

PROTECTING COMPANY INTELLECTUAL PROPERTY THROUGH EMPLOYMENT AGREEMENTS AND EMPLOYEE EXIT PROCESSES



RYAN W. O'DONNELL is a shareholder at Volpe and Koenig, P.C. His practice focuses on patent prosecution, intellectual property litigation, and licensing in the chemical, biotechnology, medical device, and mechanical industries. Ryan has served as lead trial counsel in patent infringement disputes throughout several federal district courts, the US Court of Appeals for the Federal Circuit, and before the International Trade Commission (ITC). Ryan routinely reviews IP assets and develops creative ways to maximize the value of portfolios through licensing, enforcement, and strategic partnerships.

Ryan is admitted to practice before the US Patent and Trademark Office, the US Supreme Court, the US Court of Appeals for the Federal Circuit and Third Circuit, and the US District Courts for the Eastern District of Pennsylvania and the District of New Jersey. He received his JD from Temple University Beasley School of Law and his BS in Biochemistry from Temple University.

Work environments have become more flexible, in part due to the recent necessity of remote work arrangements, allowing employers and employees alike to seek new opportunities in new geographic markets. In turn, remote work environments have generated increased employee turnover, presenting unique challenges for employers who need to protect their intellectual property (IP) rights. Remote work environments raise additional complications, for example, in situations where the activities involved in creating, maintaining, and using company IP take place at the employee's residence or with the assistance of the employee's resources, such as computers, phones, and applications.

Ownership of and disputes over IP rights can be complicated and consume resources. Such intellectual property rights typically include: (i) patents which protect inventions; (ii) trademarks which protect a company's brand and reputation; (iii) copyrights which protect works of authorship and creativity; and (iv) trade secrets which protect a company's confidential or proprietary information. As a best practice to reduce the risk of IP disputes with employees, it is important to set clear expectations regarding company IP rights at the outset of

the employment relationship and to maintain such expectations throughout the course of employment. Addressing these issues upfront can potentially avoid costly litigation at a later date.

This article addresses practices that can be adopted at the initiation of the employee relationship and during the employee exiting process to protect company IP rights and reduce the risk of IP disputes.

PRE-EMPLOYMENT SCREENING

The employee hiring process provides an opportunity to: (i) identify IP rights that may be owned by the employee or third parties (e.g., prior employers); (ii) obtain applicable IP-related representations and warranties from the employee; (iii) articulate expectations regarding treatment of the company's confidential information; (iv) secure ownership of IP developed during the course of employment; and (v) lay the foundation for post-employment obligations to protect company IP.

Potential employees may possess or have knowledge of IP rights that are owned by a third party, such as a prior employer. Such third-party IP can

include customer lists, third-party documents, formulas, marketing strategies, pricing, or templates. Often, a potential employee is unaware of complicated IP ownership issues or the full scope of any obligations owed to a prior employer. In order to avoid cross-contamination of IP rights, it is important to educate potential employees that they may have knowledge of, or be in possession of, intellectual property rights belonging to a third party.

To reduce the risk of any IP theft, employers should request that potential employees disclose information, such as:

- Prior employers and positions held;
- Confidentiality owed to a third party;
- Inventions and trade secrets assigned to another company (in a manner that does not breach confidentiality); and
- Existing non-compete agreements or other restrictive covenants.

Obtaining this information prior to the formation of an employment relationship assists with making an informed hiring decision and potentially reduces the risk for surprises down the road.

IP REPRESENTATIONS AND WARRANTIES

Every employee should sign an employment agreement as part of the hiring process. An employment agreement is typically the earliest and best opportunity to clearly define the company's expectations regarding IP owned by third parties, IP developed by the employee over the course of employment, and restrictions on and expectations of the use of company-owned IP. It is critical that the employment agreement include procedures that the employee should take to protect or maintain company-owned IP both during the course of employment and after departure.

