Fogel sentenced Mr. Ow to a term of imprisonment of 24 months and a term of supervised release of two years to follow the prison term. Mr. Ow was ordered to surrender himself to begin serving his prison sentence on January 15, 2002. Judge Fogel previously issued a preliminary order of forfeiture regarding the criminal forfeiture of Mr. Ow's interest in the computer system which he used to commit and facilitate the commission of the copying a trade secret offense. A final order of forfeiture will be issued in the near future. Mr. Ow, 31 a resident of Sunnyvale, California, and a citizen of Malaysia, was originally indicted by a federal Grand Jury on March 29, 2000. A superseding indictment was filed on March 14, 2001, which charged him with three counts of theft of trade secrets in violation of Title 18, United States Code, Sections 1832(a)(2) and (a)(3), one count of computer fraud in violation of Title 18, United States Code, Sections 1030(a)(4), and one count alleging the criminal forfeiture pursuant to Title 18, United States Code, Section 1834(a)(2). He pled guilty on September 14, 2001, to a superseding information charging him with copying of a trade secret in violation of Title 18, United States Code, Section 1832(a)(2) and admitted to the criminal forfeiture.

According to the superseding information and plea agreement, Mr. Ow copied without authorization computer files relating to the design and testing of the Merced microprocessor (now known as the Itanium microprocessor). At the time, Mr. Ow knew that the materials contained trade secrets belonging to Intel Corporation. He copied the trade secret information with intent to convert it to his own economic benefit by using it at his then new employment at Sun Microsystems. He also knew at the time that his act would injure Intel Corporation, in that he - as a former employee of Intel - possessed Intel's extremely valuable trade secret information without its knowledge. He also agreed that the information he copied was in fact a trade secret and that it was related to a product that was produced for and later placed in interstate and foreign commerce. The Itanium microprocessor was under joint development by Intel and Hewlett-Packard Co. since 1994 and was released earlier this year.

Mr. Ow also agreed to the criminal forfeiture of his interest in the computer system which was located at his residence and which he used to commit and facilitate the commission of the copying a trade secret offense.

Prior to imposing the two-year prison sentence, Judge Fogel stated that the key point in a case such as this is the gravity of what happens when people steal intellectual property of such enormous value.

U.S. Attorney David W. Shapiro said, "People and companies who steal intellectual property are thieves just as bank robbers are thieves. In this case, the Itanium microprocessor is an extremely valuable product that took Intel and HP years to develop. These cases should send the message throughout Silicon Valley and the Northern District that the U.S. Attorney's Office takes seriously the theft of intellectual property and will prosecute these cases to the full extent of the law."

The prosecution is the result of an investigation by the High Tech Squad of the San Jose Resident Agency of the Federal Bureau of Investigation and the Computer Hacking and Intellectual Property ("CHIP") Unit of the United States Attorney's Office. Ross W. Nadel, the Chief of the CHIP Unit, is the Assistant U.S. Attorney who prosecuted the case, with the assistance of Lauri Gomez. Sun Microsystems, the new employer to which Mr. Ow took the trade secret information, and Intel Corporation were fully cooperative in assisting the authorities in investigating and prosecuting this case.

This is the second case within a week in San Jose in which a defendant was sentenced to a term of imprisonment for a violation of the Economic Espionage Act. Last week, on December 4, 2001, Mihakel K. Chang was sentenced in a separate case to a term of imprisonment of 12 months on his guilty plea to a theft of trade secrets in violation of the Economic Espionage Act of 1996. A copy of the press release regarding the sentencing in that case is attached. These cases highlight the importance of investigations of and prosecutions for violations of the federal laws protecting intellectual property rights.

A copy of this press release and related court documents may be found on the U.S. Attorney's Office's website at www.usdoj.gov/usao/can (<http://www.usdoj.gov/usao/can>).

21. [United States v. Mark Everheart, CR-00-56 \(W.D. Pa. 2000\)](#).

This EEA indictment involved an alleged EEA violation relating to sales and pricing data from Werner Ladder by an employee (Everheart). Defendant pled guilty on 3/30/00 and was sentenced on 3/30/00 to 1 year probation, \$100 special assessment.

22. [United States v. Mikahel Chang and Daniel Park, CR-00-20203 \(N.D. California 2000\)](#).

This indictment involves an alleged EEA violation relating to a customer list/database involving Chang and a third-party buyer.

Mr. Change, 32, and Mr. Park, 33, both of San Jose, California were indicted by a federal grand jury on June 14, 2000. Both defendants were charged with one count of theft of a trade secret in violation of Title 18, United States Code, Sections 1832(a)(1) and (a)(3). Mr. Chang was charged with two counts of criminal forfeiture pursuant to Title 18, United States Code, Sections 1834(a)(1) and (a)(2). Mr. Park was charged with one count of criminal forfeiture pursuant to Title 18, United States Code, Section 1834(a)(2). Under the plea agreements, Mr. Chang pled guilty to all three counts and Mr. Park pled guilty to a superseding information charging the criminal copyright infringement violation.

In pleading guilty, Mr. Chang admitted to having received, possessed and without authorization appropriated stolen trade secret information belonging to Mr. Chang's former employer, Semi-Supply, Inc. of Livermore, California, knowing such information to have been stolen, obtained and converted without authorization, Specifically, Mr. Chang admitted to having received, possessed and appropriated without authorization customer and order information in databases relating to Semi Supply's sales.

In pleading guilty, Mr. Park admitted to having aided and abetted the willful infringement of a copyright for purposes of commercial advantages and private financial gain. Mr. Park admitted to having aided and abetted the willful infringement of a copyright by accessing a FoxPro database program, which he knew had been copied without authorization and which had been infringed for the purposes of commercial advantage and private financial gain. Specifically, Mr. Park admitted that the FoxPro database program was used to access the stolen trade secret information belonging to Semi Supply.

The sentencing of Mr. Chang is scheduled for July 10, 2001 at 9:00a.m. before Judge Fogel in San Jose. The maximum statutory penalty for this violation of the criminal copyright statute is 1 year imprisonment, and a fine of \$100,000, plus restitution if appropriate. Again, the actual sentence will be dictated by the Federal Sentencing Guidelines, which take into account a number of factors, and will be imposed in the discretion of the Court.

The prosecution is the result of an investigation by agents of the High Tech Squad of the Federal Bureau of Investigation which was overseen by the Computer Hacking and Intellectual Property ("CHIP") Unit of the U.S. Attorney's Office.

23. [United States v. Jolene Neat-Rector and Steven Snyder, CR-123-T-24C \(M.D. Fla. 2000\).](#)

Prior to August 20, 1999, Johene Hilda Neat-Rector ("Rector") obtained proprietary documents and data owned by R.P. Schorer, Inc. (RPS) from a friend(s) in Florida.

The proprietary information included gel formulas, fill formulas, sheer weights, and experimental production order (EPO) data.

RPS is a leading international manufacturer of drug, cosmetic and recreational product delivery systems. RPS's proprietary advanced drug delivery systems improve the efficacy of drugs by regulating their dosage, rate of absorption and place of release.

On or about August 20, 1999, Rector had a conversation with the Production Manager of Nelson Paint Ball, Inc., located in Kingsford, Michigan. Rector advised him that she had gelatin formula that she wanted to sell for \$50,000.00. Subsequent communications confirmed that Rector had 65 paint ball color formulas and 108 gelatin formulas from RPS.

Thereafter, Rector faxed several pages to Nelson Paint Ball, Inc. and Nelson Paint Inc. notified the FBI.

A sting operation ensued. On October 14, 1999, an undercover agent of the FBI met with Rector pretending to have been sent by Nelson Paint Ball. The meeting was videotaped. Rector turned over a maroon colored, three-ring binder containing machine maintenance instructions, paint ball and gel formulas and a list of sheer weights. The undercover FBI agent gave her a check in the amount of \$25,000.00.

