LAW FIRM 2.0®

FISHERBROYLES

A LIMITED LIABILITY PARTNERSHIP

NEWSLETTER

IP Law Update: March 2017
Volume 6, Issue 1

info@fisherbroyles.com
www.fisherbroyles.com

Contributors:

TJ DoVale
Direct: (678) 743-1125
tj.dovale@fisherbroyles.com

Deborah Fletcher
Direct: (704) 442-7263
deborah.fletcher@fisherbroyles.com

R. Mark Halligan
Direct: (312) 607-0102
rmark.halligan@fisherbroyles.com

Michael Khoury
Direct: (248) 921-8266
michael.khoury@fisherbroyles.com

Marty Robins
Direct: (847) 277-2580
martin.robins@fisherbroyles.com

Intellectual Property Law Update

Now that we've made it through another winter, it is a great time to address several IP issues which will likely make a difference to your 2017 bottom line:

- Dealing with infringement of your IP;
- Handling of employees leaving for competitors;
- Development of proper responses for when you are hacked;
- Borrowing against IP – key watchouts … and opportunities!

Someone is infringing your IP – Now What?

So you own some kind of valuable IP which is not being respected. What to do? The answer depends on the type of IP and nature of infringement, as well as the competitive threat. For example (and most assuredly **not** addressing all potential infringement situations):

- Your copyrighted photo, text or video shows up on someone else's website. You'll want to send a 'takedown notice' to the person designated on the site as 'DMCA' [Digital Millennium Copyright Act] agent on the website. Such notice must conform to a prescribed format, but if it does, it is usually the case that recipients remove the material.
- Your web address is being used by a competitor which is diverting your traffic. A federal law, the Anti-Cybersquatting Act, may allow you prompt relief. At the least a letter to the offender is in order. If this is ineffective, and there is a substantial impact on your business, you may need to file suit under this law.
- Your federally registered trademarked name or logo is being misused by a competitor on their website or otherwise. If the issue involves the website, a letter to the DMCA agent is a good place to start. If this does not work or the misuse involves something else, a letter from us, as your attorney, illustrating the likelihood of consumer confusion , to the company's CFO or general counsel is in order. If this does not work or the issue is clear 'counterfeiting' of your product, legal action, possibly including a referral to authorities, is in order, and may in some cases, allow immediate corrective action.
- Your patent is being infringed. In that pursuit of legal action usually results in a challenge to the patent's validity and may lead to a claim of infringement of the other party's patent, you will want to discuss with patent counsel the sorts of challenges and outcomes to be anticipated as well as whether the other party is actually infringing. If these do not appear to be too daunting, a 'cease and desist' letter from us to the other party's

LAW FIRM 2.0®

FISHERBROYLES

A LIMITED LIABILITY PARTNERSHIP

CFO or GC is in order with legal action to follow if satisfaction is not obtained.

Above all, you need to very promptly talk to us so that one of our IP or litigation partners can help to determine the best, most cost-effective step for your specific circumstances.

Key Employee Going to a Competitor – Managing Trade Secret and other Risk

Your key employee walks in (or sends an e-mail after disappearing) and says that they are leaving to join (or start) a competitor. What now?

There are state, and now, federal, laws which are likely to be useful. However, before pursuing relief, it is essential to ensure that you have a reasonable position, as federal law now allows for significant sanctions against those who pursue such claims without a good faith basis. Someone going into competition with you is not likely to be actionable by itself unless they are violating an express contract of some sort and/or 'misappropriating any of your trade secrets'. Not all business information is a 'trade secret' under law.

You need to address the following:

- Pull their file to see what was signed when they came on board. Hopefully, there is at least a nondisclosure and invention assignment agreement covering material such as customer lists and pricing data, supplier lists and employee lists. Perhaps there is an employment contract containing this material and possibly a non-compete or non-solicitation provision.
- Disable electronic access to sensitive materials.
- If circumstances appear suspicious, FisherBroyles, LLP can assist with the engagement of an independent forensic consultant to create a forensic image of the departing employee's computer and to assist in determining whether unauthorized activities occurred before the departing employee's termination of employment. The former employee's office or work space should be cordoned off and internal IT should be instructed not to turn on or off the computer pending the acquisition of an EnCase image for preservation of evidence by the independent forensic consultant.
- Determine what material is most sensitive and poses the greatest competitive threat.
- For the most sensitive material, enumerate the steps you have taken to safeguard it, such as physical access limitations and electronic access controls.
- See what notices of whistleblower rights were given to the person in question. The answer may dictate whether you can obtain enhanced damages and/or attorneys' fees.
- Determine what you want to be done to protect your business. For example, if there is no non-compete or it would be difficult to enforce, can you live with a limitation on solicitation of your customers? For how long? For technical information, what restrictions do you want regarding transfer and/or use of information? If damage has been done, do you have a realistic estimate and evidence that it arose from the departure?

LAW FIRM 2.0®

FISHERBROYLES

A LIMITED LIABILITY PARTNERSHIP

While you are compiling this information, talk to your FisherBroyles lead to develop a customized plan to rectify the situation. Every plan is different, but we will work with you to apply all laws, including the new Defend Trade Secrets Act of 2016, which may get you into federal court. Sometimes prompt litigation is needed, but in many other cases, a properly worded letter will be enough to minimize the competitive threat.

