MAINTAINING TRADE SECRETS AMID THE COVID-19 PANDEMIC

by Steven A. Caloiaro and Caleb Green

Over the last few months, the widespread transmission of the coronavirus disease of 2019 (COVID-19 or the "coronavirus") has prompted immediate action from employers and businesses throughout the United States. As of publication, 42 states have issued statewide stay-at-home orders, limiting several business operations. While many companies have ceased public- facing operations, many remain operational to provide essential and public health services and are making abrupt changes to their work environment, resulting in an unprecedented increase in employees working remotely for the first time. Additionally, several organizations are scrambling to make employment and corporate adjustments, in response to the changing landscape and effects of the coronavirus crisis.

s a result, companies are also facing novel challenges for safeguarding their trade secrets and confidential business information as many employees are forced to work remotely from home. Meanwhile, many of these same businesses are shifting away from their normal business operations and are creating new products to address public needs in the face of the COVID-19 pandemic, including manufacturing hand sanitizer and personal protective equipment ("PPE"). Finally, some unfortunate companies are facing the complicated reality that layoffs and personnel changes might be necessary to save their businesses.

Crises like COVID-19 can make or break a company's intellectual property assets. Accordingly, as businesses scramble to navigate the changing legal landscape and adopt alternative methods of operation, they should remain vigilant and take the proper precautions necessary to maintain valuable trade secrets and confidential information. While addressing business disruptions due to COVID-19, businesses should take reasonable steps now to ensure the preservation of intellectual property rights once this pandemic is over.

WHAT IS A TRADE SECRET

A trade secret can be any information that derives financial value from being secret, provided the owner takes reasonable steps to protect the information. Trade secrets have no expiration date so long as they remain secret, and therefore they tend to create perpetual monopolies. Courts have protected various forms of information under this broad definition, s uch a s fi nancial, bu siness, scientific, tec hnical, eco nomic, or engineering information. Coca-Cola's secret formula, the secret recipe for Kentucky Fried Chicken, the Google search algorithm, Tinder's dating software, and even client lists are all examples of court recognized trade secrets.

Trade secret protection is a counterpart to patent protection. While patents require the inventor to provide detailed disclosures about the invention in exchange for the right to exclude others from practicing the invention for a limited period, trade secrets require complete secrecy. Furthermore, trade secret protection vests instantly once information derives financial value from its confidentiality, whereas patent protection requires a rigorous application and vetting process.

Throughout the ongoing pandemic, companies may experience urgent and unexpected demand as they scramble to adjust and respond to the effects of COVID-19. In fact, some companies may fi nd new opportunities to introduce products or pivot their business operations to take advantage of these new business opportunities, address public health issues, or supplement growing demand. However, during this time of transition, company confidential information and trade secrets may be at an increased risk of exposure. As such, company leadership should implement proper measures to ensure protection of its intellectual property during and post-pandemic.

Creating and protecting trade secrets throughout the current pandemic and post-coronavirus requires a continuous process of constant vigilance to ensure the secrecy of your new process, method, or formula. A key step to establishing trade secret rights is limiting the knowledge to key employees, and then having key employees, who have access or have knowledge of key trade secrets, sign a confidentiality agreement or non-disclosure agreement ("NDA"). Additionally, companies should consider having employees sign non-compete agreements to ensure their competitors do not steal their new trade secret assets and projects amid employee turnover during the COVID-19 crisis.

Each state has adopted its own trade secret protection laws, which provide a different degree of protection. Accordingly, business leaders should consult with an attorney to determine their trade secret rights and ensure they are taking the proper steps to preserve their rights therein.

DESTRUCTION OF TRADE SECRET

As mentioned above, trade secrets can be created instantaneously. However, as quickly trade secret protection can be established, it can be destroyed if proper measures are not taken. Trade secrets, unlike other forms of intellectual property, can be destroyed by inadvertently failing the keep them secret. As such, during these unprecedented times, companies should exercise prudence and take the necessary precautions to protect proprietary information from third parties and competitors.

Risks Associated with Remote Working

Several employers are providing employees with remote access options, in response to the effect of COVID-19, enabling them to work outside of the traditional corporate environment. While providing a work-from-home option for employees is a convenient and necessary measure to reduce transmission of the coronavirus, business leaders must be aware of the risks that remote systems pose to trade secrets. Remote access relies on the exchange and transfer of information and data, typically over the Internet. While teleworking, employees are often transmitting, accessing, and handling sensitive information, including company trade secrets, customer personal information, or confidential financial data. With more employees relying on technology to work remotely and access proprietary information, hackers are increasing their attempts to exploit sensitive data through company information systems.

For example, in 2018, over 10 years of confidential car manufacturing trade secrets were exposed after hackers infiltrated a robotics engineering firm storing sensitive information. Among the car manufactures were clients of the engineering firm, including Volkswagen, Chrysler, Toyota, General Motors, Tesla, and ThyssenKrupp. The 157 gigabytes of compromised trade secrets were made available online and included over a decade of assembly line schematics, factory floor plans, robotic configurations and documentation, employees ID badge request forms, contracts, and non-disclosure agreements.

