crowell moring

CLIENT ALERT

Trade Secret Protection During the COVID-19 Pandemic

Apr.03.2020

The COVID-19 pandemic presents unique and unprecedented challenges to the ongoing need to protect confidential information and trade secrets. The massive business disruptions that enterprises of all kinds now face include (1) entire workforces forced to work remotely, accessing and using confidential information and trade secrets from home; (2) exigent circumstances created by the cessation or substantial slowing of commercial activity that may result in the disclosure of confidential information or trade secrets to third parties outside normal procedures; and (3) the off-boarding of remote employees who are accessing confidential information and trade secrets remotely.

Trade secret protection may not be the immediate priority of a business facing massive business disruptions, but taking reasonable steps now to protect the security of trade secrets and confidential information is critical to the preservation of these valuable assets when this crisis is over. Trade secret law – both federal and state – requires that a trade secret holder take reasonable measures under the circumstances to protect trade secrets.[1] Reasonable measures relate not only to prevention of unauthorized disclosures, but also the minimization of the impact of any such disclosures after they occur, and these measures must be reasonable now under the current exigent circumstances.

As explained below, many of the major confidentiality risks associated with business practices during the COVID-19 pandemic are identifiable and actionable. The measures referenced below are examples of actions that reflect the needed focus on trade secrets and confidentiality and should serve as a guide in adopting reasonable confidentiality measures during the pandemic. What constitutes reasonable measures is dependent on at least the nature of a business's critical trade secrets, and the circumstances that business now faces, but the following four-step analysis should help guide most businesses on the adoption of appropriate measures.

1. Identify High Value, High Risk Areas.

Prioritize your security measures by broadly identifying the high value and high risk areas of your business, where the confidential information and trade secrets are most important to protect or are most vulnerable during the pandemic, including:

- High value/risk business divisions, departments, or teams.
- High value/risk products or services.
- High value/risk servers, networks, drives, computers or other media.

Once you have identified your high value and high risk areas, you will be better equipped to select the protection measures that make most sense and identify the personnel who require the most direct and urgent counseling for the implementation of those measures.

2. Address the Risks Associated with Remote Work.

Remind your employees that working remotely does not create any exception to existing confidentiality and non-disclosure agreements or company policies, manuals, or practices. Consider reminding employees that when working remotely they should:

- Limit printing of confidential information, and restrict access to any such printed information within their homes, just as they would in the office (e.g. in locked rooms or storage areas).
- Not send or save confidential information to their personal devices (e.g. personal email accounts, cloud-based services, external storage devices, printers, etc.).
- Not allow others (e.g. friends, family, smart devices with microphones) to hear their confidential discussions.
- Be aware of the new surge of fraudulent cybersecurity threats seeking valuable information under false claims of authority or false offers of relief or information relating to the COVID-19 pandemic.

If you have not yet done so, designate an individual or team to handle confidentiality inquiries, and encourage employees to ask questions regarding how to maintain confidentiality while working remotely.
Also consider implementing or updating the following security measures, which may warrant additional attention in the context of a remote workforce:

- Limit and monitor remote access to electronic networks and files through: (1) multi-factor authentication; (2) encryption; (3) complex password protection; and (4) the maintenance of access logs.
- Institute pop-up messages that remind employees when they are accessing confidential or trade secret information.
- Maintain an inventory of company devices and information that employees have taken off site (consider asking employees for this information now if it is not yet documented).

In implementing or updating these protections, it will be necessary to work with and consult your IT team for an understanding of the scope of employees' electronic access and the corresponding security measures.

3. Limit and Track Your Third-Party Disclosures.

During the pandemic, your business may receive urgent or unexpected requests, demands, or opportunities to disclose confidential information or trade secrets to a third party – or receive such assets from a third-party. It may be tempting to do so outside the terms of an existing confidentiality agreement, or without obtaining an appropriate confidentiality agreement. Counseling under these circumstances is critical to advise employees, including key members of the business, that securing critical trade secrets and confidential information remains a high priority notwithstanding the demands or opportunities the business now faces.