More helpful to most organizations than after the fact efforts to restrain former employees is likely to be proactive steps to support your trade secret position. Our IP partners can help with both.

Privacy and Information Security

Cyber Incident Response Planning

Articles and notices about data breaches have become commonplace, but the actions required by companies in the event of such an incident are considerable and the potential liability substantial. Cyber incident response planning should not be taken lightly and actions are needed in the event of a potential incident. The following are some suggestions for planning for your company and responding in the event of an incident. Contrary to some views, the use of cloud vendors and other third parties does not negate the need for such a plan. The US Federal Trade Commission has provided a good deal of specific guidance on this topic which must be taken into account when formulating a plan.

To be meaningful, the plan must be **in writing** and communicated to all key employees. In developing your incident response plan, each company needs to evaluate its own internal processes and the information it maintains. The specific parts of the plan may include the following:

- Who will be the point person? This person is responsible for execution of the plan and communicating and overseeing with members of the response team and third parties. In larger organizations, this will often be the responsibility of someone in the compliance or legal department.
- Who will be on the team? These will be resources that have critical skills and knowledge that will be needed. Representatives from executive management, IT, HR, legal, public relations and risk management. A back up person in each category should also be identified. Contact information must be shared and updated.
- Understand what data the organization has, where it is kept, how is it secured and where backups are maintained.
- Who is responsible for preventing an incident from happening? Who is responsible for detecting one when it does? This may be the same person, but may include outsourced functions.
- How will the organization work to contain the breach and investigate the incident, as well as providing legally required notices?
- Does your organization have cyber insurance coverage? Should you? Who will initiate claims?

Once the incident response plan is developed, it is important to determine how employees within the organization should be trained to be sensitive about the privacy of information, recognize a potential problem and the response needed.

If your organization learns about a cyber incident, immediate implementation of the response plan and developing an action plan are important and some aspects are **legally required**. As you are assembling the team, you should begin to assess the threat level and the nature of the response. There are some suggested points to consider:

- Determine the kind of data that has been compromised and the manner in which the incident occurred. Is the information proprietary or confidential? Does it contain personally identifiable information? Is it subject to regulatory compliance (such as health related data subject to HIPAA)?
- Determine if the incident is potentially ongoing (for example through a compromise of your information systems) or a one-time incident (such as through the loss or theft of devices storing information).
- Contact counsel to assist in the legal aspects, determine which notices are required and who provides them, and to coordinate the response. The retention of some professionals should be through your outside counsel in order to potentially preserve the confidentiality of any information.
- As part of the investigation of the incident, determine if a security or forensic firm should be brought in to assist. (Hint: the answer is almost always yes.) Often the lawyer should hire the forensics firm for confidentiality purposes.
- Complete remediation, if necessary, of your information systems and determine whether notification obligations exist. Depending on the scope of the breach, you may also need to retain the services of a public relations firm to tailor the disclosure and the message.
- Evaluate what weaknesses existed in your systems, processes and policies and implement fixes and updates to your systems. Review and update your incident response plan as well.

Any of the members of our Privacy Practice Group are available to assist you. Please call us.

Borrowing Against IP – Additional Financial Flexibility

One asset which is under-appreciated by both borrowers and lenders is intellectual property, particularly patents and trademark registrations. Such assets may allow expansion of borrowing bases – i.e. allow borrowers to borrow more – and enhance lender security. Credit agreements customarily cover 'intangible assets' such as receivables or notes, but there is no inherent reason why they can not cover patents and trademarks as well.

While institutional lenders must comply with regulatory obligations which may impact permissible collateral, other lenders are free to accept and lend against these items in the same manner as all other collateral. Borrowers having substantial amounts of such assets should make sure to discuss the same with potential secured lenders.

All parties interested in going this route need to keep in mind several fundamental considerations:

- Proper description of this collateral (by number and date) in financing documents is essential; a reference to 'all intellectual property' is not likely to be sufficient
- Several governmental filings, going beyond UCC-1's, are necessary;
- Lenders need input from technical subject matter experts to establish commercial value of items – all patents are not created equally! A patent which is clearly valid, but which has only two years left in its term or pertains to obsolete technology, is of no more value than obsolete, unsalable inventory;

LAW FIRM 2.0®

FISHERBROYLES

A LIMITED LIABILITY PARTNERSHIP

- Lenders proposing to lend substantial amounts against such assets (especially those involving software or e-commerce) will usually want input from patent or trademark counsel as to the likelihood that they will withstand legal challenges to their validity. Recent developments in statutory and case law create a number of questions.
- While pending applications can, in theory, be used as collateral, in practice, the burdens of their completion in the event of foreclosure may minimize their value.
- Loan and security agreements should specifically provide for the mechanical steps associated with foreclosure on these assets, which will differ from those associated with real estate, inventory, machinery and even receivables.

Our corporate and IP partners can provide customized guidance for lenders and borrowers interested in addressing this possibility.