Immediately after the exchange, the FBI notified Rector that the meeting had been a sting and Rector cooperated with the FBI and admitted that she received the notebook from a former RPS employee (Steven Michael Snyder) via the U.S. Mail.

Pursuant to a plea agreement, both Rector and Snyder have entered guilty pleas to a two-count indictment charging conspiracy to convey trade secrets and the theft of trade secrets. In the plea agreement, both Rector and Snyder admit that to gel formulas, fill formulas and EPOs are proprietary trade secrets of RPS.

The defendants face a maximum term of ten-year imprisonment and a fine up to \$250,000 for each offense.

Further details of the sentencing have been provided by the U.S. Attorney's Office in Tampa, Florida as reported by the United States Department of Justice.

The United States Attorney announced today that Jolene Hilda Neat Rector and Steven Michael Snyder were both sentenced Friday afternoon by District Court Judge James S. Moody, Jr., after having entered guilty pleas to a two count indictment charging them with conspiracy to convey trade secrets and the substantive offense of conveying trade secrets, a case of first impression in the Middle District of Florida. Rector was sentenced to 14 months confinement (seven months to be served in a community correctional center), two years supervised release, and a special assessment of \$200. A fine was waived in her case. She had entered her guilty pleas before Magistrate Judge Jenkins on March 13, 2001. Snyder was sentenced to 10 months confinement (five months to be served in a community correctional center), two years supervised release, and a special assessment of \$200. A fine was also waived in his case. He had entered his guilty pleas before Magistrate Judge Jenkins on March 2, 2001.

Rector, age 45, and Snyder, age 36, each were convicted of conspiring to convey trade secrets, in violation of 18 U.S.C. § 1832(a)(5), and conveying trade secrets, in violation of 18 U.S.C. §§ 1832(a)(2) and 2. Both offenses are crimes under the Economic Espionage Act of 1996 (EEA) and the prosecution of these offenses constitute the first ever prosecution under this statute in the Middle District of Florida, one of a growing number of prosecutions under this statute nation-wide since the statute was enacted in October of 1996. This case has national significance because it reinforces the impact Congress desired to make in limiting the damage industrial espionage causes United States companies, both here and abroad.

The facts, as agreed to by both defendants in their plea agreements with the United States, establish that at some time prior to August 20, 1999, the defendant, Jolene Hilda Neat Rector, obtained numerous pieces of proprietary information owned by R.P. Scherer, Inc. (RPS) from a friend(s) in Florida. This information included gel formulas, fill formulas, shell weights, and experimental production order (EPO) data. This information was known by the defendant to be proprietary information and trade secrets of RPS. RPS is a leading international developer and manufacturer of drug, supplement, cosmetic and recreational product delivery systems. RPS's proprietary advanced drug delivery systems improve the efficacy of drugs by regulating their dosage, rate of absorption and place of release. RPS customers include global and regional manufacturers of prescription and over-the-counter pharmaceutical products, nutritional supplements, cosmetics and recreational products such as paint balls. RPS products are produced for and placed in interstate and foreign commerce.

Both Rector and Snyder admitted that the gel formulas, fill formulas, and EPOs were

proprietary trade secrets of RPS, developed by them and used by them in the production of drug, nutrient supplement and paint ball delivery systems (capsules) as well as the fill material inside the capsules.

The investigation of this case was accomplished through the collaborative efforts of Special Agents of the Federal Bureau of Investigation in Michigan, Nevada, and here in the Middle District of Florida. This case also demonstrates a situation where a competitor corporation (NPB) actively cooperated with federal authorities and the victim corporation (RPS). Without the assistance of this competitor corporation, the successful prosecution of this case would not have been possible.

The case was prosecuted by Assistant United States Attorney Donald L. Hansen, Computer Technology Crimes Coordinator for the Tampa Division of the United States Attorney's Office.

24. United States v. Peter Morch (N.D. Calif. November 21, 2000).

Peter Morch, a resident of San Francisco and a citizen of Canada and Denmark, was arrested on November 21, 2000 and charged with the theft of trade secrets in violation of 18 U.S.C. § 1832.

According to an affidavit filed in support of the criminal complaint, Morch recently resigned from his position as a software engineer at Cisco Systems in Petaluma, California. While at Cisco, Morch was a team leader for a research and development project pertaining to voice-over and optical networking. The day before his final date of employment at Cisco, Morch allegedly burned onto compact discs ("CDs") numerous proprietary documents, including but not limited to Cisco project ideas, general descriptions, requirements, specifications, limitations of design, and special procedures relating to voice-over and optical networking software product(s). Shortly thereafter, Mr. Morch started working at Calix Networks, a potential competitor with Cisco.

The prosecution is the result of an investigation by special agents of the Federal Bureau of Investigation and the Computer Hacking and Intellectual Property Unit of the United States Attorney's Office.

25. United States v. Fausto Estrada (S.D.N.Y. March 21, 2001).

Fausto Estrada was a contract food services employee working at MasterCard's headquarters in Purchase, New York. Estrada worked for Flik International Corp., a catering company in Rye Brook, New York. The company catered, inter alia, Mastercard's private lunches in the Mastercard boardroom. Estrada worked at Mastercard's offices on January 29, 2001 and

March 7, 2001 (among other dates). Estrada's court-appointed attorney told the press that Estrada only work at MasterCard's headquarters a total of a week on various dates.

According to the Complaint, Estrada offered to sell Visa proprietary information that he had stole from MasterCard. In February, 2001, Estrada -- using the alias "Cagliostro" -- mailed a package of information stolen from MasterCard to Visa's offices in California. The package allegedly contained a letter demanding \$100,000 for MasterCard secrets for the years 1999 and 2000 and another \$1000,000 for what Estrada promised was "a lot of valuable information for this year." Estrada apparently planned to tell Visa about a confidential business alliance proposal between Mastercard and a large U.S. entertainment corporation according to published reports in the New York Times.

A sting operation was conducted by the FBI's Computer Intrusion and Intellectual Property Squad. An FBI agent posed as a Visa representative and negotiated the purchase of the MasterCard documents in Estrada's possession. These negotiations culminated in a covert meeting in which an undercover FBI agent met with Estrada in a hotel room to exchange money for the stolen MasterCard documents. Estrada reportedly bragged to an undercover FBI agent, posing as a Visa executive: "I even know where they [MasterCard executives] eat."

On March 21, 2001, in a five-count Complaint, Estrada was charged with the theft of trade secrets a violation of 18 U.S.C. § 1832, mail fraud and interstate transportation of stolen property. Prosecutors portrayed Estrada as a man cloaking his identity as an international spy. However, Estrada's court-appointed lawyer (Philip Weinstein) told the Judge: "This was hardly the most sophisticated scheme in the world."

26. [United States v. Kurtis Kenneth Cullen and Bruce Zak \(W.D. KY April 18, 2001\)](#).

A federal grand jury in the Western District of Kentucky returned an indictment charging Kurtis Kenneth Cullen (age 31) and Bruce Zak with conspiracy to steal trade secrets, attempted theft of trade secrets, and wire fraud. The indictment alleges that between January 21, 2001 and January 27, 2001, Cullen and Zak, in concert with others, engaged in a scheme to buy a proprietary source code from an employee of ZirMed.com, a Louisville company that has developed a computer application for processing health care benefit claim forms. The indictment further alleges that Cullen contacted a ZirMed.com employee by telephone and offered to pay \$10,000 for a clear text version of the source code. The arraignment was set for April 24, 2001.

27. [United States v. Junsheng Wang and Bell Imaging Technology Corp. \(N.D. Calif. April 19, 2001\)](#).