An employment agreement can include representations and warranties to avoid third-party IP disputes and to set expectations regarding company-owned IP. Such representations and warranties can include:

- Disclosure of all prior relevant agreements, particularly those involving IP ownership, confidentiality provisions, and non-compete provisions;
- Representation that the employee is not aware of, nor has disclosed, any obligations in prior agreements that would limit the scope of employment;
- Agreement that the employee will not divulge or use any third-party inventions or third-party confidential or proprietary information;
- Affirmation that the employee has returned all IP owned by previous employers;
- Agreement that the employee will notify the company of any concerns regarding third-party IP that is relevant to the employee's scope of work; and
- Agreement that the employee will disclose and assign all relevant inventions, works, or trade secrets to the company during the course of employment.

While these representations and warranties do not indemnify the company, they can operate to strengthen the company's position if there are any accusations of IP theft resulting from the new employee's actions.

EMPLOYEE CONFIDENTIALITY OBLIGATIONS

The employment agreement should clearly define the company's policy regarding protections for and use of company confidential information. As a starting point, a confidentiality provision should clearly articulate the type of information that the company considers "confidential" or "proprietary." It should also include obligations to protect the company's confidential and proprietary information which is utilized or created during the course of employment, including a requirement that the employee return all confidential information at the termination of employment. Finally, the obligations of confidentiality should expressly extend beyond the term of employment for as long as the information remains confidential.

Confidentiality agreements should include reasonable restrictions. For example, “confidential information” should not include:

- Information that the employee had knowledge of prior to joining the company;
- Information that is in the public domain or may be accessed by the public; and
- Information that the employee can prove was received from a third party that is authorized to share it.

In addition to providing confidentiality provisions in an employment agreement, it is prudent to create a culture of confidentiality in the workplace. For example, an employer should periodically review the company’s expected confidentiality practices during employee meetings, use specifically tailored confidentiality and non-disclosure agreements for particularly sensitive projects, and remind departing employees of their continuing confidentiality obligations during the exit interview.

Employers should also adopt reasonable practices to protect confidential information within the workplace, such as by:

- Establishing physical and digital security measures;
- Restricting visitor access, both in the physical and digital workplace environments;
- Marking confidential and sensitive materials “CONFIDENTIAL,” in the subject line of an email or in the title of an electronic document;
- Limiting access to the most sensitive information to those employees with a need to know; and
- Conducting periodic training on use and protections for confidential information.

Confidentiality provisions should also contemplate use of confidential information in the digital world. For example, reasonable security measures should be taken for employees accessing company systems using personal or mobile devices, and the confidentiality provisions should set forth the company’s expectations regarding privacy settings for

such remote access. Sensitive documents should be encrypted or password-protected. Use of external storage devices for downloading company information should be limited or restricted. Social media policies should be established to provide guidelines on company-related information that can/cannot be shared. The company should also encourage immediate reporting of lost or stolen computing devices or other company information.

The establishment and enforcement of confidentiality provisions is a critical aspect of maintaining company information as proprietary and trade secret. Under the federal Defend Trade Secrets Act (DTSA), the owner of a trade secret must establish that it took reasonable measures to keep the information as secret. Some non-exhaustive factors that courts consider when determining if an employer has protectable trade secret information under the DTSA include: (i) whether the employer had confidentiality agreements in place with its employees; (ii) whether the employer notified its employees of information that it considered confidential; (iii) whether any employee training on confidentiality was provided; (iv) whether there were any restrictions on access to confidential information; and (v) whether the information was marked “Confidential.”

Having a well-established confidentiality policy set forth in an employment agreement and practices in place to reinforce confidentiality expectations are critical to protecting company IP.

