



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 6, No. 32, 08/06/2007. Copyright © 2007 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Trade Secrets

Data Security, Employee Issues

The top two data security risks for many companies are the misappropriation of trade secrets and security breaches. However, businesses often approach the protection of trade secrets and the protection of private information from different perspectives. M. Todd Sullivan and John E. Pueschel of Womble Carlyle Sandridge & Rice, PLLC, argue for a more holistic approach to data security as the most effective way to protect both types of information, particularly in the context of the dishonest current or former employee. They write that trade secret protection can benefit from application of the generally more regimented security measures applied to private information, while private information may be better protected by observing some of the lessons learned in trade secret cases about preventing and putting a stop to an attack on business information.

Disloyal Employees and the Misappropriation Of Trade Secrets and Private Information

By M. TODD SULLIVAN AND JOHN E. PUESCHEL

Betrayal. Disloyal. Thief. Saboteur. Cyber crime. These words generally are *not* the words you hear companies use to describe their employees in meetings, annual statements or press releases. However, with increasing frequency, these exact words are often used in court documents and public notices when

a company claims to have been victimized by an employee who has taken trade secret information or private information about consumers or employees for his or her own personal gain.

Experience has shown that the vast majority of employees are hard-working, dedicated, and loyal to the businesses for which they work. Experience also has

proven, however, that just one employee with malicious intent can devastate a business by stealing or mishandling proprietary information, trade secrets or the private information of employees or customers.

In a business climate that is becoming increasingly cognizant of the need for data security procedures to protect both trade secret and private information, companies find themselves facing an array of risks that can challenge even the most sophisticated security measures. Chief among these risks are two that are not easily addressed by training employees on proper policies or procedures. First, there is the risk of the employee who seeks to intentionally misappropriate trade secrets to advantage himself or his new competing employer. Second, there is the frequently underestimated risk of the rogue employee who steals private information regarding customers or employees for financial gain or identity theft purposes.

Perhaps unknowingly playing into the hands of such employees, many businesses tend to compartmentalize data security issues. For example, companies that build their business on technical information or intellectual property tend to focus their data security on protecting those trade secrets, failing to recognize or protect the vast amount of private information they may have concerning their employees or customers. On the other hand, businesses that trade in consumer information or other information subject to privacy protection laws tend to approach data security from a legal compliance perspective, seeking to ensure proper handling and use of that private information, yet failing to focus on their trade secrets. The reality is, however, that virtually all businesses tend to have both trade secret information and private information. Accordingly, it is critical to take a holistic approach to data security to ensure that data security policies and procedures are harmonized so as to optimize, on an enterprise-wide basis, the protection of all of the company's valuable trade secret and private information.

Why Businesses Tend to Approach the Security of Trade Secrets and Private Information Differently.

A 2006 study polled more than 800 companies about data security issues. The respondents rated the top two data security risks as the misappropriation of trade secrets and security breaches resulting in the disclosure of private information. Interestingly, the study's respondents considered the loss of trade secrets as a more serious threat to the company than the disclosure of private information. This study's finding may lend empirical support to what our experience leads us to believe, which is that because of the substantial regulatory guidelines and established procedures on the protection of private information, businesses tend to view themselves as having a firmer grasp of how to manage the private information entrusted to them, as compared with the less defined, case-by-case analysis applied in the law when it comes to the necessary requirements for securing trade secret information.

Most states have adopted some form of the Uniform Trade Secrets Act (UTSA). The UTSA offers broad protection for proprietary business information. Indeed, trade secrets can include highly technical information, as well as more general business information and compilations of information about methods, techniques and business processes. Whether something constitutes a

trade secret is generally not decided by looking to a statute or regulation. Rather, this decision is almost always made on a case-by-case basis during litigation over the alleged trade secret. Courts have held a wide variety of information to be trade secrets, such as customer and supplier lists, pricing information, market research and forecasts, and business strategy documents.

However, it is not sufficient merely to fall into a category held by the courts to be a type of trade secret. In addition, the information must have commercial value as well as be kept secret and not generally known or easily recreated by reverse engineering. Under the UTSA, the information has to be the "subject of efforts that are reasonable under the circumstances to maintain its secrecy." Thus, in order to preserve the information's trade secret status, the business is required to take affirmative steps to protect the trade secrets and to maintain their confidentiality. Again, what is "reasonable" is decided on a case-by-case basis, and can include a host of legal and practical restrictions such as confidentiality agreements and policies, computer password protections, physical security such as locks and keys, special handling of confidential documents and information, and secure disposal methods. It is in this aspect of trade secret protection that we believe many of the statutory and regulatory-driven data privacy practices may be adapted to enhance company trade secret protections.