Wang, age 53, of Fremont, and Bell Imaging, a California corporation based in Fremont, were charged in a criminal indictment filed in federal court on April 19, 2001. Wang was charged with theft of trade secrets in violation of Title 18, US Code, Section 1832(a)(1), and Bell Imaging was charged with copying of trade secrets in violation of Title 18, US Code, Section 1832(a)(2). A related company, Belson Imaging Technology Company Limited, a joint venture based in the People's Republic of China, was also charged with copying trade secrets; the charge remains pending.

On April 26, 2001, the United States Attorney's Office for the Northern District of California announced that both Junsheng Wang and Bell Imaging Technology Corporation pled guilty to the theft and copying of trade secrets of Acuson Corporation. The sentencing of Wang and Bell Imaging are scheduled for October 23, 2001, in San Jose, California. The maximum statutory penalty for each count in violation of Title 18, US Code, Section 1832, is 10 years and a fine of \$250,000 for an individual and \$5 million for a corporation, plus restitution if appropriate.

In pleading guilty, Wang admitted that prior to August 24, 2000, that he took without authorization and copied for Bell Imaging a document providing the architecture for the *Sequoia* ultrasound machine that contained the trade secrets of Acuson Corporation.

According to Wang's plea agreement, he had been able to obtain access to the Acuson trade secret materials because his wife was employed as an engineer at that company and because she had brought that document home with her. After he had copied the document, he took it with him on business trips to the People's Republic of China on business trips for Bell Imaging. According to Bell Imaging's plea agreement, it is a California corporation involved in the manufacture and distribution of ultrasound transducers. Bell Imaging also admitted that it has been a partner with Henson Medical Imaging Company, a Chinese company, in a joint venture (Belson Imaging Technology Company Limited), the remaining defendant in the case.

Mr. Wang was arrested carrying the Acuson trade secret documents at San Francisco International Airport as he was about to board a flight to Shanghai, P.R.C. in August of 2000.

The sentencing of Mr. Wang and Bell Imaging are scheduled for October 23, 2001 before Judge Jeremy Fogel in San Francisco. The prosecution was the result of a joint investigation by the Federal Bureau of Investigation (FBI) and agents of the United States Custom Service.

The United States Department of Justice reports (April 26, 2001) that Junsheng Wang and Bell Imaging Technology Corporation pled guilty today to theft and copying of the trade secrets of Acuson Corporation.

Mr. Wang, age 53, of Fremont, and Bell Imaging, a California corporation based in Fremont, were charged in a criminal information filed in federal court on April 19, 2001. Mr. Wang was charged with theft of trade secrets in violation of Title 18, United States Code, Section 1832(a)(1), and Bell Imaging was charged with copying of trade secrets in violation of Title 18, United States Code, Section 1832(a)(2). A related company, Belson Imaging Technology Company Limited, a joint venture based in the People's Republic of China, was also charged in the information with copying trade secrets, and that charge remains pending.

In pleading guilty, Mr. Wang and Bell Imaging admitted that prior to August 24, 2000, Mr. Wang took without authorization and copied for Bell Imaging a document providing the architecture for the Sequoia ultrasound machine that contained the trade secrets of Acuson Corporation. According to Mr. Wang's plea agreement, he had been able to obtain access to the Acuson trade secret materials because his wife was employed as an engineer at that company and because she had brought that document into their home. After Mr. Wang had copied the document, he took it with him in the year 2000 on business trips to the People's Republic of China for Bell Imaging. According to Bell Imaging's plea agreement, it is a California corporation involved in the manufacture and distribution of ultrasound transducers, and has been a partner with Henson Medical Imaging Company, a Chinese company, in Belson Imaging Technology Company Limited, the final defendant in this case. Mr. Wang was arrested carrying the Acuson trade secret documents in San Francisco International Airport as he was about to board a flight for Shanghai, P.R.C., in August of 2000.

The sentencing of Mr. Wang and Bell Imaging are scheduled for October 23, 2001, before Judge Jeremy Fogel in San Jose. The maximum statutory penalty for each count in violation of Title 18, United States Code, Section 1832 is 10 years and a fine of \$250,000 for an individual and \$5 million for a corporation, plus restitution if appropriate. However, the actual sentences will be dictated by the Federal Sentencing Guidelines, which take into account a number of factors, and will be imposed in the discretion of the Court.

The prosecutions are the result of an investigation by agents of the Federal Bureau of Investigation with cooperation from agents of the United States Customs Service. Joseph E. Sullivan is the Assistant U.S. Attorney who prosecuted the case with the assistance of Lauri Gomez.

A copy of this press release and key court documents filed in the case may also be found on the U.S. Attorney's Office's website at www.usaondca.com (<http://www.usaondca.com/>).

28. **United States v. Hai Lin, Kai Xu, Yong-Qing Cheng (May 3, 2001)/United States v. ComTriad et. al. (D.N.J. May 31, 2001).**

Two Lucent scientists (Hai Lin and Kai Xu) who had been on the technical staff of Lucent's Murray Hill's headquarters--and former distinguished members of the Lucent development team for the PathStar Access Server-- and a third individual (Yong-Qing Cheng) who worked at Village Networks, an optical networking vendor (and consultant on the PathStar project) were arrested on May 3, 2001 and charged with violating the Economic Espionage Act of 1996 and conspiracy to commit wire fraud. The U.S. Assistant Attorney strenuously argued that all three men should be withheld without bail because none of the three men are U.S. citizens and there is a risk of flight to China where all three men have business interests. However, according to published press reports, bail was set on May 14, 2001 in the amount of \$900,000 for each defendant.

Court filings by the FBI outline a trail of electronic transmissions including a boast by the suspects that their joint venture with the Chinese company would become "the Cisco of China" by selling a copy of Lucent's product there. According to published reports, a substantial amount of the source code for Lucent's crown jewel--the PathStar data and voice transmission system was sent to the trio's Chinese partner, Datang Telecom Technology Co. Ltd. of Beijing. The suspects incorporated as "ComTriad" and then formed a partnership controlled by Datang called DTNET in February, 2001, which was funded with \$1.2 million from Datang according to the FBI criminal complaint. ComTriad calls its product CLX-1000 but there are references to the Lucent PathStar system. According to its website, Datang was founded in 1998 by the China Academy of Telecommunications Technology (a part of the Ministry of Posts and Telecommunications that runs the Chinese Post Office) and 12 unidentified Chinese companies. According to published reports, Datang has been a reseller of Lucent switching equipment for wireless systems.

An indictment was returned by a grand jury in Newark four weeks after the defendants were arrested on a criminal complaint charging conspiracy to commit wire fraud. The indictment charges each of the defendants with one count of conspiracy to steal trade secrets and to possess stolen trade secrets in violation of 18 U.S.C. Section 18329a)(5). The indictment closely mirrors the allegations in the criminal complaint describing how the trio of defendants ("ComTriad")-- via email and a password-protected web site-- conspired to transfer "the source code, software and entire design" for the PathStar server to China in concert with the trio's Chinese joint venture partner Datang.

The trio--Cheng, Lin and Xu---founded ComTriad Technologies, Inc. as a New Jersey high-tech startup company in January 2000 purportedly to develop products integrating the transmission and reception of voice and data over the Internet. However, the trio secretly entered into a joint venture arrangement with Datang. Datang funded the start-up with \$1.2 million in return for a substantial equity interest in ComTriad. To cover up their connection with Datang, the trio of defendants used a commercial post office box to receive mail.

Bail has been set at \$900,000 for each defendant and the release of each defendant is conditioned upon residence confinement with electronic monitoring.