IP OWNERSHIP

An employment agreement should address IP ownership issues and include an assignment of rights for employee-created IP. While there is often an assumption that all IP rights created during the course of employment are owned by the employer, this is not always the case. For example, in *Board of Trustees of the Leland Stanford Junior University v. Roche Molecular Systems*, the Supreme Court emphasized the well-established law that intellectual property rights to an invention belong to the inventor (i.e., employee) absent an express grant of those rights to the employer.¹

Employment agreements should include a standard assignment of all IP rights to the employer pertaining to company IP developed during the course of employment. Because employees may occasionally be unwilling to sign an assignment of rights to an invention or may have departed the company prior to executing an assignment, it is prudent to require employees to execute a standard assignment at the commencement of employment which can be included in the employment agreement. Such an agreement should reflect that, but for the employee's execution of the agreement, the company would not employ the individual.

Assignment provisions need to be drafted with express, nonconditional language in order to be enforceable. Assignment provisions with future or conditional provisions, such as "I will assign," may not be enforceable. As an example, in *Stanford University v. Roche Molecular Systems*, a researcher signed an agreement upon joining Stanford stating, "I agree to assign or confirm in writing to Stanford and/or Sponsors that right, title and interest in ... such inventions as required by Contracts or Grants."² The US Court of Appeals for the Federal Circuit interpreted this clause as a promise to assign rights at some point in the future and not as a present assignment. As a mere promise to assign rights in the future, such language was held to be unenforceable without a subsequent assignment to transfer legal title.

Assignment language should be included in an employment agreement and should be drafted with present, non-conditional language such as, "I do hereby assign," in order to be enforceable.

POST-EMPLOYMENT CONSIDERATIONS

An employment agreement should also include expectations of departing employees for protection of company IP. This should include obligations to execute any future documents related to IP that was created during the course of employment. For example, in the case of patent applications for inventions, the patent application could be filed

after termination of the employee and require a declaration from the employee/inventor.

Employment agreements should also include an obligation to return all confidential materials to the company prior to departure. Such a provision should require the return of all documents, electronically stored information, electronic devices or storage media, and other company property. In addition, the agreement should require the employee to confirm satisfaction of this obligation in writing at the end of the employment relationship.

Finally, the employment agreement should include an obligation that confidentiality will survive termination.

EXIT INTERVIEWS

The end of an employment relationship should conclude with a comprehensive exit interview for all departing employees. Due to lapse of time or complicated provisions in the employment agreement, employees may forget or be unaware of their obligations at the end of employment and their continuing obligations post-termination. Employers should provide the departing employee with a copy of their employment agreement and review the termination details with the employee. For example, it is critical to review non-compete clauses, confidentiality obligations, return of company information/materials, and any other restrictive covenants to ensure that the employee understands these obligations. It is also prudent to ensure the employee has returned all company-owned computers, mobile devices, office keys, badges, access cards, and other company-owned property and devices prior to the employee's departure. Finally, the departing employee should certify that they deleted or otherwise destroyed all copies of company materials stored on their personal devices.

After reviewing the foregoing information with a departing employee at the exit interview, the employee should execute an acknowledgement to confirm an understanding of all such obligations. It is also beneficial to request updated contact information for the departing employee.

POST-EMPLOYMENT SECURITY

After the employee's departure, it is important to immediately disable the employee's access to all company information. This may include terminating key cards, deactivating all accounts associated with the employee, updating passwords for shared accounts, and deleting permissions to devices, data, infrastructure, and the employer's facility.

CONCLUSION

The employee hiring process is an ideal time to set expectations regarding company intellectual property and to avoid intermingling any third-party intellectual property rights carried over from past employers. Inclusion of IP protection provisions in an employment agreement can reduce the risk of costly litigation down the road.

In the event of departure, a comprehensive employee exiting process can further protect a company's IP rights and reduce the risk of disputes. Exiting processes can serve as a timely reminder of an employee's legal obligations, ensure the security of information, and provide information on new employment to determine the risk of disclosure of company IP rights. 🍀

Notes

1 563 U.S. 776 (2011).

2 583 F.3d 832, 842 (Fed. Cir. 2009).