Is your company protected from departing employees who possess confidential information and trade secrets?

by Rachel Yarch, Partner, Burke, Warren, MacKay & Serritella P.C.

Imagine losing a valuable, high-level employee without warning. Think about the sensitive nature and types of information that your key employees possess. For example, what if this involves the head of your Research and Development (R&D) department, who is the only person with knowledge of certain valuable and sensitive company information? Or, what if your Director of Sales is lured away by a lucrative offer from a direct competitor? There are endless scenarios that could occur depending upon the nature of your company's business. It is critical for companies to consider the harm that they could suffer by an unexpected employee departure. The good news is that companies can take a number of steps to minimize the exposure and risks associated with losing a key employee.

CONFIDENTIALITY/NON-DISCLOSURE AGREEMENTS

First, if the company has information that it considers to be confidential, that information should actually be protected. A company has a right to designate information as "confidential," and to define the consequences for disclosure of confidential information. In many instances, companies attempt to rely on a Confidentiality Policy contained within an Employee Handbook to protect their information. However, this practice is utterly insufficient for a couple of reasons: (i) the Confidentiality Policy is not contractual, meaning it is neither binding nor enforceable; and (ii) the Policy serves only to govern the conduct of employees while employed. Simply put, employee handbooks cannot legally restrict the conduct of former employees. And, even if a handbook policy attempts to govern post-employment conduct, it is simply not binding after the employee has left, which is often when the protection is needed the most.

It is a best practice for companies that possess sensitive, confidential information, such as customer /client/vendor lists, pricing information, non-public company financials, scientific formulas or other valuable intellectual property, strategic plans, and/or marketing information, to enter into Confidentiality/Non-Disclosure Agreements with the employees who will have access to such information. However, to be enforceable, these agreements should not be "boilerplate" and, in most cases, should not be entered into with each and every employee, regardless of their position with the company. Courts are very reluctant to enforce agreements that are not tailored to specific employees and are over-inclusive. Rather, companies should identify only the employees who possess or have access to sensitive, confidential information and require them to enter into agreements.

Second, it is critical that the company identify the types of information that a particular employee possesses that must be protected. Courts are unlikely to enforce agreements that do not specifically describe the confidential information to be protected. Confidentiality/Non-Disclosure Agreements should be drafted to be narrowly tailored to the specific circumstances of a particular employee or a class of similarly situated employees. Well-drafted, narrowly tailored agreements - targeted to employees who actually have access to confidential information - will greatly increase the likelihood that the company will be able to enforce them.

TRADE SECRETS

A tortoise is an animal, but not all animals are tortoises. By the same token, trade secrets are a form of confidential information, however, not all confidential information is a trade secret. There are some specific state and federal laws which govern the protection of trade secrets and prohibit misappropriation of trade secrets.

Specifically, the Uniform Trade Secrets Act defines "trade secret" as information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. In determining whether or not certain information constitutes a trade secret, courts will often analyze the following:

- the extent to which information is known outside of the company;
- the extent to which the information is known by employees and others involved in the business;
- the extent of measures taken to guard the secrecy of the information;
- the value of the information to the company and competitors;
- the amount of effort or money expended by the company in developing the information; and
- The ease or difficulty with which the information could be properly acquired or duplicated by others.

Thus, in order to best protect its trade secrets, a company must first have internal controls in place. While some confidential information may be widely known within a company, such as customer or client lists, actual trade secrets require a higher level of protection. Only certain classes of employees with a business need-to-know should be given access to your company trade secrets. To the extent that trade secrets are contained in physical files, those files should be under lock and key and employee access should be limited. To the extent that trade secret information is stored electronically, it must be

password-protected and the passwords provided only to those who require access to the information to perform their jobs. The bottom line is if your company is an open book, it will be very difficult, if not impossible, to claim that certain company information is confidential or constitutes trade secrets.
In addition, trade secret information should be specifically defined within a Confidentiality/Non-Disclosure Agreement, so that the parties to the Agreement know exactly which information is deemed a trade secret. Further, the Defend Trade Secrets Act of 2016 ("the Act") created federal jurisdiction for trade secret litigation, which can be highly preferable over litigation in state court. However, the Act requires certain language related to whistleblower immunity to be included in an Agreement for a company to implement all of its federal remedies against a former employee who misappropriates trade secret information. Some of those remedies include double damages, attorneys' fees and seizure of the information. To the extent that your company has Confidentiality/Non-Disclosure Agreements governing trade secret information, which were drafted prior to 2016, those Agreements should be updated for compliance with the Act.

NON-COMPETITION AGREEMENTS

Perhaps your company has only a few direct competitors. If your company loses a key employee to a direct competitor, you could lose serious advantage in the market in the event that the employee leverages his or her knowledge, experience and relationships to take business away from your company. There are steps that can be taken to attempt to prevent this from occurring, but those steps must be taken properly and reasonably to be effective.