The US Attorney's Office in New Jersey reports that a federal grand jury returned a new indictment against three men - two of them former employees of Lucent Technologies - for stealing trade secrets from Lucent for transfer to a joint venture with a Chinese telecommunications company, U.S. Attorney Christopher J. Christie announced.

The Superseding Indictment adds, in Count Two through Count Fifteen, allegations of possession of trade secrets stolen from Lucent; and, in Count Sixteen through Count Twenty-Four, allegations of wire fraud.

The original one-count Indictment charged conspiracy to steal trade secrets and to possess stolen trade secrets. It was returned on May 31, 2001, and charged Hai Lin and Kai Xu - both former Distinguished Members of the Lucent staff developing the PathStar Access Server - and Yong-Qing Cheng, who served as a Lucent consultant on the PathStar project.

Lin, Xu and Cheng are scheduled to be arraigned on the new Indictment on Monday, April 15, 2002 at 9:30, before U.S. District Judge William H. Walls. Each of the defendants are currently free on bail.

A trial for the defendants is scheduled to begin September 24, 2002. Lin, 30, is of Scotch Plains; Xu, 33, is of Somerset, and Cheng, 37, is of East Brunswick. All three are legal U.S. resident aliens from China.

Count One carries a maximum penalty of 10 years in prison and a \$250,000 fine. Each of the counts of possession of stolen trade secrets carries a maximum penalty of 10 years in prison and a \$250,000 fine. The wire fraud counts each carries a maximum penalty of five years in prison and a \$250,000 fine.

The Superseding Indictment, like the original Indictment, describes how the defendants, via e-mail, a password-protected Web site and visits to China, conspired to steal and transfer the software and hardware of the PathStar Access Server to a joint venture with Datang Telecom Technology Co. of Beijing, according to Assistant U.S. Attorney Scott S. Christie.

According to the Superseding Indictment, the PathStar Access Server was a sophisticated computer that facilitated the transmission of voice communications over the Internet. It converted analog voice signals to and from Internet-recognized transmission units ("IP packets"), merged voice and data IP packets, and handled delivery and routing of these

merged IP packets over the Internet while, at the same time, providing call waiting, speed dialing, conference calling and dozens of other telephony features.

As the Superseding Indictment alleges, Lin, Xu and Cheng founded ComTriad Technologies, Inc., a New Jersey high-tech startup, in January 2000, purportedly to develop products integrating the transmission and reception of voice and data over the Internet.

Among new allegations raised in the Superseding Indictment:

* that the defendants had attempted to obtain private financing for ComTriad through a venture capital consultant to manufacture and market its own modified version of the PathStar server based on the stolen trade secrets.

In April 2000, Lin, Xu and Cheng sought the venture capital for the product they called the CLX-1000. However, when the consultant insisted upon a demonstration and review of the CLX-1000 prototype and for related technical documents, Lin, Xu and Cheng allegedly ceased contact with this individual to avoid disclosing the theft of PathStar components from Lucent. In July 2000, the defendants then turned to Datang and proposed that Datang provide venture capital for an ownership interest in ComTriad and that they create a joint venture in Beijing for the development of products based upon the CLX-1000.

* that, in early September 2000, Lin, Xu and Cheng demonstrated their CLX-1000 prototype for representatives of Datang in the basement of Lin's home.

By late December 2000, Lin Xu and Cheng received an investment of \$500,000 from Datang and had formally agreed with Datang to form the joint venture in Beijing, to which the defendants agreed to contribute the stolen PathStar technology incorporated in the CLX-1000.

Beginning in early January 2001, soon after the business relationship between ComTriad and Datang had been formalized, Lin, Xu and Cheng allegedly attempted to distance themselves from ComTriad and obscure their connection to the company to avoid disclosure of their theft and possession of the PathStar components and proprietary technical documents.

The defendants did this, according to the charges, by removing their names from the publically-filed ComTriad articles of incorporation and obtaining a post office box as the new mailing address for ComTriad; Cheng removed his name from an Internet registry record linked to the password-protected ComTriad Internet Web site - www.comtriad.com(<http://www.comtriad.com/>) - and Lin and Xu began using ComTriad electronic mail addresses that did not identify them by name and obtained cell phones in their wives names to use for ComTriad business. Lin and Xu also assumed the aliases Howard Lin and Roy Xu when communicating with the public regarding ComTriad business, going so far as to obtain business cards in these aliases, according to the charges.

In mid-February 2001, Lin, Xu and a co-conspirator began the transfer of the stolen PathStar technology to the joint venture in Beijing with portions of the stolen and modified PathStar software. In late April 2001, Lin and this co-conspirator electronically transferred to China more of the stolen and modified PathStar software.

By early March 2001, Lin, Xu and Cheng had allegedly stored several versions of the stolen and modified PathStar software on their password-protected ComTriad Internet Web site, www.comtriad.com (<http://www.comtriad.com/>). FBI agents obtained the contents of this Web site with a search warrant. On May 3, 2001, the day the defendants were arrested and their homes were searched, FBI agents seized large quantities of the component parts of the PathStar Access Server, both software and hardware, as well as schematic drawings and other technical documents related to the PathStar Access Server marked "proprietary" and "confidential." Among other things, the agents seized a modified PathStar machine from Lin's basement.

Among other new details appearing in Count One, which alleges that the defendants conspired to steal trade secrets from Lucent and to possess stolen trade secrets:

* victims of the trade secret theft are not only Lucent, but other companies that licensed portions of their software to Lucent for use in the PathStar Access Server and sold Lucent custom-designed circuit boards for use in the PathStar Access Server, including:

- Telenetworks, a business unit of Next Level Communications, headquartered in Rohnert Park, Ca.

- NetPlane Systems, Inc. (formerly Harris & Jeffries, Inc.), a wholly-owned subsidiary of Mindspeed Technologies, Inc., headquartered in Dedham, Mass.

- Hughes Software Systems, Ltd., a division of Hughes Network Systems, Inc., headquartered in Gurgaon, India; and

- ZiaTech Corporation, a wholly-owned subsidiary of Intel Corporation, headquartered in San Luis Obispo, Ca.

* that before approaching Datang, Lin, Xu and Cheng first sought financing through a venture capital consultant.

* Lin and Xu began transferring the PathStar software to China in mid-February 2001.

* a large percentage of the software files stored on the ComTriad Web site was identical to or modified from PathStar software.

Count One of the Superseding Indictment also sets forth in greater detail the trade secrets of the PathStar server that were seized during searches at the defendants homes and Village Networks, Cheng's employer in Eatontown.

Counts Two through Fifteen of the new Indictment allege that Lin, Xu and Cheng possessed specific PathStar components and proprietary technical documents on the day of their arrest.

Counts Sixteen through Twenty Four allege that Lin, Xu and Cheng also victimized Lucent by committing wire fraud. The fraud scheme is alleged to be that Lin and Xu deprived Lucent of their loyalty and honest services by stealing trade secrets and by owning and participating in ComTriad, a competitor, while employed at Lucent. The scheme was carried out by Lin, Xu and Cheng sending e-mail among themselves and to China.

Despite Indictment, every defendant is presumed innocent, unless and until found guilty beyond a reasonable doubt following a trial at which the defendant has all of the trial rights guaranteed by the U.S. Constitution and federal law.

Under U.S. Sentencing Guidelines, actual prison sentences are, upon conviction, determined under a formula that takes into account the severity and characteristics of an offense and the criminal histories, if any, of the defendants. Parole has been abolished in the federal system. Under Sentencing Guidelines, defendants who are given custodial terms must serve nearly all that time.

U.S. Attorney Christie credited Special Agents of the FBI, under the direction of Special Agent in Charge Phillip W. Thomas, of the FBI's Newark Office; and Special Agents of the Defense Criminal Investigative Service, under the direction of James Murawski, Resident Agent in Charge, for their skill and persistence in investigating the case.