With respect to the protection of private information, both the federal government and many states are enacting legislation and promulgating rules designed to make businesses take better care of personal information regarding their customers and employees. In large measure, this legislation and regulation is a response to the vast amounts of private financial and health information being compiled by the government and the private sector, as well as in response to the growing identity theft crisis. So, in recent years Congress has passed the Gramm-Leach-Bliley Act imposing privacy requirements on the financial services industry, and the U.S. Department of Health and Human Services has promulgated privacy and security rules under the Health Insurance Portability and Accountability Act (HIPAA) that apply to many health care providers and health plans. Congress also amended the Fair Credit Reporting Act to strengthen consumers' ability to fight identity theft. This amendment includes the "Disposal Rule" requiring all businesses to use reasonable methods and due diligence to ensure that sensitive information from consumer reports is properly destroyed so that criminals cannot recover it. The Federal Trade Commission has also been active in enforcing Section 5 of the FTC Act regarding the protection of sensitive consumer information.

Almost weekly, there are new reports and cases involving departing employees attempting to steal their employers' trade secrets.

In addition, overlaying this federal regulatory framework, many states are passing further regulatory requirements (and creating potential sources of liability)

for businesses concerning the proper handling of Social Security numbers and the private financial and health information of individuals. Furthermore, privacy laws generally provide that in the event of a breach resulting in disclosure of private information, the responsible company must provide written notices to each affected individual and even government agencies such as state attorney generals.

As is plain, the strictly regulated approach to protecting private information is fundamentally different from the trade secret regime, where the protections required are generally left to business judgment as to what is a reasonable protection for the trade secrets. For this reason, it is our experience that businesses often approach the protection of trade secrets and the protection of private information from different perspectives. It is our view however, that a more holistic approach to data security is the most effective way to protect both types of information, particularly in the context of the dishonest current or former employee. Trade secret protection can benefit from application of the generally more regimented security measures applied to private information, while private information may be better protected by observing some of the lessons learned in trade secret cases about preventing and putting a stop to an attack on business information. To do so, it is helpful to look at how companies may be victimized by employees in these contexts.

The Competitive Threat: Departing Employees, Inside Jobs, and Trade Secrets.

From a business perspective, the situations in the data security realm that tend to draw the most attention are often those cases where former employees are alleged to have taken their former employer's most sensitive trade secret information with them. These situations, which almost always involve the threat that trade secrets will be used against the company to advantage a competitor, pose tremendous financial risks to the jilted company. First, there is the loss of the trade secret information itself, often representing a tremendous asset and advantage in the marketplace. Second, there is the potential loss of market share that could result from a competitor taking the confidential information and using it to directly compete against the company. Third, there are the significant legal litigation expenses and fees that are involved in seeking to prevent the departing employee and his new competing business from misappropriating a former employer's trade secrets. Such litigation typically involves seeking a preliminary injunction, which causes the litigation to be "front loaded," in that the case requires a tremendous effort at the outset to stop the misappropriation of the trade secrets. And of course, there is the intangible loss of time and human resources, because if a business and its key employees are focused on such litigation, they cannot devote their full attention to the company's core business.

A recent study found that fully 20 percent of security breaches at medical centers in 2006 resulted from "insider malfeasance."

Almost weekly, there are new reports and cases involving departing employees attempting to steal their employers' trade secrets to advantage themselves or their new employer in competition. What such cases all have in common are employees who use their access to information and the trust placed in them by the company to circumvent data security protections to steal proprietary and trade secret information. In just one recent example, a client service representative at Morgan Stanley left the company intent on starting a consulting company. However, to aid his new venture, the departing employee allegedly conspired with two other Morgan Stanley employees to steal proprietary information, including a client rate list, and e-mailed this sensitive business information to the departing employee's home e-mail account. In this case, the employees' conduct was discovered and their plan thwarted, ending in criminal charges against the employees.¹

What can we learn from these trade secret cases involving departing employees? They give some indication as to whom the company should scrutinize as a potential risk. That advantage does not exist in a more sinister type of trade secret case, where a current employee sets out to steal trade secrets for personal gain while remaining employed. One high profile case involving the owner of perhaps the best known trade secret of all, the formula for Coca-Cola, illustrates this point. A secretary for a senior executive at Coca-Cola conspired with two men who did not work for the company. The plan, it appears, was to have the secretary steal trade secrets to which she had access by virtue of her position, and then sell the secrets to rival Pepsi. The plan fell apart because Pepsi informed law enforcement and Coca-Cola of the plot, resulting in criminal convictions for the conspirators.²

While the foiled Coca-Cola plot seems almost humorous due to the lack of sophistication of the conspirators, it should give all employers concern because until Coca-Cola received the call from Pepsi, it apparently had no reason whatsoever to think that the secretary was out to damage the company for her own profit. More sobering is a case involving Corning Inc. An employee allegedly found blueprints for highly proprietary technology *in a bin to be discarded*. The value of the technology contained in the plans was estimated to be \$100 million. The employee sold the plans to competitor in 2000 for \$34,000, but Corning did not discover the theft until the next year.³

¹ Christopher Faille, *Suspect in Morgan Stanley's Leak' Arrested*, Daily News (White Plains, New York, Apr. 5, 2007).

