SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, SEPTEMBER 26, 2011

How businesses can protect their valuable trade secrets

GUEST COLUMN

By Gay Grunfeld and Aaron Fischer of Rosen, Bien & Galvan LLP

With the recent multi-million dollar verdict in the Bratz fashion dolls case, the recurring leaks of unreleased next-generation iPhones, and other high profile cases, trade secret misappropriation remains highly relevant to innovative companies, big and small. In today's world of virtual offices and 24-hour remote access, a company's own employees are often the greatest threat to its intellectual assets. Employees may engage in blatant theft of trade secrets, or may lack sufficient certainty as to what company information can or cannot be disclosed or used. Each company should have a sound understanding of applicable trade secret laws and should take affirmative steps to protect itself from employees' misappropriation of trade secrets, which can cause enormous disruption and damage.

The California Uniform Trade Secrets Act (CUTSA), California Civil Code Sections 3426, provides companies with a powerful tool against the misappropriation of trade secrets. A trade secret may arise from an innovative design or idea, or an aggregation of valuable proprietary data such as customer information. A legally protectable trade secret is defined as information that: derives independent economic value, actual or potential, from not being generally known to the public or to others who can obtain economic value from its disclosure or use; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Trade secret protection is distinct from patent protection, and is available for any company information so long as such information is not publicly revealed, is not independently obtained by others, and is subject to steps to maintain its secrecy.

Under the CUTSA, an employer may seek injunctive relief based on a showing of "actual or threatened misappropriation" — that is, wrongful acquisition, disclosure, or use — of its trade secrets. Importantly, where an employer is able to show actual or threatened misappropriation, the court may compel *affirmative* acts by the employee, such as the return or electronic deletion of stolen data. The CUTSA also provides monetary damages in cases where the employer suffers an actual loss, or where the employee is unjustly enriched, as a result of the misappropriation.

Often, the critical element in a trade secrets case is whether the company information at stake is a protectable trade secret under the CUTSA. The "reasonable efforts" element is a common hurdle, particularly for companies that have not taken a deliberate and methodical approach to data security.

Many factors in today's business world make safeguarding trade secrets from misappropriation by employees and former employees particularly challenging. Employees must have daily access to the company's intellectual property to do their jobs. Employees typically have multiple means of gaining access to this information, including through company hardware, remote access to the company's intranet system, email, and cloud computing products, which allow online access to information from virtually any connected device.

If an employee or departing employee decides to steal company data, even a successful application for judicial relief, including a temporary restraining order, may come too late to stop misappropriation that jeopardizes the company's research and development efforts, customer relationships, and future viability.

Yet measures to increase the security of companies' trade secrets will almost certainly reduce efficiency. For example, a company may provide employees direct, unrestricted access to sensitive company data in order to facilitate their work on systems development or analysis, customer-specific issues, and other day-to-day operations. At the other end of the spectrum, that company may grant access to a single database administrator, requiring employees to request access to specific data on a case-by-case basis, thus limiting opportunities for theft and enhancing tracking of employees' access to data. The former policy does nothing to protect the company's proprietary information, while the latter creates a distrustful work environment and an information bottleneck that can hamstring operations.

The reality is that a small- or medium-sized company must balance many competing interests, and it may not be practical to take every possible step to prevent trade secret misappropriation. At the same time, as a company grows and develops a valuable intellectual repository of ideas, innovations, and aggregated data, there are a number of best practices that it can and should consider to protect itself from costly and even devastating misappropriation. Should litigation become necessary, these same best practices will bolster a company's case that it has made the required "reasonable efforts" to maintain the secrecy of its proprietary information. These practices can also benefit employees, providing useful guidance as to what is expected of them. Clear expectations promote a more positive work environment and allow employees to plan responsibly for future professional opportunities.

Gay C. Grunfeld *is a partner at San Francisco's Rosen, Bien & Galvan LLP, where she specializes in complex litigation.*

Aaron J. Fischer *is an associate at San Francisco's Rosen, Bien & Galvan LLP. His practices focuses on complex litigation.*

How businesses can protect their trade secrets

Require all employees to sign non-disclosure agreements (NDAs). Confirm that all current employees have signed an NDA by conducting an audit of personnel files. The NDA should specifically identify or define the nature of the company's trade secrets and confidential information. The NDA should indicate the employee's obligations to protect the information from disclosure and to return or destroy such information at a later date.

Provide initial and periodic training to employees on their obligations regarding trade secrets. Make clear what the company considers to be a trade secret and employees' duties as to maintaining the secrecy of such information. Remind employees that their obligations not to expose company secrets apply to social media, including professional networking sites such as LinkedIn.

Inventory all hardware that employees "check out" from the company. This includes all phones, PDAs, computers, and electronic data storage devices.

Assign administrator access and establish protocols for employees' access to sensitive company data. Company policy should delineate an administrator's discretion to grant other employees access to data, whether on the company's intranet or through cloud computing applications. Smart companies have a few information technology and/or human resources staff members share administrator privileges, which helps to minimize undue disruption if problems arise within either of those departments.

Maintain a system to track which employees have access to which company databases, files, and information. Conduct periodic data access audits to determine what data employees are accessing, both in the office and remotely.

Implement the "principle of minimal privilege." Ensure that employees have access to company data as is necessary for them to do their job, and restrict access to other sensitive data sources.

Develop an electronic communications policy that limits or prohibits transmitting confidential company information through personal email or to personal devices without authorization. Companies may utilize web-based applications for sending large or sensitive electronic company files. Such applications should have tools to audit the transmission of such data.

Develop a protocol on the use and dissemination of passwords needed to access confidential company data. Identify how passwords are assigned, protected, and changed on a periodic basis. Require all hardware, particularly mobile hardware such as Blackberries, to be password protected, and require employees to provide their company passwords to HR or a network administrator.

Develop a protocol for employee terminations and other departures. Access to confidential company data should be discontinued as soon as possible after the employee is terminated, and "checked out" company hardware should be recovered promptly.

Develop a process to identify and segregate company information from employees' personal files. It is likely that some personal data will be placed on corporate hardware. When an employee leaves or is terminated, supervise the disentangling of these files, ensuring that the employee may keep personal files (such as family photos) and return all company data.

Conduct an exit interview for departing employees. Departing employees should execute a certification as to whether they still possess any company data in electronic or hard copy form. (Many companies make a severance package contingent on the execution of this certification.) Use the exit interview to remind departing employees of their obligation not to copy, retain, disclose, or use trade secrets.

For sensitive or high-risk departing employees, create a forensic image of the employee's hard drive and maintain a library of such images. Maintain a documented chain of custody of these files, and preserve metadata.

While there is no surefire strategy to prevent the misappropriation of company information, California law — and good business sense — make it incumbent upon an employer to take proactive steps to protect its intellectual assets.