The government is represented in the case by Assistant U.S. Attorney Christie of the U.S. Attorney's Office Fraud and Public Protection Division, and by Special Assistant U.S. Attorney Jennifer Martin, a trial attorney with the Computer Crime and Intellectual Property Section of the Department of Justice.

29. [United States v. Takashi Okamoto, Hiroaki Serizwa, \(N.D. Ohio, May 8, 2001\)](#).

Two Japanese researchers were charged with violating Sections 1831(a)(1), 1831(a)(2) and Section 1832 of the Economic Espionage Act of 1996. This is the first indictment prosecuted under Section 1831 of the EEA. Hiroaki Serizwa was arrested in Kansa City, Kansas. According to the indictment, Defendant Takashi Okamoto was employed by the

Lerner Research Institute (LRI) of the Cleveland Clinic Foundation (CCF) from January 1997 to July 26, 1999. Hiroaki Serizawa met Okamoto in the mid-1990s and the two became close friends. Serizawa was employed by the Kansas University Medical Center in Kansas City, Kansas.

According to the indictment, Okamoto met with a representative from The Institute of Physical and Chemical Research (Riken), a quasi-public corporation located in Saitama-ken, Japan. Riken (according to the indictment) receives 94 per cent of its operational funding from the Japanese Ministry of Sciences and Technology of the government of Japan. In 1997, Riken formed the Brain Sciences Institute (BSI) to conduct research regarding the causes and treatment of Alzheimer's disease.

Okamoto was engaged in research at the LRI/CCF in Lab 164 where experiments were conducted and research was being undertaken to understand how three mutated genes (a mutant APP gene located at chromosome 21 near the beta amyloid fragment, and two other specific genes known as Presenilin-1 and Presenilin-2) caused inherited, early-onset type of Alzheimer's disease. To study the inherited, early-onset form of Alzheimer's disease, Okamoto and the researchers in Lab 164 developed "designer genes" which are called "reagents." Almost \$2 million in funding to conduct this research came from three sources—the CCF, the National Institutes of Health (NIH) and the Prentiss Foundation.

According to the indictment, in April, 1999 (while still employed by LRI/CCF, Okamoto accepted employment at Riken as a neuroscience researcher with employment at RIKEN to commence in the Fall of 1999. On the evening of July 8, 1999, it is alleged that Okamoto and his (unindicted) co-conspirator Dr. A misappropriated DNA and cell in reagents and constructs from Lab 164 and in the early morning hours of July 9, 1999 "destroyed and sabotaged" the remaining DNA and cell line reagents and constructs in Lab 164.

On July 10, 1999, Okamoto stored four boxes containing the stolen DNA and cell line reagents at the Cleveland, Ohio home of Dr. B, a colleague of Okamoto. On July 12, 1999, Okamoto retrieved the four boxes of stolen DNA and cell line reagents from Dr. B's home and sent them by private interstate carrier to defendant Serizawa in Kansas City.

On July 26, 1999, Okamoto resigned from his research position at CCF. On August 3, 1999, Okamoto commenced his employment with Riken in Japan. On August 10, 1999, Okamoto returned to the United States from Japan. On August 16, 1999, Okamoto retrieved the stolen DNA and cell reagents and constructs at Serizawa's laboratory at KUMC, and on August 17, 1999 Okamoto departed the United States with the stolen DNA and cell line constructs and reagents.

The issue of ownership rights in scientific research will be at issue in this litigation. However, the most serious allegation is set forth in Paragraph 30 of the indictment as follows: "On or about August 16, 1999, defendants Okamoto and Serizawa filled small laboratory vials with tap water and made meaningless markings on the labels of the vials, and defendant Okamoto instructed defendant Serizawa to provide the worthless vials to officials of the CCF in the event that they came looking for the missing DNA and cell line reagents."

The indictment alleges, *inter alia*, that Okamoto and Serizawa "knowingly and with the intent to benefit RIKEN, an instrumentality of the government of Japan, without authorization, did steal, appropriate, take, carry away, conceal, and obtain by fraud, artifice and deception, certain trade secrets that were the property of CCF, specifically ten DNA and cell line reagents developed through the efforts and research of researchers employed and funded by the CCF and by a grant from the National Institutes of Health...All in violation of Title 18, United States Code, Sections 1831(a)(1) and 2."

The Associated Press reported that on May 1, 2002, Hiroaki Serizawa (age 40), a researcher at the University of Kansas Medical Center, pled guilty to providing false information to the FBI in September 1999 about his relationship with Takashi Okamoto.

Mr. Serizawa admitted that he lied when he denied knowing that Okamoto has taken a position with Riken, a Japanese government-sponsored research facility. Mr. Serizawa also "underestimated the number of vials that were taken."

The plea agreement eliminates the more serious charges under the Economic Espionage Act. The trial was scheduled to begin May 13, 2002. Robert Wallace, a senior trial attorney for the U.S. Department of Justice, said the government entered into the plea agreement in order to get Serizawa's assistance in the case against Okamoto.

"Dr. Serizawa was deceived and manipulated by Dr. Okamoto" according to Serizawa's attorneys.

The FBI has estimated the missing materials cost the Cleveland Clinic about \$2 million. The alleged theft and destruction of genetic materials has now led to the termination of the Cleveland Clinic's Alzheimer's studies.

No trial date has been set for Okamoto. Federal officials are continuing to pursue Okamoto's extradition from Japan.

The maximum penalty for providing false information is five years in prison and a \$250,000 fine. As part of the deal, the Immigration and Naturalization Service agreed not to deport Serizawa.

30. [United States v. Nicholas Daddona, Case No. 3:01CR122AVC \(D. Conn. June 6, 2001\)](#).

A federal grand jury sitting in Hartford, Connecticut returned a three count indictment against Nicholas Daddona (age 44) charging him with two counts of theft of trade secrets and one count of unauthorized access of a computer.

According to the indictment, Daddona, while employed by Fabricated Metal Products, Inc. ("FMP"), located in Naugatuck, began secretly working for a competitor, Eyelet Toolmakers, Inc. of Watertown, without FMP's knowledge. FMP is engaged in the business of custom designing and producing deep drawn metal products including ammunition components, sprinkler parts and fuel filter cans. While working simultaneously for both companies, the indictment charges that Daddona stole and duplicated FMP's unique engineering plans for the development and manufacture of a large transfer press and certain tooling plans and delivered them to Eyelet (and another company working for Eyelet). The plans were stored on FMP's computers.

On March 12, 2002, the United States Attorney for the District of Connecticut (John A Danaher III) announced in a press release that reported that Nicholas Daddona, age 45, of 22 Catering Road, Wolcott, Connecticut, was sentenced yesterday in United States District Court in Hartford to 5 months of home confinement with electronic monitoring to be followed by 36 months of probation. Daddona was convicted of stealing trade secrets from his former employer, Fabricated Metal Products, Inc. ("FMP"), located in Naugatuck. The Honorable Alfred V. Covello, Chief United States District Court Judge, also ordered Daddona to pay a fine in the amount of \$4,000.00 and a special assessment in the amount of \$100.00. Daddona previously agreed to pay restitution in the amount of \$10,000 to the victim.

On September 7, 2001, Daddona entered a plea of guilty to one count of theft of trade secrets. The charge arose out of his former employment with Fabricated Metal Products. While employed by FMP, Daddona began working for a competitor, Eyelet Toolmakers, Inc., of

Watertown, without FMP's knowledge. Daddona admitted that he stole unique engineering plans stored on FMP's computers and delivered them to Eyelet and associated entities.

The case was investigated by Special Agents of the Federal Bureau of Investigation and was prosecuted by Assistant United States Attorneys Maria A. Kahn and Joseph Metcalfe, Trial Attorney, Department of Justice, Computer Crimes and Intellectual Property Division.

