Holland & Knight

10 Practical Tips for Employers to Safeguard Their Trade Secrets During COVID-19

April 20, 2020

Holland & Knight Trade Secrets Blog

Nipun J. Patel | Paul Bond | Steven E. Jedlinski | Mark S. Melodia | Tracy Zurzolo Quinn

As a result of both mandatory government restrictions and voluntary safety measures to combat the spread of coronavirus (COVID-19), many companies have transitioned all or part of their workforce to a remote working environment. Others have been forced to reduce staff or institute employee furlough policies, all within a short timeframe. These unprecedented and challenging circumstances pose a unique risk for any company with trade secrets. In some cases, companies had to act quickly to provide remote access to their systems, such that trade secrets now can be accessed by employees who are working remotely and may be accessible to employees who recently departed from the organization.

The protection of trade secrets is often vital to a company's business strategy, good will and the ability to maintain competitive advantages that have been developed through substantial investment in research and personnel over time. By definition, a trade secret's economic value depends on maintaining its secrecy.

Even prior to the pandemic, courts saw an uptick in trade secrets litigation as a result of a strong labor market that incentivized the voluntary mobility of employees, as well as the passage of the federal Defend Trade Secrets Act (DTSA) of 2016, 18 U.S.C. § 1836, *et seq.* Under the DTSA and state analogs, an essential element for stating a claim for trade secret misappropriation is proving that the company has taken "reasonable measures" to keep secret the information it wishes to protect and deems a "trade secret." The reasonableness of measures taken to protect trade secrets is often viewed on a sliding scale. It remains to be seen whether that scale will be changed in light of the unprecedented nature of the pandemic. Employers who actively manage and scrutinize their policies and practices may mitigate the risk of waiving trade secret protections by considering the following list of practical tips.

1. Remind employees of confidentiality policies and any security protocols generally associated with the access and use of sensitive business information and documents. If existing policies do not address or are unclear about protocols for accessing business information remotely or from personal devices, update them and provide appropriate training to employees. Emphasize that safeguarding information is more critical now than ever.
2. Retrain employees remotely on the importance of nondisclosure and confidentiality policies. Have employees acknowledge receipt and certify their understanding of the policies.
3. Remind and expressly advise remote workers that discussions or viewing of sensitive business information should occur in an isolated part of the home, outside the purview of others – even family.
4. Minimize to the extent possible the use of personal devices, email accounts, communication services, social media or other cloud-based services that may lack critical information security features. Remind employees that all work-related communication should be conducted via company-authorized software and systems, and ensure that appropriate training is available for all who need it.
5. Remind and train employees who use video conferencing services such as Zoom to discuss sensitive topics to use the services' security features, such as enabling passwords for meetings, auto-muting of participants, the use of randomly generated meeting IDs and the disabling of any auto-recording.
6. Institute two-factor authentication and encryption measures, if they have not already, for information technology personnel before remote workers can access sensitive documents and information remotely. Such access should be

limited to employees with a need to know the particular information.

7. Train and refresh employees on the importance of recognizing and avoiding phishing scams.
8. For departing employees who had access to sensitive business information, ensure that exit interviews are conducted (even if done remotely) that expressly demand the return of any tangible sensitive business information and any company-issued computers, storage media or other equipment. For intangible items that may have been retained through memory, remind employees that disclosure remains prohibited under company policies.
9. For departing and furloughed employees, remove access to the company's network immediately and ensure that audits are conducted of returned company-issued devices to confirm that sensitive information has not been transferred, misused or retained.
0. For furloughed employees, remind them that their directive to "not work" during the furlough period includes not attempting to seek access to the company's network or information, following applicable confidentiality and nondisclosure policies, and a reminder that the company remains the owner of any intellectual property created during or as a result of the employment.

For questions, comments or additional information on considerations for protecting trade secrets in the age of COVID-19, please contact the professionals who contributed to this article: Nipun Patel (restrictive covenant, trade secret and employment litigation); Paul Bond and Mark Melodia (data security, strategy and litigation); or Steven Jedlinski and Tracy Quinn (intellectual property protection and litigation).

DISCLAIMER: Please note that the situation surrounding COVID-19 is evolving and that the subject matter discussed in these publications may change on a daily basis. Please contact your responsible Holland & Knight lawyer or the author of this alert for timely advice.

Nipun J. Patel is a partner and trial lawyer in Holland & Knight's Philadelphia office who focuses his practice on a wide variety of complex litigation matters.

215.252.9527 | Nipun.Patel@hklaw.com

Paul Bond is a litigation attorney who focuses his practice in the areas of data security, privacy and artificial intelligence. Mr. Bond helps clients make the best use of new technologies, including opportunities for automation, while identifying and managing the relevant risks.

215.252.9535 | Paul.Bond@hklaw.com

Steven E. Jedlinski is a trial lawyer with a national practice litigating all types of complex intellectual property disputes. He is widely recognized and sought after for his experience with patent and trade secret matters. His patent experience includes litigating and counseling client’s regarding the myriad of unique and ever-changing issues surrounding standard essential patents (SEPs) and design patents.

312.715.5818 | Steven.Jedlinski@hklaw.com

Mark Melodia is a privacy, data security and consumer class action defense lawyer in Holland & Knight's New York office and serves as the head of the firm's Data Strategy, Security & Privacy Team. Mr. Melodia focuses his practice on governmental and internal investigations, putative class actions and other "bet-the-company" suits in the following areas: data security/privacy, mortgage/financial services and other complex business litigation, including defamation.

212.513.3583 | Mark.Melodia@hklaw.com

Holland & Knight

Tracy Quinn is an intellectual property litigator in Holland & Knight's Philadelphia office. Ms. Quinn focuses her practice on patent, trademark, trade dress and copyright infringement disputes, trade secret litigation and other technology-related matters.

215.252.9522 | Tracy.Quinn@hklaw.com