It is possible to have an employment agreement with an employee that governs confidential and trade secret information, in addition to post-employment restrictive covenants such as non-compete and non-solicit provisions. Like Confidentiality/Non-Disclosure Agreements, non-compete provisions should be narrowly tailored in scope in order to protect the company's legitimate business interests, but not so restrictive that they are rendered unenforceable. In most cases, it is not good practice to have company-wide non-competes. Your receptionist or after-hours maintenance worker is probably unlikely to inflict damage on the company by going to work for a competitor, so long as your company has internal controls in place regarding its confidential information and trade secrets. Again, the focus should be on those employees who have the greatest ability to harm the company's interests.

Courts generally disfavor non-compete agreements and will only be inclined to enforce those agreements that are not unnecessarily restrictive. Placing a five (5) year restriction on an employee's ability to compete will most likely be unenforceable. Similarly, posing a nationwide restriction is often unenforceable unless the company's business is so unique that any employment with a competitor would significantly threaten the business. A best practice is to restrict the employee only from performing similar functions for companies who directly compete with your company. Additionally, if the non-compete is narrowed to a specific geographic area and the restriction limited to two years or

less, your company will be in the best possible position to enforce the restriction. Moreover, current law in Illinois requires some form of additional consideration to make post-employment restrictive covenants (like non-compete and non-solicit provisions) enforceable on new employees. This is a relatively recent development in the law. Accordingly, if your agreements have not been updated for several years, there is a good chance that they are no longer enforceable under Illinois law as they relate to your more recent hires.

NON-SOLICITATION AGREEMENTS

Perhaps worse than losing an employee to a competitor would be losing an employee who then assists a competitor in raiding your sales force one employee at a time. Or, having a former employee share your CRM system with a direct competitor, who reaches out to each of your customers/clients/vendors. The risk of either of these scenarios happening to your company can be minimized by entering into enforceable non-solicitation agreements. Non-solicit provisions can be aimed at a former employee's contact with company customers/clients/vendors or solicitation of other employees of the company, or both. Non-solicit provisions often go hand in hand with non-compete provisions and can also be contained within the same agreements as provisions related to confidential information and trade secrets. Again, these provisions should also be narrowly tailored to serve the company's interest, without unreasonably hindering a former employee's ability to secure new employment. In many cases, courts will not prohibit individuals from contacting any customer/client/vendor who, at any time, did business with your company. Rather, in most cases, an agreement will only be enforceable if it is limited (i) in time and (ii) to customers/clients/vendors with whom the former employee came into contact during his or her employment with your company.

The law governing post-employment restrictive covenants, including non-compete and non-solicit agreements, is rapidly changing. Courts tend to disfavor restrictions on an individual's ability to make a living. In fact, many agreements are struck down as improper restraints on trade. However, well-drafted, enforceable agreements could save your company from potential financial ruin if the wrong information finds itself in the hands of your competitor. It is crucial to have employee agreements legally reviewed and updated at least every two years, to maintain conformity with the frequent updates in the law and to maximize the likelihood of enforceability.

Litigation to enforce these types of employment agreements can be very costly and typically involves motions for temporary restraining orders, preliminary injunction hearings and expedited discovery. Whether or not your company attempts to enforce a post-employment restrictive covenant is a choice the company can make on a case-by-case basis by evaluating the costs and benefits associated with doing so. Depending on the circumstances, the level of risk associated with a former employee's new employment may not warrant costly litigation. In other instances, sending a cease and desist letter and

placing the new employer on notice of the threat of litigation can lead to a resolution. However, unless a company has these measures in place, it likely has no legal recourse.

OTHER RISK MANAGEMENT CONSIDERATIONS

On one hand, while protecting company information and providing access and passwords only to those with a need to know is best practice, it should never be the case that only one owner or employee of a company holds all of the cards. Remember, you may have little or no advance notice of a key employee exiting the company. Similarly, accidents, illnesses and injuries can take a key employee out of service. Do not let your company's operations come to a screeching halt because the one person with the password or knowledge of sensitive information becomes temporarily or permanently unavailable. Whether it is your head of IT, R&D or sales, your company must ensure that there is backup in place for situations where that individual abruptly leaves the company, is taken ill or is otherwise unavailable. While trade secret information is sensitive, and limiting its dissemination is fundamental, a company cannot leave itself in a position where no one has knowledge of a sensitive password or the ability to access your server. Considering these scenarios in advance and putting measures in place can save your company a significant amount of time and money.

If and when you do face a situation where an employee with access to confidential information abruptly leaves your company, having an established checklist of actions to consider for protecting the company's interests could prove invaluable. In addition to collecting company property such as keys, credit cards, laptops, cellular phones and other technology, companies should have standard protocols for immediately terminating the former employee's access to its server, including email and remote access. It goes without saying that such actions are time-sensitive and that any delay, especially in dealing with a disgruntled employee, can result in harm to the company.

While the existence of bad actors is inevitable, there are steps that companies can take to limit potential exposure. Confidentiality/non-disclosure agreements, non-competition and non-solicitation agreements, along with clearly established internal procedures are essential tools for your company to manage risks, prepare for crises, and minimize damage if an unexpected employee departure occurs.