31. [United States v. Xingkun Wu, Case No. _____ \(Rochester, NY July 31, 2001\).](#)

The United States Department of Justice reports that on July 31, 2001 Special Agent in Charge (SAC) Peter J. Ahearn, Buffalo Division, Federal Bureau of Investigation (FBI), announced the filing of a federal criminal complaint and the issuance of a federal arrest warrant against Mr. Xingkun Wu, age 40, of Los Angeles, California. The complaint and arrest warrant were the result of an investigation conducted by FBI Special Agents assigned to the Elmira, New York, Resident Agency, with the assistance of the New York State Police, the FBI's Los Angeles Division, and Corning Incorporated.

The Criminal Complaint, which was issued July 30, 2001, charged Wu, a former employee of Corning Incorporated, with violations of Title 18, United States Code (USC), Section 1832, which pertains to Theft of Trade Secrets. The Criminal Complaint alleges that on or about March 10, 2000, and May 4, 2000, in the Western District of New York, Wu knowingly attempted to convert a trade secret to the economic benefit of someone other than its owner (Corning Incorporated), knowing that the offense would injure Corning Incorporated as the owner of the trade secret. Investigation by the Los Angeles Division of the FBI has developed information that Wu may have returned to his native country, China.

The federal criminal complaint and arrest warrant were issued by the Honorable Jonathon W. Feldman, United States Magistrate Judge, Rochester, New York. Assistant United States Attorney Richard Resnick (United States Attorney's Office for the Western District of New York) will prosecute this matter.

The prosecution is the result of an investigation by special agents of the FBI. Michael Malecekis the Assistant U.S. Attorney who is prosecuting the case with the assistance of Joseph Keefe.

The maximum statutory penalty for violations of both 18 U.S.C. § 1832 and 18 U.S.C. 2314 is 10 years in prison and a fine of \$250,000.

32. United States v. Thomas Kissane, Case No. _____ (SDNY February, 2002).

The United States Attorney for the Southern District of New York, and Barry W. Mawn, the Assistant Director in Charge of the FBI's New York Office, announced that Timothy Kissane was arrested and charged today in Manhattan federal court with theft of a trade secret in connection with his prior employment at System Management Arts Incorporated ("Smarts"), a software company based in White Plains, New York.

According to the Complaint, Kissane worked as a release engineer at Smarts, and was responsible for the packaging of multiple components of the Smarts software package, including its source code. "Source code" is the underlying computer program that is used to create a software package that can be sold to customers. If a competitor obtained the source code for a software program, it could convert some or all of its features into its own software.

As stated in the Complaint, Smarts developed and sells a custom software program called "InCharge", which monitors large computer networks, and identifies operational problems on the network. Smarts sells "InCharge" to large telecommunications companies around the country and abroad. "InCharge" is a proprietary computer program, and its source code is a guarded secret. According to the Complaint, on February 21, 2000, Kissane signed an employment contract in which he agreed to "forever keep secret" confidential Smarts information that he had access to, including "software codes."

The Complaint charges that on November 28, 2001, Kissane's employment at Smarts was terminated. Several weeks later, two of SMARTS' competitors received email messages from a "Joe Friday" at a Yahoo! email account, offering Smarts' source code for sale. According to the Complaint, one of the email messages stated that the sender possessed the "cvs repository of Smarts InCharge code, from 11/20/01 as well as custom code for specific bug fixes and customer-requested enhancements." The competitors brought these email messages to the attention of Smarts.

According to the Complaint, connections to the Yahoo! email account from which the "Joe Friday" email messages were sent was opened at the White Plains Library, White Plains, New York. As the Complaint charged, this Yahoo! account was then accessed approximately thirty-three additional times in December 2001 from a Verizon DHL Internet account located at the Lavallette, New Jersey address where Kissane had previously informed Smarts that he would be living.

Kissane, 41, is a resident of Lavallette, New Jersey.

Kissane was presented before United States Magistrate Judge James C. Francis, IV today, and released on a \$100,000 personal bond and strict pretrial supervision.

The charge of theft of a secret trade in the Complaint carries a maximum possible sentence of 10 years in prison and a fine of \$250,000 or twice the gross gain or loss resulting from the crime.

Mr. Comey praised the FBI's Computer Hacking and Intellectual Property Squad for its outstanding efforts of this case. He thanked Smarts for its cooperation during the investigation.

Assistant United States Attorney Robert R. Strang is in charge of the prosecution.

33. United States of America v. Tse Thow Sun, Case No. _____ (Monterey, California, April 11, 2002).

According to the Monterey County Herald (April 11, 2002), a Singapore national, Tse Thow Sun (age 31) was arrested in an FBI sting operation on or about April 11, 2002 culminating a month-long investigation which began when an unidentified man (and woman) called the President (Dennis Dracup) of Monterey-based Language Line Services, Inc., the nation's largest translation business. The unidentified man offered to sell certain trade secret information of Online Interpreters (located in Chicago) including customer lists and detailed billing information. Online Interpreters is a direct competitor of Language Line Services.

Dennis Dracup reported the telephone call to outside counsel (Dan Archer) who reported the call to the FBI in San Francisco. Cooperating with the FBI, Dracup met with the unidentified man at a hotel on March 24 and the man -- calling himself "John"-- turned over a sample of the trade secret materials for \$5,000 (he asked for \$30,000 for the sample but the FBI told Dracup to pay only \$5,000). The materials included an online profit-and-loss statement, billing summaries, call counts and an E-mail message discussing Language Line.

After the March 24 meeting, Dennis Dracup visited Online's headquarters in Park Ridge, Illinois (Language Line Services was already engaged in negotiations to buy Online Interpreters) and Dracup was able to identify from company photos (and FBI surveillance photos) that "John" was Tse Thow Sun, a computer specialist for Online Interpreters.

Peter S. Speciale, Vice President of Online's Monterey offices was quoted as saying that Mr. Sun was "a very savvy person" -- with an Internet pornography site -- with the capability of incapacitating Online's operations.

After the \$5,000 payment was made, Dracup agreed to meet again with Sun to receive additional proprietary information in exchange for \$3 million. Sun wanted cash or a wire transfer, but Dracup (again coached by the FBI) insisted on a cashier's check. The second meeting was scheduled on March 29, 2002 at the same hotel.

Shortly before the March 29 meeting, Sun quit his job at Online (telling co-workers that he had taken a new job in Washington D.C.) and he flew to California carrying a laptop computer allegedly filled with trade secret information taken from Online Interpreters. At the second hotel meeting, Tse Thow Sun, was arrested by the FBI.

Mr. Sun has been charged with theft of trade secrets in violation of the EEA and interstate transportation of stolen property.

The United States Attorney's Office for the Northern District of California announced that a federal grand jury returned an indictment this afternoon against Tse Thow Sun, age 31, and a resident of Chicago, Il, for theft of trade secrets and interstate transportation of stolen property.

The indictment against Tse Thow Sun, a Singapore national, alleges one count of theft of trade secrets in violation of 18 U.S.C. § 1832 and one count of interstate transportation of stolen property in violation of 18 U.S.C. § 2314. Mr. Sun was arrested on March 29, 2002, as the culmination of a sting operation conducted by the FBI based on a criminal complaint filed with the Court.

An affidavit filed by an FBI agent in the case alleges that Mr. Sun contacted the president of Language Line Services in Monterey, California in March 2002 and offered to sell to him proprietary information of Language Line Service's chief competitor, Online Interpreters, for \$3 million. Attorneys for Language Line Services promptly contacted the FBI. With the continuing assistance of individuals from both companies, the FBI arranged a meeting on March 24, 2002. At that meeting, Mr. Sun provided certain documents to prove that he had access to the trade secrets of Online Interpreters. In return, Mr. Sun received \$5,000. A subsequent meeting was arranged to deliver the remaining trade secrets on March 29, 2002, in exchange for \$3 million. Following this meeting, Mr. Sun was arrested.

