New Jersey Law Journal

VOL. CXCVIII – NO. 10 - INDEX 793 DECEMBER 7, 2009 ESTABLISHED 1878

Employment & Immigration Law

Besides The Pudding: Where To Find Proof of What Trade Secrets Left With a Departing Employee

By James P. Flynn

Though many will say that "the proof is in the pudding," the original phrase is a bit fuller. "The proof of the pudding is in the eating," is what Cervantes said in his masterwork, *Don Quixote*. Nothing leaves a more sour taste in the mouth of an employer than a departing employee setting up shop to compete with that employer by using the employer's own information, client lists and know-how, and nothing makes a former employer hungrier for the proof necessary to stop such unfair competition. But one must ask how an employer can make sure the efforts to stop ex-employees amount to more than quixotic windmill tilting. The simple answer is grounded in the reality of proof, and the present discussion centers on how one can amass that proof quickly and cost-effectively.

To start the process, one must understand that the ingredients of this "pudding" are, and how they can be stored in a manner that keeps them and the business safe and productive. Some review or "intellectual property audit" is often how this is done. Such audits revolve around three essential sets of inquiries: (i) Is it now being protected sufficiently? If not, what should be done to improve the protection of the company's intellectual property?; (ii) In terms of the intellectual property of others (license, etc.), is company abiding by its obligations, and do we need to alter or amend them?; (iii) Is the company's intellectual property being adequately and properly promoted and exploited? Hancock (ed.), "Corporate Counsel's Guide To Intellectual Property," BLI, at 5.101-202. Depending on one's experience in dealing with intellectual property, this is an appraisal that can be managed internally, or can be done with outside assistance.

Assuming that one understands that special mix that represents a company's "pudding" as it were, one must patrol vigilantly to prove that an employee has departed with samples of it. A 2009 study by the Ponemon Institute confirms a human resources truism: departing employees frequently steal company data while heading out the door. According to the study, 59 percent of departing employees admit that they stole company data; 92 percent of departing employees admit that they took CDs/DVDs; and 73 percent admit taking USB memory sticks. While none of the study's findings should be a surprise to those who regularly address these issues, it is interesting to see a study which quantifies the scope of the problem.

But it is usually not as easy to see who took confidential data as it is to see who ate the pudding. Simply stated, one does not see something as visible in most cases as the child with the empty bowl, and chocolate smeared across his or her face. If the proof is in the eating, one must be ready to prove that the departing employee helped him- or herself to these treats without such visible signs. One way to do this is to be ready, upon an employee's departure, to go quickly through appropriate technology, document, and employee departure checklists.

In going through the technology checklist, one may address a number of

Flynn is a member and co-chair of the national intellectual property litigation practice of the Newark office of Epstein Becker & Green.

available sources of proof, and having a planned checklist will allow this to be done quickly and systematically. Every internal investigation should include a survey of the following potential sources of information.

Office Personal Computer/ Laptops/PDAs: Electronic Files: may contain records of thefts, correspondence with prospective employers, competitors, and confederates, new business plans, and unauthorized data downloaded from confidential files. Segregate and maintain the relevant hard drives of the computers and servers used by suspected employees. Preserve all back-up tapes. Also check diskettes, the company's master tapes, back-up systems, hard copy files and the employee's laptop. Carry out the same process for close associates of the subject and the subject's assistant.

E-mail: Download the subject's company e-mail. Barring the existence of a company policy that specifically guarantees the privacy of e-mail (which is unlikely), it is likely lawful for a company to examine an employee's company e-mail. But take care to understand the issues that may arise if an employee's personal e-mail account is being used through a company computer, as the employer's rights and employee's respective rights may be different than in the case of company e-mail. See *Stengart v. Loving Care*, 408 N.J. Super. 54 (App. Div. 2009).

Voicemail: Voicemail may be subject to claims of privacy and the protection of eavesdropping statute. However, a company policy stating that voicemail is subject to company review may defeat such a claim. So will a custom within the office of checking one another's voicemail. The investigator should consult with company counsel before gaining access to voicemail because of legal issues regarding wiretap laws.

Telephone Dial-out/Dial-in Records: Retrieve the records of telephone calls made from the subject employee's telephone extension and cellular phone. Investigators can use reverse directories (available on compact discs) or other investigative means to identify the subscribers. Telephone dial-out records may show that the subject called competitors and other parties he or she would have no business reason to call. Some telephone systems record the numbers of incoming calls. These records can be used to analyze calls made to the subject. Investigators also should examine call message records. These frequently are conveniently contained either in message logs or imprinted on duplicates.

Card Access Records: Electronic card readers systems contain data showing what portals were entered and by which employees. This is important when seeking evidence that an employee attempted to enter a restricted area, especially during off-hours.

Video Surveillance Cameras: Unusual times of access or egress to the work area prior to departure from employment should be explained. In addition, large folders or boxes entering or leaving the premises shown on film can be strong evidence of misappropriation.

Traditional hard copy sources also should be reviewed. In going through the paper checklist, one may address a number of available sources of proof, and having a planned checklist will allow this to be done quickly and systematically. Every internal investigation should include a survey of the following potential sources of information:

Search the Employee's Office: When conducting an internal investigation of misconduct, particularly in cases involving the theft of intellectual property, investigators should begin their search right in the suspect employee's office. There is a potential warehouse of incriminating information available there. In almost all cases, a search of the employee's office and desk are lawful. This includes the employee's telephone directory, but investigators should consult company counsel before searching personal belongings such as a briefcase, overcoat or before searching a locker. Also, one should check sign in/ sign out sheets as well.

U.S. Mail/Express Mail Service Records: Mail records will contain evidence of letters and packages sent by a subject to questionable recipients. There have been cases of corrupt employees actually mailing blueprints, designs, prototypes and samples directly out of the company mailroom. Investigators also should check the routing slips and instructions given to internal and external messenger services, for both incoming and outgoing deliveries.

Expense Account Records: Expense accounts are commonly abused by corrupt employees. An audit of expense accounts may provide evidence of abuse and of entertainment of questionable parties.

Cancelled Paychecks: Investigators should examine the endorsements on pay, bonus and expense checks to see if there are endorsements in addition to the employee's. Employees in serious financial difficulty may endorse a check over to a creditor. If a highly compensated employee cashes a check at a check cashing business or finance agency, it would suggest the employee is in financial difficulty.

W-4 Statements: If the employee has overexempted or recently raised the number of exemptions without evident cause, it would suggest financial difficulty.

Human Resource Files: Human resource files may reflect complaints against the employee by other associates, requests for loans, medical notes, evidence of frequent residence changes, garnishments and other relevant information.

In addition to checklists aimed at seeing what the departing employees may have already done, one should also take steps to make sure that they do not do anything else damaging to their former employer:

- Delete the employee's passwords to computers and e-mail, and disable any ability to log in remotely;

- Delete the employee's card entry access;

- Cancel the employee's credit

cards and telephone PIN numbers;

• Retrieve all company documents and company-owned equipment from employee's office and home. (When issued, these should be numbered and receipted);

• Do not permit a former employee to clean out his or her office. Permit the employee to retrieve personal items required to depart the premises, such as outer garments and briefcase. The company can pack other personal items for shipment to the employee;

• Notify the company that the employee is no longer employed (a simple e-mail is the fastest, most effective way).

If one can digest lessons like these, the prompt location and segregation of the proofs necessary to demonstrate the theft of trade secrets and confidential information becomes a reality. These facts are the most important ingredient in providing the courts to which an employer turns for relief a flavor of what has occurred. The proof of the pudding is, indeed, in the eating. ■