Remote workers can also jeopardize company trade secret exposure

from the comfort and convenience of their own homes, via voice assistance systems, smart speakers, and home surveillance systems such as Siri, Google Assistant, Amazon Alexa, Echo, and Ring. These popular household gadgets have a history of security vulnerabilities that have led to several instances of eavesdropping and spying. For example, hackers have focused on the home security company Ring by gaining unauthorized access to homeowner's accounts and commandeering cameras and microphone hardware embedded within the security system. Recently, hackers successfully accessed Ring security cameras within the home and spied on the homeowners and their family members.

Given the increased risk to trade secrets in the work-from-home environment, companies must adopt measures to protect their proprietary information. It is paramount that businesses create a culture of compliance by establishing corporate policies and exercise reasonable efforts to maintain the secrecy of trade secrets. Namely, companies should work with legal counsel to craft remote-working policies that address the importance of protecting confidential company information. For example, companies should limit printing and physical copies of confidential information, and restrict remote access to any such printed information within their homes, just as they would in the office. Companies should also prevent employees from storing proprietary information on their personal devices or transmitting work-related information over public networks by equipping employees with work-issued devices and secure network access (e.g. virtual private network accessibility). Companies should require that the most confidential documents are password protected when its most sensitive documents are transferred electronically and that the email or communication containing the password is sent separately and part from the document. Finally, if you are setting up remote virtual desktops, ensure only key employees have complete access to the trade secret information.

Companies should also ensure that existing confidentiality practices are transitioned and enforced in the remote setting. Teleworkers and employees should be consistently reminded that working remotely does not create any exception to existing confidentiality and non-disclosure agreements or company policies, manuals, or practices. For example, if your standard practice is to have third parties sign an NDA during an in-person meeting, in the work-from-home environment, employees should be sure to send NDAs to third parties before a phone call or virtual meeting. Company policies should also prohibit employees from discussing confidential information in the presence of third parties, including family members, friends, or smart devices (i.e. speakerphone, Ring, Google Assistant, Alexa, etc.). Finally, teleworkers should be brought up to speed on increased cybersecurity threats that seek sensitive information under fraudulent communications related to the COVID-19 pandemic.

Risk Associated with Off-boarding Employees

The most common way trade secrets can be exposed is through disclosures by employees and workers. When employees who have been trusted with confidential trade secret information are laid-off, furloughed, or otherwise let go from their positions in the company, many will transition to other companies and competitors, carrying trade secrets and proprietary information. Accordingly, a company must have employees sign non-disclosure agreements and have a proper off-boarding process in place to ensure employees are not taking its valuable confidential information. Departing employees subject to non-disclosure agreements should be reminded of their post-employment contractual obligations. These measures and practices can increase the likelihood of enforceability and amass rapport and social capital with the outgoing employees.

Limitation to Trade Secret Enforcement

Additional trade secret protection protocols are especially necessary during the ongoing pandemic. Successfully obtaining enforcement of trade secret rights from courts is unlikely at this time as access to the courts is extremely restricted or completely unavailable. As a result, obtaining temporary restraining orders and preliminary injunctions are difficult amid the current climate. Even post-pandemic, when the courts are fully accessible again, the backlog of pending matters will likely delay any relief or enforcement of intellectual property rights. Therefore, businesses must take active steps immediately to protect their confidential and proprietary information.

CONCLUSION & RECOMMENDATION

In the face of the COVID-19 pandemic, businesses must adopt measures to prevent exposure and destruction of its valuable trade secrets. Companies are at an increased risk of losing valuable intellectual property and proprietary information. While businesses navigate through these unprecedented times, they must prioritize the preservation of confidential information throughout the pandemic. Further, they must keep in mind that because court enforcement is likely to be extremely limited, the existence of sound protection protocols is of the utmost importance.

Businesses must have policies and measures in place to safeguard their trade secrets. Even if your company already has a trade secret preservation policy in place, protocols should be analyzed and revised to address COVID-19 specific threats that may jeopardize your company's valuable intellectual assets, including employee turnover and cyber-security threats. For businesses venturing or considering a transition into new areas of operation to address the COVID-19 emergency (i.e., manufacturing sanitization products, medical products, PPE, etc.), business leaders should consider protecting emerging intellectual property rights.

For new initiatives that will take time and resources to incorporate into the corporate infrastructure fully, businesses should consider patent protection. New inventions, products, or methods are patentable until a year after they are publicly disclosed. However, trade secrets are well suited for new processes, products, inventions that will be rushed or introduced into the market more swiftly.

As employers and businesses consider new measures to protect confidential information, corporate leadership should seek legal counsel. Intellectual property attorneys can assist companies in identifying proprietary information, recommending best practices, and constructing proper policies and safeguards to insulate your trade secrets from exposure. Dickinson Wright's attorneys have considerable experience in assisting companies and individuals in protecting their intellectual property. The firm remains committed to helping our clients navigate this unprecedented time and remains fully available to provide any assistance that may be required.

ABOUT THE AUTHORS

Steven A. Caloiaro is a Member in Dickinson Wright's Reno office. He can be reached at 775.343.7506 or scaloiaro@dickinsonwright.com.

Caleb Green is an Associate in Dickinson Wright's Las Vegas office. He can be reached at 702.550.4417 or cgreen@dickinsonwright.com.