Seyfarth

Weathering COVID-19 With Your Trade Secrets and Customer Goodwill Intact

COVID-19 has changed the way most companies are currently doing business, from requiring remote work, to using new technology to meet the daily needs of their employees and customers, to furloughing and laying off employees and making other hard decisions to reduce costs. This new environment has made the risk of trade secret theft substantially greater. What steps can companies take, both inside the courts and outside, to protect their trade secrets?

This is a summary only; please contact a Seyfarth attorney for any legal advice or guidance needed.

Practical Tips for Protecting Your Trade Secrets During a Pandemic

Even during these unprecedented times, companies are required to take reasonable measures to keep their confidential information private. These tips are intended to give companies guidance on steps they can take to ensure they are taking the proper precautions with regard to their trade secrets.

Set Clear Expectations. Establish policies, procedures, and agreements with employees about how to protect confidential information. A strong policy will describe what type of information is confidential and what steps employees should follow to ensure its confidentiality.

Training. While a strong policy is essential, training in necessary to reinforce the policy. This is especially important with regard to the unique challenges that arise with employees working remotely. Employees need to understand how to use secure and encrypted services to transmit data, make sure they protect login credentials, and restrict access to information from third parties such as family members or roommates. In this era where the use of video conferencing has significantly increased, employees also need to be cognizant of what is in camera view so as to not expose confidential information.

Monitoring. Technologies should be in place to monitor usage of company data. One common sign that suggests possible trade secret theft is a high volume of data activity that is inconsistent with the employee's ordinary behavior. Other signs include email from an employee's work account to his or her personal account, use of unauthorized devices like USB thumb drives, or access to cloud storage sites.

Technical Infrastructure. Companies must ensure that they have the right technologies in place that allow employees to do their jobs while also protecting company information. Available technologies include requiring passwords to access computer systems and requiring employees to change passwords regularly, use of two-factor authentication, implementation of software with internal triggers to identify suspicious behavior, ensuring secure file sharing and video conferencing, and limiting access to sensitive information on a need-to-know basis.

Remote Security. This goes hand-in-hand with technical infrastructure. Make sure that your employees, especially those working remotely, are using secure networks to access company information and to communicate with each other and clients. If suspicious activity is identified, remote investigations can be performed to analyze network access, email activity and download history.

What *Not* to Do. Many businesses have moved to remote work for the first time and many did it within a matter of days or weeks. Now more than ever, companies need to protect their confidential information and not loosen security requirements for the sake of convenience or efficiency. Preventative steps are substantially more cost-effective than recovering stolen information. Consider a trade secrets audit to review and update your company's policies and ensure technologies are sufficient to protect company data.

Beyond Prevention: Additional Considerations for Protecting Trade Secrets

Beyond the preventative measures outlined above, what other steps do companies need to take to protect trade secrets? The pandemic has not changed the legal framework for enforceability of restrictive covenant agreements, although the current period of high unemployment may cause some courts to give such agreements a more discerning look. However, whether or not a particular restrictive covenant will be enforced does not mean that former employees can misappropriate trade secrets. Companies should be vigilant about protecting their confidential information and should be prepared to go to court if necessary. Although almost all state and federal courts are limited in some capacity at present, they are continuing to hear and decide trade secrets and restrictive covenant cases, often on an expedited basis. These types of cases are considered "emergency" or "essential" matters in most courts, and a significant number of courts have ruled on injunction applications in the trade secrets context in the last few weeks alone.

If the court near you is closed, there are still out-of-court actions that you can take such as conducting investigations, preparing cease and desist letters, and monitoring the employee's actions and your business in general. Companies can also explore alternatives to seeking emergency relief, such as switching to an alternate forum/court, stipulated injunctions, and expedited discovery and alternative dispute resolution. In addition, if emergency injunctive relief is not available due to court limitations, or is delayed or does not entirely remediate the harm, companies can still pursue money damages for any harm they suffer due to a misappropriation of their confidential information or a breach of a restrictive covenant. Damage can include lost profits, unjust enrichment, reasonable royalties, and exemplary damages and/or attorneys' fees. If a company is having liquidity problems as a result of the current economic downturn, or has a mandate from stakeholders to limit expenses so as to avoid layoffs, furloughs, or other cuts, or to maximize profits during a difficult economic time, litigation finance may be a good option. Most important, companies should stay vigilant and be ready to take prompt action when the courts reopen for business as usual.

Material is Summarized From a Presentation By:

Jeremy Cohen, Partner

Marcus Mintz, Partner

Erik Weibust, Partner