



Portfolio Media, Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

6 Steps For Avoiding Expensive Trade Secret Disputes

Law360, New York (July 6, 2016, 11:07 AM ET) -- Employees are increasingly digitally integrated. A simple scan of any downtown crowd reveals that most American workers have a mobile device, likely a smart phone or a tablet. Your employees probably bring those devices to work and may use them both at work and at home. Employees also send and post information on internet resources such as LinkedIn and other social media, and send information to and from personal email.

Do you know how many of your employees have sent files to their personal email so they could access information remotely? Does this violate any employment policy? How can you be sure that your data is safe? These common behaviors combined with ever evolving technology make it difficult to monitor the flow of company data, including potential trade secrets. And unlike other forms of intellectual property, a trade secret ceases to exist once disclosed.



Danielle Ochs

While the newly enacted Defend Trade Secrets Act of 2016 adds another weapon to the arsenal of litigation tactics available to fight the theft of trade secrets, trade secret litigation remains a costly endeavor. The better strategy continues to be avoiding costly trade secret litigation, as plaintiff or defendant, by implementing procedures, policies and practices that minimize the threat that your company will become entangled in an expensive trade secret dispute.

If you are not convinced that trade secret theft poses a real risk to your business, you need only review some of conclusions that led to the enactment of the DTSA. In 2013, the Obama administration issued the "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," which observed:

Emerging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating ... Foreign competitors of U.S. corporations, some with ties to foreign governments, have increased their efforts to steal trade secret information through the recruitment of current or former employees.

The report explained that “[a]dvancements in technology, increased mobility [and] rapid globalization” have created “growing challenges in protecting trade secrets.” The report advised that, “Companies need to consider whether their approaches to protecting trade secrets keeps pace with technology and the evolving techniques to acquire trade secrets enabled by technology ...”

The economic risks of trade secret misappropriation are readily reflected in several high-profile trade secret cases.

- A former automotive industry employee resigned to work at a foreign automotive company and copied 4,000 company documents onto an external hard drive, which he took out of the country. The company valued the loss of the trade secrets at \$50 million dollars.
- A research chemist stole confidential Organic Light Emitting Diodes (OLED) valued at \$400 million dollars and passed them to a foreign university.
- A former engineer and her husband stole confidential hybrid vehicle technology worth \$40 million and tried to pass them on to a foreign automaker.
- An investment firm spent \$500 million dollars developing computer source code to support its high frequency trading program. On his final day of employment a computer programmer transferred this computer code to an external computer server and transferred thousands of proprietary computer code files to his home computers.

These cases exemplify the significant economic risk to the U.S. economy posed by interlopers, but the risk arises from negligent acquisition as well (where an employee inadvertently brings third-party data to a subsequent employer), which can be equally harmful and disruptive.

The risks and costs of the theft of trade secrets are well documented and something that all employers should guard against. Here are six basic steps employers can take to protect trade secrets and minimize the risk of becoming entangled in a costly trade secret dispute.

1. Review and Identify Company Trade Secrets

While your company may maintain a confidentiality or similar agreement that states that employees may not use or disclose confidential or proprietary information, take an inventory of what that confidential information comprises. Trade secrets may include sensitive product information, research and development, critical and unique business processes, sensitive business information, or IT systems and applications. Under the DTSA, that information must be maintained confidentially and must gain value from not being known to others in your industry.

2. Assess the Value of Trade Secrets

Once identified, it is appropriate to examine the role trade secrets play in your company’s business and the impact to the business if improperly disclosed or used. How would improper disclosure or use impact the company’s reputation, fundamental operations, corporate culture and/or the uniqueness of the product used or sold? What would the value be to competitors? Would improper disclosure or use impact revenue? Assessing and quantifying the value of your company’s trade secrets is an important part of the preventive process but may also assist in bolstering your company’s ability to recover lost profits or reasonable royalties in any necessary litigation.

3. Audit the Risk of Trade Secret Misappropriation

Once the company has identified its trade secrets and quantified their value, it must assess the risks that could lead to improper disclosure or use. What measures has the company taken to secure the data? Who has access to it? Is information quarantined or accessed on a need-to-know basis? Are passwords in place and is the facility secure? Are employees taking home data? Are employees using personal smart phones and tablets or other storage devices to transfer company information? Do employees use personal file transfer accounts such as Drop Box or Google Drive for business? What about social media accounts such as LinkedIn?

Don't forget cloud computing and other backup systems where data may be stored. Understanding how your employee-handled data flow through your company is key to developing security protocols designed to maintain confidentiality. Not only is confidentiality key to maintaining trade secret protection, failing to maintain proper levels of security designed to assure confidentiality could undermine a later DTSA claim.

4. Implement Proactive Onboarding Strategies

While there are several data security practices available to protect the flow of information within your company, setting expectations among employees is equally important. Proactive onboarding strategies communicate your company's attitudes and expectations concerning confidential data, including the company's desire to avoid acquiring third-party confidential information that may belong to a prior employer.