Identify and make available to the business a template confidentiality agreement that can be used as consistently as possible, where appropriate, in advance of disclosing or receiving valuable confidential business information. Having this template on hand should streamline the process for any emergent opportunities, and the uniformity will provide you a clear understanding of the terms in place for all of your disclosures (or receipt of third-party disclosures) during the pandemic. Consider adding

language to your template explicitly emphasizing that the rights and obligations established therein apply with equal force during the COVID-19 pandemic and through any related exigencies.

Keep in mind that many confidentiality agreements include an exception for the disclosure of confidential information required by law, regulation, court order, or other legal process. These exceptions often require advance notice of any such required disclosure, and that the party whose information is being disclosed be given time to seek appropriate relief or protection. Check your template and your existing agreements for any such exception. Be mindful of the rights and obligations they create, and their potential impact on your contractual relationships during the pandemic.

To the extent your business shares confidential information or trade secrets with third parties – or third parties do so with your business – exercise additional care during the pandemic to document and track the disclosures, including the following key information:

- What information was shared?
- When?
- With whom?
- For what purpose?
- Under what agreements and restrictions?
- Was the information returned or destroyed as required after the project was complete?

Maintaining this information should be useful: (1) to ensure that third parties protect your information; and (2) as proof in any later dispute over the unauthorized use of your information. It also may minimize the risk of successful claims by third parties over the alleged unauthorized use of their information.

4. Adapt Your Off-Boarding Procedures.

It is always important to ensure that employees being off-boarded return all confidential and trade secret information before their departure, and that they be reminded of their continuing obligations to protect, and not improperly use, that information. Now the need for adequate off-boarding is greater, yet the circumstances now make the process more challenging. Off-boarding can be particularly challenging during the pandemic, given that many employees may be off-boarded in a short period of time, and exit interviews, execution of documents, and the return of company property cannot be conducted in person as usual. However, many off-boarding procedures can be performed remotely, including:

- Disabling access to company systems, electronic devices, and accounts, and monitoring any unauthorized access thereafter;
- Conducting an exit interview by video or phone.
- Requiring e-signature of documents establishing the off-boarded employee's continuing confidentiality obligations.

For parts of the off-boarding process that absolutely cannot be executed during the pandemic, keep clear records of what remains outstanding for each employee, so those items can be addressed as soon as practical. In particular, take inventory of all company property and information the employee has taken off site, and confirm this inventory with the employee during the exit interview. Establish a plan for the secure destruction and/or return of this property and information as soon as possible.

Using the four steps above as a framework, businesses should vigilantly adopt measures tailored to the present circumstances in order to protect valuable trade secrets and confidential information, deter misappropriation, and minimize the risk of third-party misappropriation claims.

---

[1] The Uniform Trade Secrets Act includes the language "under the circumstances," and while the Defend Trade Secrets Act does not, courts have interpreted both laws to take account of the circumstances. *See, e.g.*, *Xavian Ins. Co. v. Marsh & McLennan Companies, Inc.*, No. 18CV8273(DLC), 2019 WL 1620754, at *5 (S.D.N.Y. Apr. 16, 2019) ("Efforts reasonable under the circumstances," does not appreciably differ from the DTSA's "reasonable measures" standard."); *PNR Mktg. Sols. LLC. v. Fun Flicks of S. California, No. SACV1801600AGKESX*, 2019 WL 3220019, at *3 (C.D. Cal. Mar. 6, 2019) ("[B]oth statutes use essentially the same definition: A trade secret is information that (1) derives its economic value from not being generally known, and (2) is subject to reasonable measures of secrecy by its owner under the circumstances.").

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

James K. Stronski
Partner – New York
Phone: +1 212.895.4217
Email: jstronski@crowell.com

Anne Elise Herold Li
Partner – New York
Phone: +1 212.895.4279
Email: ali@crowell.com

Robert B. Kornweiss
Associate – New York
Phone: +1 212.803.4045
Email: rkornweiss@crowell.com