



## Protecting IP Assets

A business guide for what to watch

by *Gregory Sitrick*

With so many people working from home, many of the safeguards and systems that companies rely on to protect their information become less effective, partially compromised or even completely obsolete. The fact is that a company's sensitive information is at greater risk of being pirated when it's being handled outside the office. For example, many of us have smart devices such as home monitoring systems, speakers, baby monitors and smart doorbells that are connected to the internet. Some of these devices are listening all the time to our conversations. In addition, most people don't have the same level of security on their home computers as they do at work; they use weaker passwords than are required at work, and thus they are more susceptible to phishing and hacking attempts. Pirates know this and are on the attack trying to get companies' sensitive information.

Here are a couple areas to monitor:

### **Confidential Company Information**

This type of information often includes user names and passwords, and other information that hackers use to gain access to encrypted business systems. Typically, this type of information is stored on encrypted company computers that interact with encrypted business systems that are regularly updated to protect against the latest cyber attacks. Usually, this type of information gives the company its competitive advantage, or details the procedures and policies that it follows to drive its success.



*Greg Sitrick is an intellectual property attorney and partner at Quarles & Brady LLP*

Right now, there are a lot of people utilizing text or personal email to conduct company business while they work from home. It's critical to remind employees to be on the lookout for phishing scams and, as a best practice, to not send confidential company information over email or text.

### **Customer and Employee Information**

This type of information often includes personnel records, financial records and personal health information. Disclosure of this type of information is particularly troubling because it carries with it the potential for sanctions against the company. For example, disclosure of key financial account information, or healthcare information about the physical or mental health of an employee, can subject the company and its executives to civil and criminal penalties.

### **Trade Secrets**

Trade secrets are unlike other confidential business information because they require companies to take affirmative reasonable steps to maintain the secrecy of such trade secret information. It is critical that this information does not get out, because as soon as it is leaked, it loses its trade secret status. Trade secrets are typically kept under strict safeguards and can be accessed only by specifically authorized company personnel. Companies should determine and define new procedures and policies if they are going to allow different or remote access to their trade secrets. For more information on this, turn to "Minimize Risks to Trade Secrets in Remote Workspace Environments" by Quarles attorney Johanna Wilbert.

## Intellectual Property

Patents, Trademarks and Copyrights are well regulated by our Federal Intellectual Property Laws, but the COVID-19 outbreak is affecting the way we obtain Intellectual Property and our ability to enforce it.

As far as obtaining IP, the United States Patent and Trademark Office has the capability to operate without the need for applicants or their attorneys to physically interact with the examiners. It does, however, have some old rules that require certain procedures, transactions or documents to be handled via in-person meetings or original handwritten signatures, which are difficult or impossible right now in light of shelter-in-place orders and other isolation orders preventing travel and in-person meetings. This was especially problematic when the outbreak began because the USPTO indicated that it could not relax its existing deadline requirements.

Fortunately, the USPTO on its own stepped up to waive the requirements for an original handwritten signature for certain correspondence with the Office of Enrollment and Discipline and certain payments by credit card.

In addition, Congress just authorized the Director of the USPTO to toll, modify, adjust or waive any deadlines in light of the COVID-19 outbreak. With all the advancements in technology, it will be interesting to see if the USPTO adopts some of these procedures after we recover from the COVID-19 outbreak.

As far as enforcing IP, it typically takes two years and at least \$1,000,000 to enforce it. Pirates know the cost of enforcement is a large hurdle, and they are taking full advantage of it right now while companies are struggling to make ends meet. Compounding the enforcement problem, Federal Courts around the country have banned in-person hearings, opting instead for telephonic hearings or delaying or postponing them at least 30–60 days, if not longer. Most courts have suspended jury trials in response to the coronavirus. The Court of Appeals for the Federal Circuit will now remotely conduct all cases scheduled for argument during the month of April 2020, and there will be no in-person hearings held. The United States Supreme Court has [postponed oral arguments](#). As a result, counterfeits are making their way into the marketplace in large numbers due to the soaring demand for certain products that are normally abundant but are now hard to find.

*Greg Sitrick is an intellectual property attorney and partner at [Quarles & Brady LLP](#)*

---