Articles + Publications | April 21, 2020

Locke Lord QuickStudy: Protecting Trade Secrets While Employees Work From Home During the COVID-19 Pandemic: Proactive Measures and Considerations for U.S. Companies

Locke Lord LLP

WRITTEN BY

Michael Wolak, III | Paul G. Nason

RELATED OFFICES

Dallas

The Heightened Risk from the "New Normal"

With the COVID-19 pandemic forcing companies to face unprecedented challenges, the shift to employees working remotely from home creates new risks and challenges regarding the protection of trade secrets and other confidential information. In the midst of this widespread and unfamiliar work-from-home dynamic, coupled with the uncertainty over when employees can safely return to regular office attendance, it is crucial that companies adjust to this "new normal" and implement and maintain effective measures to safeguard trade secrets.

Trade secrets can include many different types of information that give the trade secret holder an advantage over competitors, such as formulas, product specifications, software programs, source codes, algorithms, manufacturing methods, marketing and advertising strategies, sales methods, customer or supplier lists, and cost structures. For information to be protectable as a trade secret, the information must not be generally known or readily ascertainable to the general public, and it must derive economic value from its confidential nature. Additionally, the information must be the subject of a company's reasonable measures to maintain its secrecy, including efforts to prevent and mitigate unauthorized disclosure. Importantly, trade secret holders must be able to demonstrate that such measures were reasonable under the current circumstances, in particular, the remote working environment during this pandemic.

Proactive Measures to Minimize the Risk

The following are several proactive measures that companies should consider implementing to safeguard their trade secrets and minimize the risk of unauthorized disclosure during this work-from-home environment:

- Perform an audit to identify and inventory trade secrets. This is an opportune time to identify (i) what the company currently considers to be, or has designated as, a trade secret; (ii) whether any new or additional information should be designated as a trade secret; and (iii) who has access to trade secrets.
- Ensure that there is a formal written company policy implemented regarding the confidentiality of trade secrets and other sensitive business information that puts all employees on notice of their obligation to maintain the

secrecy of certain information. Consider having employees acknowledge their receipt and understanding of the company policy.

- Re-examine existing policies and procedures regarding the safeguarding of confidential information and trade secrets and determine whether any vulnerabilities need to be addressed and/or whether the policies and procedures need to be updated to account for working remotely. For example, companies should ensure that there are sufficient procedures in place regarding the protection of trade secret and other sensitive business information accessed and printed from home, including proper destruction of those hard-copies.
- Remind employees of existing or updated policies and procedures regarding the safeguarding of trade secret and other confidential information, including their ongoing obligation to maintain the secrecy of such information while working remotely.
- Remind employees subject to existing confidentiality or non-disclosure agreements of their ongoing obligations regarding trade secrets and other confidential information, and that such obligations are not waived or excused when working remotely.
- Ensure that all current employees with access to confidential information and trade secrets have signed a confidentiality/non-disclosure agreement. Ensure that all new employees that will have access to confidential information and trade secrets sign confidentiality/non-disclosure agreements at the beginning of their employment.
- Utilize a VPN network with multi-factor authentication and complex password protection for remote access to the company's network. Prohibit the use of public or insecure home networks and Wi-Fi for remote access.
- Consider temporarily restricting access to trade secret and other confidential business information to certain individuals to reduce the risk of inadvertent or unauthorized disclosure. At a minimum, ensure that employee access to trade secrets and other sensitive information is limited to a "need to know" basis.
- Consider the use of software programs that alert the company or its IT department when trade secrets and other confidential information are remotely accessed or downloaded, and that remind employees of their confidentiality obligations when they access such information.
- Train employees regarding how to identify fraudulent phishing and other malicious emails so they understand the importance of safeguarding confidential information and are encouraged to practice strong cyber-hygiene while working remotely. Remind employees to be vigilant and to expect a surge in fraudulent COVID-19-related emails and other malicious attempts to access the company's network. Designate a person or certain persons as the principal contacts for addressing any employee questions or concerns regarding the protection of trade secrets.
- Prohibit employees from downloading or sending confidential information or trade secrets to or from their personal devices, personal email accounts, and other unauthorized cloud-based services.
- Perform remote exit interviews for departing employees that require electronic certification that they are aware of their obligation to maintain the confidentiality of company trade secrets and other confidential information; that they complied with that obligation during their employment; and that they understand that any future violation of that continuing obligation could subject them to legal proceedings. Ensure that departing employees have returned all trade secret and other confidential information, as well as all company-issued laptops and devices. Establish a plan for the destruction of such information. Verify that the departing employee's access to all company networks and systems has been disabled.
- Confer with third-party vendors or other contracting business partners with whom you share trade secrets or other sensitive company information in the ordinary course of business. Reassess their existing policies and procedures for the safeguarding of such information and determine whether additional measures should be implemented. Ensure that all trade secret and other sensitive information is shared only under a confidentiality/non-disclosure agreement. Consider adding language making clear that the rights and obligations remain in full force and effect during the COVID-19 pandemic and any related exigencies.

Key Takeaways

A company's intellectual know-how is one of its most valuable assets, creating the ongoing need to vigilantly

safeguard and deter unauthorized disclosure of such information. The current work-from-home environment, coupled with the staggering number of layoffs nationwide, increases the risks of inadvertent disclosure and misappropriation, heightening the need for companies to implement additional measures to protect sensitive business information. Indeed, implementing such additional measures may be critical to a company's ability to successfully obtain legal relief to protect their trade secrets. Moreover, with more employees likely to work remotely even after the country reopens, and the risk of a second COVID-19 wave that could result in the issuance of new shelter-in-place orders next Fall or Winter, taking proactive steps now will help companies be prepared for this new reality and uncertainty.

RELATED INDUSTRIES + PRACTICES

- Labor + Employment
- Litigation + Trial