² Harry R. Weber, *Ex-Con Gets 2-Year Sentence In Coca Cola Trade Secrets Conspiracy Case*, Associated Press Financial Wire (June 7, 2007).

³ Ben Dobbin, *Consultant Provided Corning Glass Secrets to Taiwanese Rival*, Associated Press Financial Wire (June 13, 2007).

The Rogue Employee and the Risk to Private and Protected Personal Information.

More and more people, and perhaps especially the unscrupulous, now know that private financial and health information about both consumers and employees is valuable. As identity theft claims continue to increase every year, affecting millions of Americans, the regulatory response at the state and national level has been to impose protections and obligations on businesses to control the circumstances under which such private information can be gathered, used, stored, and disposed of. One might wonder if the increased protections have caused such private information to become harder for criminals to obtain—and thus a more valuable commodity—since it appears to present a temptation that an increasing number of trusted employees have been unable to resist.

This summer, Fidelity National Information Services, a financial processing company, announced that an employee of one of its subsidiaries stole the records of 2.3 million customers and sold them to marketing companies for his own personal gain. Fidelity reported that the employee was a “senior level data base administrator” with access to the bank and credit card account information of consumers. A subsequent filing with the Securities and Exchange Commission indicated that the number of stolen employee records actually was closer to 8.5 million. The situation began to come to light when the company had a customer question the correlation of a number of transactions with the subsequent receipt of mail and telephone marketing attempts directed to consumers. Laudably, the company promptly investigated, and when unable to identify any breach of the company’s computer security, enlisted the assistance of the U.S. Secret Service. According to Fidelity, the Secret Service investigation tracked the compromised information to a company owned and operated by the employee. In what Fidelity called a “betrayal,” it appears that to avoid detection, the employee removed the information “via physical processes, not electronic transmission.”⁴

Fortunately for the consumers affected by the Fidelity situation, it appears that information was sold to legitimate marketing businesses, and that no identity theft issues were created by the security breach. But that incident is not without obvious and significant costs. In addition to the costs of human resources devoted to the situation, Fidelity announced that it filed lawsuits to recover the information, made required notices to state regulatory agencies about the security breach, notified the major credit reporting bureaus and credit card companies, and individually notified the millions of consumers at issue. Notwithstanding the tremendous costs involved in this process, such breaches also can result in the intangible costs of damaging the trust between the companies and the individuals affected by the breach.

Often consumers claim tangible losses when victimized by rogue employees’ actions. For example, in 2005 authorities broke up a pernicious scheme involving employees at a number of banks. The alleged ringleader of the scheme owned a company and would sell the pur-

loined information to debt collection agencies. Over a four-year period, these employees then systematically began gathering financial information on customers, either by printing screens or manually writing down the information, apparently to avoid detection or leaving an electronic trace of their crime. In exchange, it is alleged that the ringleader would pay the bank employees \$10 per name. This ring is alleged to have compromised the identities of more than 500,000 bank customers. In addition, some of the affected customers have pursued class action litigation against some of the banks for failing to adequately safeguard their information and remedy the breach.⁵

While these dramatic inside jobs targeted private financial information of consumers, businesses must realize that the theft of personal information is *not* limited to consumer or financial information. Indeed, the FTC reported in 2003 that approximately 90 percent of business record thefts involved payroll or employment records. This should not be a surprise considering the wealth of personal information maintained in company files regarding employees (and their family members), including drivers’ license numbers, Social Security numbers, bank account numbers for direct deposit, tax information, retirement account information, and health insurance and medical information. Furthermore, the risk of this is not limited to financial information. A particularly insidious form of identity theft is directed toward the protected health information of individuals. In this “medical identity theft,” thieves obtain the medical and insurance information of individuals, then use the information to have medical care or drugs provided to them but billed to the unsuspecting victim. It should be alarming to all that a recent study found that fully 20 percent of security breaches at medical centers in 2006 resulted from “insider malfeasance.”⁶

How Can Businesses Protect Trade Secrets and Private Information From Dishonest Employees?

While there is likely no panacea to completely eliminate the risk of a dishonest employee who has the time to plan, access to information, and the desire to steal, there are definite steps that a company can take to limit that risk. Furthermore, in undertaking these steps, the company can actually put itself in a better position to minimize its exposure, bring legal means to bear to stop and mitigate the damage, and perhaps even reduce any attendant negative publicity or damage to customer relationships.

