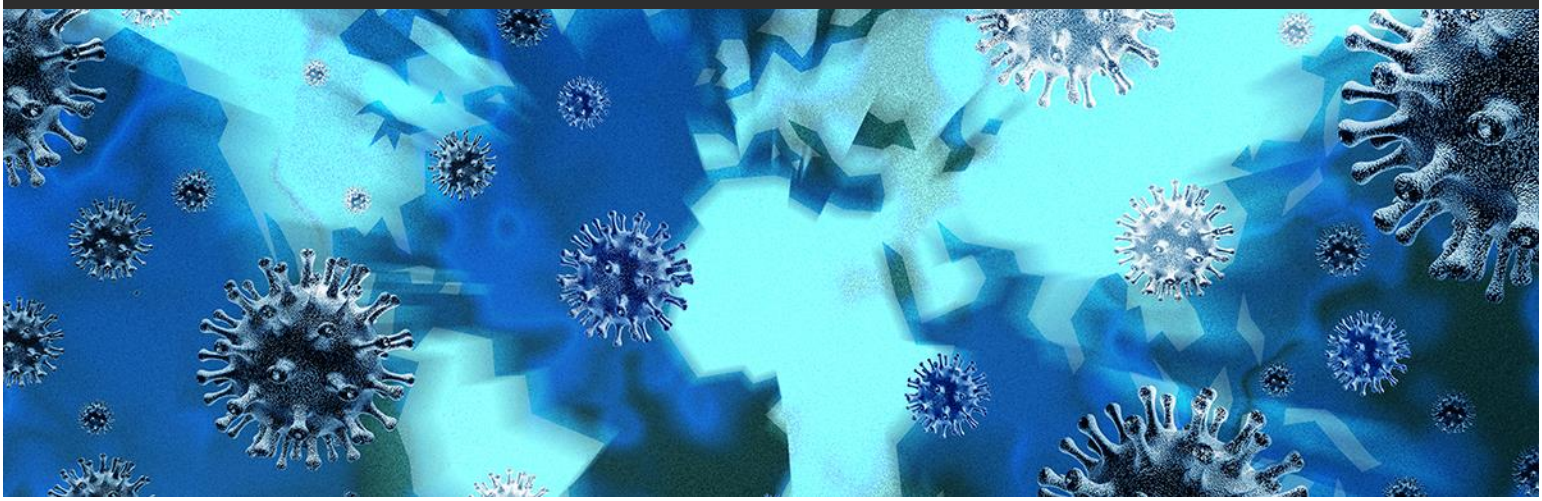
GT GreenbergTraurig

Alert | Health Emergency Preparedness Task Force: Coronavirus Disease 2019



March 30, 2020

Trade Secret Protection and Remote Work: Considerations for Employers

Because of the Coronavirus Disease 2019 (COVID-19) pandemic, certain states and cities are enforcing shelter-in-place orders. As a result, some companies have instituted protocols for their employees to work remotely. Other companies may already have had remote-work options that have been relaxed or revised due to the pandemic.

With this sudden proliferation of remote work, companies may consider taking additional precautions to protect valuable trade secrets and proprietary information. Such steps may reduce the chances of theft of trade secrets during remote work. They may also serve to position companies to continue to keep their information protected by trade secret laws by taking "reasonable efforts" to ensure the information remains "secret." However, courts operating with the benefit of hindsight after this crisis may conclude that the surprise transition to and rapid expansion of remote workers are not valid excuses for not having proper protocols in place.

There is no single approach to maintaining status as a trade secret and protecting against misappropriation, and each company should assess the risks of misappropriation and disclosure as well as the practical steps that reasonably can be taken to protect its information. Companies may wish to factor the below considerations into their deliberations regarding trade secret protection during remote-work, including with respect to remote access to information, employees working on proprietary or trade secret information while at home, and efforts to effectively communicate with employees about remote-work.

