JENNER&BLOCK

Trade Secret and Restrictive Covenants

Safeguarding Company Trade Secrets in a "Work from Home" Environment

By: Debbie L. Berman, Andrew W. Vail, Kevin J. Murphy and Amit B. Patel

In response to the unprecedented COVID-19 outbreak, many state and local governments have issued shelter-in-place orders. As a result, millions of Americans—most of whom have spent their careers working from an office—are now working from home (WFH) for the first time. The sudden shift to widespread WFH poses unique challenges for businesses seeking to protect their trade secrets and confidential information. Companies must be vigilant in taking steps to train employees about potential security concerns for trade secrets and other confidential information in the WFH environment or risk losing protection over such information.

While many companies diligently train their employees on how to protect their trade secrets and confidential information, the training often focuses on securing such information in the workplace. WFH, however, presents a whole host of potential unique challenges to protecting trade secrets and confidential information, many of which the average worker might never contemplate despite having been trained on workplace-related risks. Federal and state laws afford protection for trade secrets only when the trade secret owner has taken reasonable measures to safeguard the trade secrets.[1] Businesses that fail to take such reasonable steps during WFH may later find that these trade secrets have lost their protected status.

Companies, therefore, should reevaluate the protocols that they have instituted to protect their trade secrets and confidential information to determine whether they are "reasonable" in the current environment. The best approach depends, of course, on the business and the nature of its trade secrets and confidential information. What is reasonable for one business and its trade secrets might not be sufficiently reasonable for another. But, there are two steps that businesses should consider taking now while WFH is the rule as opposed to the exception to try to maximize the likelihood that their trade secrets and confidential information will be afforded protection.

First, businesses should review their existing confidentiality policies to make sure they adequately address concerns that could arise in a WFH environment. Courts routinely consider company confidentiality policies in determining whether a company has taken reasonable steps to protect a trade secret.[2] The sudden nature of the COVID-19 outbreak may have left businesses with confidentiality policies that do not contemplate an entire workforce working remotely. Businesses should review and revise their policies to address any previously unaddressed concerns presented by a largely remote workforce. Some examples of the potential confidentiality challenges presented by WFH and policies that businesses should consider implementing, if needed, to help safeguard their trade secrets and confidential information include:

- For many workers, WFH necessitates working in close proximity to others who are not entitled to trade secret or confidential information access, such as family members. Businesses should implement policies directing employees not to access or discuss trade secrets or confidential information in the presence of others in their homes, regardless of whether the worker believes their household members do not pose any risk of misappropriation.

- Protecting hard-copy trade secrets or confidential materials can be more difficult outside a business's premises, such as inside private homes that the business does not control. To help protect these materials, companies should consider implementing policies: (1) prohibiting the

printing or duplication of confidential materials absent a specific need; (2) requiring employees to maintain any confidential materials in a secure location and prevent others from accessing it; and (3) barring employees from disposing of confidential materials in their home trash and instead requiring them to retain the materials in a secure location so that they may later be disposed of securely by the business.

- Remote workers likely will be accessing the business's information through their home internet connections and personal wireless networks that the business does not control. Businesses should ensure that their technical infrastructure, and particularly those components that provide remote access to business information, do not depend on the workers' home networks to be adequately secured. Home networks can be comprised of a variety of devices, including obsolete devices or those running out-of-date software that might or might not be password-protected or adequately protected by a strong firewall. Our colleagues have analyzed some minimal cybersecurity measures businesses should consider, which is available here.[3]

- Remote workers may be more likely to take shortcuts accessing confidential materials, including sending confidential materials by email to personal email accounts, saving confidential documents locally or using personal cloud storage for confidential business information. Businesses should consider implementing clear policies barring employees from engaging in these practices.

- Given the impossibility of in-person meetings, employees are turning in mass numbers to videoconferencing platforms, like Zoom, to hold internal and external meetings. Such videoconferences have become a new target of cybercriminals, and security bugs have been exposed that could leave confidential company information at risk. To protect trade secrets and confidential information, companies should, at a bare minimum, require all Zoom meetings to be password-protected and consider additional security measures like encrypting any shared data, locking meetings after they begin and only allowing individuals with a certain e-mail domain to join.

Second, in addition to reviewing and updating confidentiality policies, businesses should remind their workers of their confidentiality obligations through a written notification, and the reminder should specifically include any additional issues raised by WFH conditions, if needed. Businesses should consider whether to require a written confirmation from their employees of receipt and understanding of their obligations. Courts have recognized that reminding employees about their confidentiality obligations, including the proper use and handling of trade secrets, can support the protection of trade secrets.[4] The current environment affords businesses an opportunity to re-train their workers on confidentiality obligations, emphasize the importance of complying with these obligations and explain to workers how those obligations apply in a WFH environment. These communications—which can be tailored to different groups of workers, if appropriate—should explain, among other things, what constitutes trade secrets or confidential business information as well as the workers' confidentiality obligations as to these documents. They should also identify, if possible, a representative that workers can contact with questions regarding their confidentiality obligations while WFH. To the extent any independent contractors, vendors or other third parties also may access a business's trade secrets or confidential materials, there is a similar opportunity to remind these parties of their confidentiality obligations as well.

Updating confidentiality policies, if needed, and communicating with workers regarding their confidentiality obligations are steps businesses should consider taking to try to maximize the likelihood that their trade secrets and confidential business information remain protected while their workers work remotely. Jenner & Block lawyers have significant experience working with their clients to ensure that their trade secrets are safeguarded and are available to assist with any additional questions or concerns.

Conscious of the human, operational and financial strain that coronavirus is placing on businesses and organizations worldwide, Jenner & Block has assembled a multi-disciplinary Task Force to support clients as they navigate the legal and strategic challenges of the COVID-19 / Coronavirus situation.

For additional information and materials, please visit our COVID-19 / Coronavirus Resource Center.

Click here to visit our COVID-19 / Coronavirus Resource Center

[1] *See generally* Defend Trade Secrets Act, 18 U.S.C. § 1839(3)(A) (requiring, for protection of a trade secret, that the owner "has taken reasonable measures to keep such information secret"); Uniform Trade Secrets Act, § 1(4)(ii) (adopted by most states) (requiring, for protection of a trade secret, that the owner has taken "efforts that are reasonable under the circumstances to maintain its secrecy").

[2] *See, e.g.*, *AirFacts, Inc. v. de Amezaga*, 909 F.3d 84, 97 (4th Cir. 2018) (holding that company's confidentiality policy restricting access to electronic documents contributed to a finding that the documents were trade secrets); *ATS Grp., LLC v. Legacy Tanky & Indus. Servs., LLC*, 407 F. Supp. 3d 1186, 1199 (W.D. Okla. 2019) ("Some courts have found confidentiality policies to be reasonable efforts to maintain secrecy when combined with internal information classification and control guidelines.").

[3] https://jenner.com/library/publications/19650

[4] *See, e.g.*, *Stampede Tool Warehouse, Inc. v. May*, 272 Ill. App. 3d 580, 587 (1st Dist. 1995) (citing "constant reminders [to employees] about the confidentiality of [customer] lists" as factor in upholding trade secret protection).

Contact Us

Debbie L. Berman

dberman@jenner.com | Download V-Card

Andrew W. Vail

avail@jenner.com | Download V-Card

Kevin J. Murphy

kmurphy@jenner.com | Download V-Card

Amit B. Patel

apatel@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

Debbie L. Berman

Co-chair
dberman@jenner.com
Download V-Card

Brent Caslin

Co-chair
bcaslin@jenner.com
Download V-Card

Andrew W. Vail

Co-chair
avail@jenner.com
Download V-Card