PUBLICATION

Tips for Trusting Teleworkers with Trade Secrets

July 16, 2020

As more and more American workers are logging into their jobs remotely, many employers have been forced to enact teleworking policies on a massive scale. Some of these work-from-home policies may have been implemented in a haphazard way so that employees could begin working remotely within a matter of days. The need for speed in sending employees home may have left some employers without time to consider the potential impact of massive-scale teleworking on a company's protected confidential information. Due to the increased risk that employees may be able to expose confidential trade secrets to unauthorized individuals based on the nature of remote working, it is important that employers remain vigilant in protecting confidential and trade secret information.

Efforts to Maintain Secrecy

To protect trade secret information, employers need to understand what constitutes a trade secret in the first place. Trade secrets are *not* information that is generally known to the public or can be easily ascertained by others. For example, in Tennessee, one of the factors courts will analyze to determine the existence of a trade secret is the extent to which the employer has taken measures to protect the secrecy of the information. In many states, the definition of trade secret is similar to the definition provided in the Uniform Trade Secrets Act, including examining whether the information "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy." As the Tennessee court of appeals noted in *Wright Medical Technology, Inc. v. Grisoni*, "the extent to which the information has become available outside the confidential relationship is significant. To constitute a trade secret, it must be difficult for anyone outside the confidential relationship to acquire the information by proper means."[1]

To the extent courts face questions regarding the protection of trade secret information in the future based on actions taken during the COVID-19 pandemic, it will be important for employers to demonstrate additional steps taken to protect the confidential nature of any trade secret information utilized by teleworkers. With so many employees working from home around family members, roommates, and relatives, employers need to be aware of the precautions they should take to protect trade secrets and other confidential information, such as financial or personal health information.

Strong Policies in Place

One of the first things employers should do is make sure they have robust policies and procedures in place for protecting confidential information and trade secrets. Such policies can inform employees of their obligation to protect trade secrets and remind them of what information the company considers to be confidential trade secret information.

In addition, due to the widespread nature of workplace changes in the current crisis, it is important that employers dust off and revise any teleworking policies they may have or adopt new policies that contemplate the sweeping changes that may be taking place. A teleworking policy can outline measures employees should take to protect company equipment as well as company trade secret and confidential information.

Consider Asking Employees to Sign Confidentiality Agreements

Employers who do not have confidentiality agreements or restrictive covenant agreements with their employees may consider having employees sign off on policies that acknowledge their obligations to protect

the company's confidential and trade secret information. Employers could also ask employees to sign non-disclosure and confidentiality agreements that comply with state law. Some states, such as Tennessee, allow employers to ask employees to sign such agreements during the course of employment without any additional consideration beyond the consideration of continued employment.

Make Sure Electronic Security Measures Are in Place

In addition to having detailed policies in place informing employees of their obligations to protect company information while telecommuting, it is important that employers consider the security of their IT systems. Companies can establish a Virtual Private Network (VPN) to protect sensitive information. Employees can also be informed that they should not store company information and documents on personal computers or personal electronic devices. Keeping company information on company-owned computers can reduce the risk that the information gets into the wrong hands.

Password-protected networks can also limit access to those who have a need for the information within the company. Even among employees, companies can choose to limit access to certain documents and information to particular groups or teams. For example, if a company is protecting strategic business plans related to certain key clients as trade secrets, then it can be helpful to demonstrate to a court that the sensitive information was restricted to the sales team and managers involved in working directly with the client or who otherwise had a need for access to the plans. These rules should not change due to an employee's need to telework.

Provide Training to Employees Regarding Security Measures

Good training of employees on the sensitive and confidential nature of company information can go a long way in helping employees understand the importance of taking precautions to protect such information. Employees who are working from home should be informed that they should lock their computers when they are not in their home offices. They should also make sure they do not leave company information out in plain sight of household members or in view of computer cameras during video calls. Sensitive information should be subject to a company's normal shredding rules, and employees should seek to limit printing documents at home. Home offices should be locked when not in use if sensitive and confidential information is stored there. Employers should also caution teleworkers not to discuss confidential information in areas of the home where their conversations could be overheard by electronic virtual assistants, such as Amazon's Alexa, Google Assistant, or Siri.

Plan for Termination Precautions

When teleworking employees terminate their relationships with their employers, there should be procedures in place for the return of all company-owned property. In addition, employers may ask employees who are leaving to acknowledge that they have returned all company property and are not retaining any copies of company information. In these days of uncertain employment, including layoffs and furloughs, it is critical that employers have the means in place to ensure that terminated employees do not retain company property and information or use such information to create competing businesses. If a former employee does try to compete with the company and it becomes necessary to resort to litigation, it will be important to demonstrate to a court all the measures the company took to secure its trade secret and confidential information.

Bottom Line

When combined together, strong policies, training, security measures, and procedures for return of company property can all contribute to reducing the likelihood that employees will jeopardize the secrecy of trade secret information through their actions.

[1] 135 S.W.3d 561, 589 (Tenn. Ct. App. 2001).