Mr. Sun was ordered by a federal magistrate to remain in custody. His next court appearance is for arraignment on April 12, 2002, at 9:30 a.m. before Magistrate Judge Larson.

The United States Attorney's Office for the Northern District of California also provided the following information in a press release.

The United States Attorney's Office for the Northern District of California announced that a federal grand jury returned an indictment against Tse Thow Sun, age 31, and a resident of Chicago, Il, for theft of trade secrets and interstate transportation of stolen property.

The indictment against Tse Thow Sun, a Singapore national, alleges one count of theft of trade secrets in violation of 18 U.S.C. § 1832 and one count of interstate transportation of stolen property in violation of 18 U.S.C. § 2314. Mr. Sun was arrested on March 29, 2002, as the culmination of a sting operation conducted by the FBI based on a criminal complaint filed with the Court.

An affidavit filed by an FBI agent in the case alleges that Mr. Sun contacted the president of Language Line Services in Monterey, California in March 2002 and offered to sell to him proprietary information of Language Line Service's chief competitor, Online Interpreters, for \$3 million. Attorneys for Language Line Services promptly contacted the FBI. With the continuing assistance of individuals from both companies, the FBI arranged a meeting on March 24, 2002. At that meeting, Mr. Sun provided certain documents to prove that he had access to the trade secrets of Online Interpreters. In return, Mr. Sun received \$5,000. A subsequent meeting was arranged to deliver the remaining trade secrets on March 29, 2002, in exchange for \$3 million. Following this meeting, Mr. Sun was arrested.

Mr. Sun was ordered by a federal magistrate to remain in custody. His next court appearance is for arraignment on April 12, 2002, at 9:30 a.m. before Magistrate Judge Larson.

34. [United States of America v. Jeffrey A. Forques, Case No. _____ \(Boston April 25, 2002\).](#)

One count EEA indictment of attempting to buy trade secret information owned by AlphaGary Corp. which has plants in the United States, Canada and the United Kingdom and manufactures plastic wire and cable insulation compounds.

The indictment alleges that in January, 1999 Mr. Forques tried to receive, buy and possess the actual chemical ingredients of AlphaGary products which are protected as trade secrets with secret code names.

35. United States v. Jeffrey W. Dorn (District of Kansas May 2, 2002).

The United States Attorney for the District of Kansas (Eric Melgren) announced that nine individuals were indicted on Wednesday, May 1, 2002, by a federal grand jury in Kansas City, Kansas. Those indicted include:

* Jeffery W. Dorn, 28, currently of West Des Moines, Iowa, previously of Olathe, Kansas, is charged with one count of stealing a trade secret from the Spencer Reed Group, Inc., Overland Park, Kansas, from January 23, 2001, through January 31, 2001.

An affidavit filed with the court alleges that Dorn, while employed with Spencer Reed Group, Inc., (SRG), an employee placement firm, stole information from SRG pertaining to the matching of potential employees with prospective employers. The affidavit further alleges that in January 2001, Dorn, working independently of SRG, used SRG information to place a candidate directly with a company in the Kansas City area. The affidavit also alleges that this company paid Dorn directly for this placement.

If convicted, Dorn faces a maximum of ten years in federal prison without parole. The case was investigated by the FBI and is being prosecuted by Assistant U.S. Attorney Leon Patton.

36. United States v. Zhu, Case No. 02-M-0421 (June 19, 2002).

JIANGYU ZHU, a/k/a "Jiang Yu Zhu," age 30, and KAYOKO KIMBARA, age 32, both of 3440 Lebon Drive, San Diego, California, were charged in a criminal complaint with conspiracy, theft of trade secrets, and interstate transportation of stolen property. The charges arise out of the alleged theft of certain trade secrets belonging to Harvard Medical School, including reagents made and used by Harvard Medical School to develop new immunosuppressive drugs to control organ rejection, and also to study the genes that regulate calcineurin, an important signaling enzyme in the heart, brain and immune systems. It is alleged that ZHU and KIMBARA stole the trade secrets and then transported them from Boston, Massachusetts to San Antonio, Texas.

Zhu is a citizen of the People's Republic of China and a permanent resident alien of the United States. He received a Bachelor of Science Degree from Beijing University in 1991 and a doctoral decree in biochemistry from Temple University in 1997. From February 27,

1997 to on or about December 31, 1999, Zhu was employed as a research fellow in Dr Frank. McKeon's laboratory at Harvard. Dr. McKeon is a Professor of Cell Biology at Harvard.

Kayoko Kimbara is a citizen of Japan and a permanent resident alien of the United States. Kimbara received a doctoral edgree from Tokyo University in 1998. From on or about October 1, 1998 until on or about December 31, 1999, Kimbara was employed as a research fellow in Dr. McKeon's laboratory at Harvard.

Both Zhu and Kimbara signed a Participation Agreement upon coming to Harvard which provided that all rights to any invention or discovery conceived or first reduced to practice as part of or related to Harvard University activities are assigned to Harvard and that such obligations would continue after the termination of employment.

Despite their legal and contractual obligations, it is alleged, Zhu and Kimbara took and conspired to take proprietary and highly marketable scientific information belongint to Harvard with them to Texas with the intention of profiting from such information by collaborating with a Japanese company in the creaton and sale of related and deriative products by continuing the develop the information and by publishing the results of research began at Harvard.

On December 13, 1999, Zhu received an offer for employment from the University of Texas at San Antonio. On December 14, 1999, the day after receiving the offer from the University of Texas and whil still employed at Harvard, Zhu send an email to a biochemical company in Japan in which he stated his intent to collaborate with another researcher (Kimbara) soon after he leaves Boston to commercialize the antibodies asuggested by the calcineutrin research done in Dr. McKeon's lab at Harvard. In this email, Zhu also detailed his beief that the Harvard patent application would fail.

.ZHU accepted the position with the University of Texas, both to run his own lab and to teach. KIMBARA was also hired to work in the University of Texas laboratory. Both were scheduled to begin their employment on January 15, 2000. Thereafter, Zhu send CSP1, CSP2 and GRIP1 genes to the biochemical company in Japan and antibodies were thereafter shipped to Zhu at the University of Texas

37. United States v. Kissane, (S.D.N.Y. October 15, 2002)

Timothy Kissane was sentenced on October 15, 2002 two years in prison for theft of a trade secret in connection with his prior employment at System Management Arts Incorporated ("SMARTS"), a software company based in White Plains, New York. Kissane pled guilty on May 14, 2002.

According to the Information, KISSANE worked as a release engineer at SMARTS, and was responsible for the packaging of multiple components of the SMARTS software package, including its source code. " SMARTS developed and sold a custom software program called "InCharge", which monitors large computer networks, and identifies operational problems on the network. SMARTS sold "InCharge" to large telecommunications companies around the country and abroad. "InCharge" is a proprietary computer program, and its source code is a guarded secret.

On November 28, 2001, KISSANE's employment at SMARTS was terminated. Several weeks later, two of SMARTS' competitors received email messages from a "Joe Friday" at a Yahoo! email account, offering SMARTS' source code for sale. According to the Information, one of the email messages stated that the sender possessed the "cvs repository of SMARTS InCharge code, from 11/20/01 as well as custom code for specific bug fixes and customer-requested enhancements." The competitors brought these email messages to the attention of SMARTS.

According to the Information, connections to the Yahoo! email account from which the "Joe Friday" email messages were sent was opened at the White Plains Library, White Plains, New York. As the earlier Complaint charged, this Yahoo! account was then accessed approximately thirty-three additional times in December 2001 from a Verizon DHL Internet account located at the Lavallette, New Jersey address where Kissane had previously informed SMARTS that he would be living.