As a threshold matter, companies must take an integrated, enterprise-wide approach to data security that recognizes that the company has valuable information that is a target for thieves in both its trade secret information and in its private information on employees and consumers. For example, in fashioning a cross-functional team or task force on data security, there may be a need to include operational employees who have knowledge of the company’s technical and trade secret information, marketing employees who have

⁵ See *Jones v. Commerce Bancorp., Inc.*, Civil Action No. 05-5600 (July 16, 2007) (Slip Opinion)

⁶ Privacy Rights Clearinghouse, *Chronology of Data Breaches 2006: Analysis*, available at <http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm> (last visited July 8, 2007).

⁴ See Fidelity National Information Services Press Release (July 3, 2007), available at <http://www.fidelityinfoservices.com/FNFIS/NewsRoom/20070703.htm>.

knowledge of the consumer information maintained by the company, human resources employees who have knowledge about the private information, including protected health information, on the company's employees, the facilities or security manager who has knowledge of the company's physical security, information technology personnel who have knowledge of how to secure the company's computer and technology resources, and legal advisors aware of the requirements applicable to the company. This team should then begin with an internal audit to identify all information to be protected, and then to implement appropriate policies and procedures.

In fashioning and implementing this plan, we counsel businesses that it is critical to consider the following additional points to best secure their trade secrets and private information, being particularly mindful of the significant risk posed by a potential rogue employee:

- Review your hiring procedure to ensure that a thorough background screen and criminal history check is conducted on all potential employees, especially those who will have access either to trade secrets, or to the private information of employees or consumers. After all, the best defense to the would-be rogue employee is not to hire him in the first place. Part of this screen should include asking for and thoroughly checking references, which we find is all too frequently omitted by companies, but which provides an excellent source of information (or perhaps equally telling, a lack of information) about the applicant. Companies may consider more thorough screenings for employees handling sensitive information. In addition, with the proliferation of social networking pages, it can be useful to conduct an Internet search to see if the applicant has elected to provide additional information about him or herself online.
- Implement written policies on proper handling of both trade secret and private information. Periodically communicate policies and train employees on the importance of data security.
- Where appropriate, have employees enter into confidentiality agreements that address both trade secrets and private information. Most companies tend to use employee agreements that address only business information or trade secrets. Broadening the agreement as appropriate will provide an extra legal arrow in your quiver should you have to go to court to protect either kind of information.
- Where appropriate, have non-compete agreements that will keep key employees out of the market for a period of time after they leave the company, thus discouraging them from trying to use stolen trade secrets to jump-start their new venture. Be aware that non-competes are becoming more difficult to enforce, and need to be tailored to each specific employee to avoid being held overbroad and thus unenforceable.
- Have an ethics policy that prohibits employees from operating a side business while employed. Recall that in two of the inside jobs discussed above, the employees used their side businesses to sell and profit from the stolen information. For key employees, it may be prudent to search the Secretary of State online database available in many states to help ensure they are not running a discoverable side business.
- Have physical security on your facility, such as fences, controlled access, alarm systems, and security guards. If sensitive information is maintained in specific areas (such as computer rooms), consider prohibiting access to employees with no need to be in those areas.
- Use locks on file cabinets and storage areas where sensitive information is kept.
- If you must disseminate trade secret information to vendors or potential customers, do so only pursuant to a confidentiality agreement, thus demonstrating your commitment to keeping the information secret to the extent possible while still being able to profit from it.
- Keep important paper files and records under lock and key, or in areas where access is limited to the people who need the information. Mark paper confidential documents "confidential," and give instructions on legending practices to employees.
- To the extent possible, limit access to sensitive documents and computer systems to those employees with a need for the information. If you make use of a document management system, make sure it permits restricting access to documents. Use passwords to protect your confidential information stored on computers. Use computer features limiting screen visibility and other computer security enhancements.
- Consider banning cameras and camera phones from the workplace. Recall that in the bank scam discussed above, the employees wrote down the information or printed screens to avoid leaving an electronic trail.
- Have an Internet and e-mail use policy that includes a prohibition on using that technology to access or transmit trade secret or private information unless expressly permitted to do so.
- For information technology employees with access to sensitive information, consider implementing network security that limits access to key information unless another employee also provides a password or permission to access the data.
- Consider whether it is prudent to limit the use of external hard drives or flash memory drives, including MP3 music players, as such devices are easy to conceal and can be used to download a great deal of information quickly.
- Explore the available computer applications that are designed to detect and alert if certain types of information are accessed or transmitted outside of the company.
- If it is necessary to transmit private information, encrypt the data if at all possible.
- Prohibit trade secret information or private information from being stored on laptop computers. Lost laptops account for a large percentage of security breaches.
- Do not neglect to ensure that document disposal policies provide for the secure disposal of trade secret and private information.