- Express and repeated statements of company policy that during any remote-work situation, employees are not permitted to disseminate any trade secret or proprietary information to anyone who is not authorized by the company to receive that information, that it is each employee's obligation to take all possible steps to keep secure all company information during remote work, and that employees must immediately report any instance where the employee knows or has reason to believe that any company information has been improperly disclosed or accessed. Employers may want to consider sending out a specific notice, asking employees to acknowledge it, and following up to make sure that it is acknowledged.
- Revising non-disclosure or proprietary information agreements to specifically apply to remote work, and requiring execution by employees before permitting remote access or remote discussion of proprietary information. Where remote access has already been permitted, consider conditioning continued access on electronic signature.
- Reminding employees of the proliferation of malware, phishing, and other scams, especially during this time of crisis. Employees who have access to proprietary or trade secret information should take reasonable steps to confirm the identity of anyone with whom they may be electronically or remotely communicating about proprietary or trade secret information, especially before transmitting any such information.
- Establishing a designated point of contact person or persons at the company to address questions about remote access and to receive information about any suspected incident of improper access to or accidental disclosure of trade secret or proprietary information, and repeatedly disseminating this point of contact information to the workforce.
- To the extent feasible with the assistance of IT staff, using two-step or multi-factor authentication features for any remote access to the company's trade secret or proprietary information, through secured connections to the company's network, such as VPN or other secured portals. Have IT monitor and catalog large or significant remote access or downloading of information to better guard against theft. Commercial companies can be retained to assist with that analysis.
- Requiring that all employees who are working remotely and using personal or home WiFi to secure those points of access with a password.
- Requiring that any employee who needs to communicate about or transmit trade secret or proprietary information do so only through the secured servers or drives, like an FTP site, with credentials limited to those who are permitted access to proprietary information. If that is not feasible, requiring that any discussion or transmission of trade secret or propriety information occur only through the company's authorized email accounts with encryption, and not through personal email, text or SMS, communication applications, or social media platforms of any kind, even with other employees who are authorized to discuss or receive proprietary or trade secret information.
- Requiring employees during remote-work situations to limit review of trade secret or proprietary information to company-issued laptops or any other devices which the company's IT department can remotely access, and requiring employees to, with the assistance of IT, enable passwords for access to such devices and have their screens lock automatically after a very short interval of time without activity.
- Requiring, if possible, that employees with access to proprietary information only work in rooms that can be secured or locked, or if not feasible, to secure their laptops and any trade secret or proprietary information in a locked cabinet or space when not in use. Requiring that employees work in an area that is secluded from view by cohabitants or others who may be present at the remote-work location.

- Instructing employees not to print or copy materials while working remotely or, if this occurs, to safeguard any printed or copied materials in some secure space at the remote-work location until the employee can return those copies to their place of work.
- To the extent employees may be using video-conferencing to discuss proprietary or trade secret information, having employees avoid using any system or service that is susceptible to hacking or other unauthorized access. Attendance should be taken at the outset and, IT may work to catalog all remote-access participants. Similar steps may be taken for audio-conference calls. Additionally, consider requiring that such conferences not occur in close proximity to any home audio services that may inadvertently record such discussions about proprietary or trade secret information.
- Reviewing agreements with vendors who host or facilitate access to companies' proprietary or trade secret information and revising relationships with those entities to ensure they are taking steps to safeguard access to companies' trade secret or proprietary information.
- Regularly checking in with employees to ensure not only their compliance with reasonable steps, but to avoid employee feelings of isolation or neglect that could lower morale or loyalty to the company, and thus increase the risk of employees letting down their guard or actively engaging in misappropriation.

In situations of suspected trade secret theft, companies should immediately contact law enforcement, including the Federal Bureau of Investigation, as trade secret theft is a priority for federal and state agencies.

This list of considerations is not exhaustive, and the current situation continues to evolve. Steps taken today may not be sufficient over time, and companies should reassess over the coming weeks and months what "reasonable efforts" may be necessary to continue to protect against trade secret theft, and to avoid loss of trade secret status for their proprietary trade secret information.

For more information and updates on the developing COVID-19 situation, visit GT's Health Emergency Preparedness Task Force: Coronavirus Disease 2019.

Authors

This GT Alert was prepared by:

- Kurt A. Kappes | +1 916.868.0650 | kappesk@gtlaw.com
- Todd A. Pickles | +1 916.868.0628 | picklest@gtlaw.com