MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Steps for Protecting Trade Secrets

Scenario

A multinational company, headquartered in the United States, is reviewing its procedures and practices for handling confidential information and trade secrets, giving particular consideration to the Defend Trade Secrets Act of 2016. The company's general counsel is experienced using protective orders in litigation and maintaining non-disclosure agreements with third parties. The general counsel asks about other recommended measures to protect the company's trade secrets.

Importance of Protecting Trade Secrets and Confidential Information

Trade secret theft in the United States is estimated to cost businesses as much as $300 billion annually, with the most serious threats coming from employees and business partners. However, the real cost of trade secret theft can be difficult to measure because businesses are often unaware that their secrets have been stolen (trade secrets can be difficult to identify and value, and employees who steal trade secrets do not always appreciate that they are doing it).

With growth in the digital economy and an increase in cyber attacks, trade secret misappropriation is becoming even more significant. US President Barack Obama acknowledged that fact in his remarks at the signing of the Defend Trade Secrets Act: "As many of you know, one of the biggest advantages that we've got in this global economy is that we innovate, we come up with new services, new goods, new products, new technologies. Unfortunately, all too often, some of our competitors, instead of competing with us fairly, are trying to steal these trade secrets from American companies. And that means a loss of American jobs, a loss of American markets, a loss of American leadership."[1]

Taking Reasonable Measures to Protect Trade Secrets

One requirement for protecting a trade secret is showing that the owner has taken reasonable measures to keep the information secret. The use of protective orders in litigation is just one step. A company should determine whether it has taken such reasonable measures and whether it is prepared to protect and enforce its trade secrets and confidential information, if necessary. To do so, companies should determine whether they have appropriate procedures and policies, evaluate how they are managing inbound risks, and review how they handle confidential information, including with departing employees, consultants, contractors and third parties. If a company is uncertain about the adequacy of its procedures, it may want to consider conducting a trade secret audit.

Evaluating Policies and Procedures for Handling Trade Secrets and Confidential

Information

In evaluating corporate policies and procedures for handling confidential information, a company should reach out to relevant departments and teams to identify the company's trade secrets and to clarify how such information is designated and protected as confidential. This process may include determining what procedures exist for maintaining trade secrets, including reviewing: (i) confidentiality agreements with employees, consultants, business partners and contractors; (ii) IP assignment procedures and procedures for obtaining title to trade secrets; and (iii) the process for designating and maintaining information as confidential. With respect to confidentiality agreements, companies should determine whether their agreements, policies and procedures should be updated in light of the Defend Trade Secrets Act's notice of immunity provision.[2]

Companies also should consider whether their trade secrets are sufficiently protected and maintained, including by limiting disclosure of information, consistent with the requirement of relative secrecy for the protected information. For example, a company should determine how its trade secrets are maintained and whether such maintenance is adequate and reasonable under the circumstances. Is access limited to persons with a need to know? How is access physically and electronically controlled? Does the company have established security measures for accessing trade secret information? What are the company's policies and practices for educating employees, consultants, contractors and business partners on confidentiality requirements and practices?

Managing Inbound Risks

When bringing new employees on board, a company should prohibit the use of confidential information from a prior employer and determine whether an employee is subject to non-compete obligations. The same can be true when working with contractors, consultants and other business partners. It is helpful to create an environment of confidentiality. Also, while employees often have implied obligations of confidentiality, companies should document express obligations through agreements and policies. Risks can be managed by regularly educating employees, contractors and consultants on confidentiality requirements and practices.

Departing Employees and Security Measures

Trade secret misappropriation frequently occurs when a departing employee moves to a competitor company. To help minimize risk, determine the established procedures for departing employees. Do such procedures include disabling access to company systems and accounts, and requiring the return of company equipment? Do they include reminders or affirmations by a departing employee, including reminders about the employee's confidentiality obligations? Do they include written acknowledgements of the employee's obligations on departure?

A company also may want to evaluate whether it has appropriate security measures to protect its confidential information. In doing so, it should review its physical and electronic security measures and policies. Are they reasonable under the circumstances for protecting its confidential and trade secret information? Does the company have procedures or policies covering external access to confidential and trade secret information? What cybersecurity measures are in place? Does the company have social media policies, and how does it monitor social media?

Be Prepared

Companies should be prepared to take prompt action to protect their trade secrets and to immediately enforce their rights when necessary. A good first step is making sure that reasonable measures have been taken to protect confidential information. Companies that are unsure of the answers to the questions posed above may want to conduct a trade secret audit to determine

whether their procedures are reasonable and whether they are prepared to enforce their rights.

For inquiries related to this Tip of the Month, please contact Sharon Israel at sisrael@mayerbrown.com.

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, Ethan Hastert at ehastert@mayerbrown.com, or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

[1] https://www.mayerbrown.com/Employers-Should-Review-EmploymentContractorConsultant-Agreements-in-View-of-New-US-Trade-Secrets-Law-06-15-2016/

[2] The White House, May 11, 2016.