38. United States v. Morris (D. Delaware October 17, 2002).

Colm F. Connolly, United States Attorney for the District of Delaware, announced that John Berenson Morris of Mt. Kisco, New York, entered a guilty plea to one count of attempting to steal and transmit trade secret information belonging to Brookwood Companies, Inc., a textile company based in New York, New York.

Morris was prosecuted under the Economic Espionage Act of 1996, which makes the theft of trade secrets a Federal criminal offense. He faces up to ten years imprisonment and a fine of up to \$250,000 on this charge.

Connolly said that during July and August 2002, Morris attempted to sell Brookwood's proprietary pricing information to one of its competitors, Newark-based W.L. Gore & Associates, Inc. This pricing information related to a then-outstanding multi-million dollar U.S. Department of Defense solicitation for bid for the production of certain military fabric products. From July 26, 2002, through August 5, 2002, Morris placed a series of phone calls to a man he believed to be a Gore employee, in which Morris offered to sell Brookwood's trade secrets for \$100,000. What Morris did not know at the time, however, was that this man was actually an undercover Department of Defense agent. The phone calls culminated in a meeting at a rest stop on the New Jersey Turnpike on August 5, 2002, where Morris was arrested.

Connolly said that W.L. Gore contacted federal law enforcement shortly after Morris placed his first phone call to Gore to propose the illegal sale of information. Connolly noted that this action enabled law enforcement to arrange for the undercover special agent to receive and respond to Morris' subsequent overtures.

39. United States v. Ye (N.D. California December 4, 2002)

Fei Ye, a/k/a Ye Fei, age 36 of Cupertino, California, and Ming Zhong, a/k/a Zhong Ming, a/k/a Andy Zhong, age 35 of San Jose, California, were indicted by a federal grand jury on a total of 10 counts, including one count of conspiracy in violation of 18 U.S.C. §§ 371, 1831(a)(5) and 1832(a)(5), two counts of economic espionage in violation of 18 U.S.C. § 1831(a)(3), five counts of possession of stolen trade secrets in violation of 18 U.S.C. § 1832(a)(3), and two counts of foreign transportation of stolen property in violation of 18 U.S.C. § 2314. The charges stem from a conspiracy allegedly carried out by the defendants to take trade secrets stolen from four Silicon Valley companies to the People's Republic of China (PRC).

Fei Ye is a citizen of the United States; Ming Zhong is a permanent resident. Both defendants are originally from China. The indictment does not charge that the Chinese government was a conspirator. According to the indictment, it is alleged that Fei Ye and Ming Zhong conspired to commit the offenses of economic espionage, possession of stolen trade secrets, and foreign transportation of stolen property. The trade secrets were allegedly stolen from four companies: Transmeta Corporation (Transmeta); Sun Microsystems, Inc. (Sun); NEC Electronics Corporation (NEC); and Trident Microsystems, Inc. (Trident), all high-tech companies in Silicon Valley.

Both defendants are former employees of Transmeta and Trident. Fei Ye also worked at Sun and NEC. Some of the stolen trade secrets were seized from the defendants at the San Francisco International Airport (SFO) while they were attempting to fly to China. Other trade secrets were seized from the defendants' residences and Ming Zhong's Transmeta office in the County of Santa Clara.

The indictment alleges that the stolen trade secrets were possessed in connection with a project known as Supervision, Inc., to produce and sell microprocessors. More specifically, the indictment alleges that defendants Fei Ye, Ming Zhong and others established and promoted Supervision, Inc., a/k/a Hangzhou Zhongtian Microsystems Company Ltd., a/k/a Zhongtian Microsystems Corporation, to produce and sell microprocessors in China.

The defendants attempted to recruit others, including engineers, to participate in and work for the Supervision project. The defendants made representations to others they were recruiting for the Supervision project. They told others that: (1) funding for the Supervision project was being provided by Hangzhou, a city in China; (2) Supervision was also applying for funding from the 863 Program, a Chinese government high technology research and development program; and (3) Supervision was working with a professor from a University in the PRC, who was assisting in obtaining funding from the 863 Program.

On November 23, 2001, the defendants are alleged to have possessed trade secrets belonging to Transmeta and Sun in their luggage at SFO while attempting to board an aircraft bound for China.

On November 23 and 24, 2001, defendant Fei Ye is also alleged to have possessed trade secrets belonging to Sun, NEC, and Trident at his residence in the County of Santa Clara.

On November 23, 2001, defendant Ming Zhong is alleged to have possessed trade secrets belonging to Trident at his residence and at his Transmeta office.

On or about November 23 and 24, 2001, defendant Fei Ye is alleged to have possessed a corporate charter for Hangzhou Zhongtian Microsystems Company Ltd. at his house which states that the joint-venture will raise China's ability to develop super-integrated circuit design, and form a powerful capability to compete with worldwide leaders' core development technology and products in the field of integrated circuit design.

On November 23 and 24, 2001, defendant Fei Ye is alleged to have possessed a feasibility report review regarding Zhongtian Microsystems Corporation at his house. The report suggests that the project receive the support of the Chinese government.

On or about November 23, 2001, defendant Ming Zhong is alleged to have possessed a project application form for the National Special Foundation for Importing Knowledge of Software and Integrated Circuits printed by the National Bureau of Foreign Experts at his house. This application states that the project is of tremendous significance to the Chinese integrated circuitry industry and that the project should receive the support of the government.

Both defendants were arrested on November 23, 2001, at the airport. They were released on bail after appearing before a U.S. Magistrate Judge. Fei Ye's bail was set at \$500,000, and Ming Zhong's bail was set at \$200,000.

40. United States v. Serebryany (January 16, 2003).

Igor Serebryany, a 19-year-old student at the University of Chicago, stole trade secrets pertaining to DirecTV's latest and most sophisticated conditional access card, the "Period 4" access card.

The trade secrets were stolen from the law offices of DirecTV's legal counsel, Jones Day Reavis & Pogue in Los Angeles. DirecTV had provided this information to Jones Day in connection with civil litigation between DirecTV and one of its security vendors, NDS Americas, Inc. Serebryany allegedly stole the information while working for a document-imaging company that Jones Day had retained in the DirecTV litigation.

DirecTV delivers digital programming to millions of homes and businesses throughout the United States. A consumer wishing to subscribe to DirecTV programming must first obtain necessary hardware items, including a conditional access card, to receive the satellite signals. The access card is a key component in the security and integrity system for DirecTV satellite programming. DirecTV invested more than \$25 million to develop the Period 4 access card with the assistance of its security vendors. The three previous generations of DirecTV access cards have all been compromised by hackers who have developed ways to circumvent DirecTV's conditional access technologies.

Jones Day was outside counsel for DirecTV and represented the company in civil litigation that was commenced on September 6, 2002 by DirecTV against NDS, the developer and supplier of the proprietary encryption and smart card technology for DirecTV. In preparation for this litigation, DirecTV and Jones Day had been actively reviewing documents pertaining to the development of the Period 4 card, and in August 2002 DirecTV delivered trade secrets to Jones Day. Some of the trade secret information was so secret and valuable to DirecTV that DirecTV had previously maintained the information only in encrypted format on computer hard drives secured at DirecTV facilities.

The Indictment charges that in September 2002, some of this most highly sensitive trade secret information was stolen from DirecTV and distributed by Serebryany. These secrets included confidential internal design notes and correspondence between DirecTV and NDS regarding the Period 4 access card architecture and security features.

Serebryany is charged with three counts of theft of trade secrets, each one of which carries a statutory maximum sentence of 10 years in federal prison.