- **Offer Letters:** Most employers include the basic terms of employment in an offer letter. You should, however, include language explicitly stating the potential employee would be prohibited from bringing, disclosing, reproducing or using their former employer's confidential, proprietary or trade secret information, including, for example, electronic or hard copy client lists, pricing information, marketing strategies, formulas, etc. You should preview and/or enclose the actual agreements the employee will have to execute (e.g., third-party information, nondisclosure and confidentiality agreements). Include a fact sheet identifying the places that an employee may have unwittingly stored data (e.g., personal email, flash drives, cloud accounts and backup systems).
- **Third-Party Information Nondisclosure Agreement:** The purpose of this agreement differs slightly from the traditional confidentiality, trade secret, or noncompete agreement because it protects the company from obligations the employee may have to other employers. It inquires about restrictions that limit the employee's ability to work for the company or relate to third-party intellectual property rights. This agreement should explicitly state that the employee is prohibited from bringing, disclosing, reproducing, or using third-party confidential, proprietary or trade secret information and require the employee to represent that he or she has no such information. Walking through this in person is recommended. Any issues or concerns with an employee's ability to comply with this agreement should be resolved before the employee begins work.
- **Confidentiality Agreements:** Confidentiality agreements are often the principle vehicle used to set forth the company's policies against disclosure of its own confidential information, although they can be combined with third-party information, nondisclosure agreements where desired. These agreements may repeat the provisions covered above but also contain important additional policies which should be detailed and specific. In this agreement, the employer typically lays out what it considers to be "confidential information."

This provision should be well thought out and not merely a recitation of every possible category of information that could be deemed confidential. The policy should set forth expectations, define what is confidential, if appropriate indicate who has access to what data, and set forth the employee's duty not to improperly use or disclose the company's information, to return information at termination, and the consequences of violating the agreement. The agreement should require written acknowledgment and should be the subject of annual training. Employers may include inventions and assignment provisions, noncompete and nonsolicitation clauses (where enforceable), and return of property provisions (which require employees to return property that may not otherwise be deemed "confidential"). Employers should also consider whether to include other key provisions such as arbitration, forum selection and/or choice of law clauses, which can help to determine the jurisdiction in which any conflict will be resolved.

- **Forensic Review:** When employers learn an employee may possess third-party information, it may be appropriate to retain a third-party forensic consultant to assist with forensic removal. This process, however, can be fraught with dicey issues including abiding by preservation requirements or demands, satisfying the duty to return data to prior employers, and respecting the privacy of employee information. You should obtain legal advice if forensic review is necessary.

5. Maintain and Enforce Policies and Procedures During Employment

During employment, perhaps the most perilous yet common scenario an employer faces involves an employee's use of his or her own device to perform work on behalf of the company. Strong bring your own device policies and technological oversight are essential to protecting employer information.

- **Bring Your Own Device (BYOD):** While policies vary depending on the reality of the workplace, there are several attributes any good BYOD policy should possess. The policy should require that all devices be identified, preserve the employers right to inspect devices (during and after employment), retain the right to wipe devices (including remotely), require access to external drives and cloud accounts, require immediate reporting of lost or stolen devices, and require password protection of devices. Employers should retain an IT professional to maintain and oversee these policies, limit access to confidential information, and track confidential information (it is helpful to stamp or serialize confidential information). It is also important and helpful to have clearly delineated guidelines covering who may access, modify, copy or delete confidential information, and to conduct periodic audits to enforce and ensure compliance with these policies. As with all important employment policies, regular training is a must.
- **Technology Solutions:** There are several technology solutions that track which documents are accessed, when, by who, and with what device. Using technology, employers can also allow employees to securely use their own cloud services without locking employees or IT into specific content repositories, and can encrypt work documents when stored in the personal cloud, allowing employers to set policies that prevent unauthorized use. Stay abreast of the evolving protections available in data security so the company satisfies current standards around confidentiality.

6. Follow Through with Effective Offboarding Strategies

Offboarding strategies focus on assuring that when your employees depart, your data does not go with them!

- **Exit Interview:** The exit interview continues to be a key opportunity to mitigate your company's risk of losing key confidential data. The exit interview presents an opportunity to review with the departing employee all of the information to which he or she had access and to assure that access has been terminated and that all data have been returned. You should include a member of IT on the exit interview team. During the exit interview, you should review and gain the employee's acknowledgment that access has been restricted, review the company's confidentiality and related agreements, review a checklist of property to assure that all company property and devices have been returned, and that all data has been removed from BYOD devices and accounts of all kinds including social media, cloud-based, file transfer, and backup accounts. Some level of forensic review may also be required.
- **Post-Employment Follow-Up:** While the tone and content may vary depending on the post-employment relationship with the former employee, it may be prudent to send a letter outlining any continuing obligations the former employee may owe to the company concerning the use or disclosure of confidential information and/or any applicable restrictive covenants, where enforceable.

While the DTSA provides another tool in the arsenal of tools an employer may use to protect its trade secrets, it also represents a threat for those employers faced with allegations of misappropriation. These steps are not fool proof, but they offer employers a road map to evaluating how to increase the possibility of avoiding the need for, or the exposure to, costly trade secret litigation.

—By Danielle Ochs, Ogletree Deakins Nash Smoak & Stewart PC

Danielle Ochs is a shareholder in Ogletree Deakins' San Francisco office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2016, Portfolio Media, Inc.