Dilworth Paxson

E-ALERT

Related Lawyers

Christopher C. Nana-Sinkam

Related Practices

Labor & Employment

Media Contact

Peter Dunn
Director of Client Relations and Communications
Philadelphia, PA
pdunn@dilworthlaw.com

PROTECTING YOUR BUSINESS IN THE WAKE OF PENNSYLVANIA'S PROPOSED "FREEDOM TO WORK ACT"

03/26/2018

By: **Christopher Nana-Sinkam**

With the start of 2018 well under-way and companies as susceptible as ever to data breaches and corporate theft, every employer should take a moment to revisit and reflect on its company policies – most notably those involving their confidential business information.

Last November, Pennsylvania legislators introduced the "Freedom to Work Act" (the "Act"), House Bill 1938, which proposes an outright ban on "covenant[s] not to compete" in Pennsylvania. Under the Act, a covenant not to compete is defined as "[a]n agreement between an employer and employee that is designed to impede the ability of the employee to seek employment with another employer" and would be deemed "illegal, unenforceable and void as a matter of law." The Act does not apply retroactively and contains select exceptions to the its enforcement including: (1) covenants involved in the sale of a business or goodwill; (2) covenants involved in a dissolution or disassociation of a partnership or limited liability company; or (3) covenants that are reasonable and entered into prior to the effective date of the Act. Effectively, employers would no longer be able to prevent their employees from leaving to work with competitors. This proposed law however, would have no effect on non-solicitation agreements. Employers would still have the ability to limit their former employees from poaching clients and employees when they leave for a new position.

Whether the Act becomes law has yet to be seen, but regardless, employers still have a number of tools at their disposal, including non-solicitation agreements, to help protect their confidential business information, employees, client relationships, and overall goodwill. Employers should revisit their policies and employment agreements to ensure their business is protected irrespective of the Act's outcome. To get you started, below is a list of strategies for securing your company's business information:

(1) Clearly identify your company's valuable business information

This is the first step in protecting your company's confidential business information and business relationships. Without first identifying the sensitive information you cannot implement policies to protect it. When trying to classify this information, ask yourself the following:

- Is the information known outside the company?
- How much money and effort was expended by your company to develop the information and business relationships?
- What is the value of the information to your company? To your competitors?

– How difficult would it be for others to acquire or duplicate the information?

Non-competition agreements or not – every employer should identify its most sensitive and important business information.

(2) Continue to use non-solicitation agreements

Even though the Freedom to Work Act proposes prohibiting non-competition agreements, the primary concern of most employers is not that the former employee will go to work for a competitor, but will leave with the employer's clients, confidential information, or other employees. Therefore, employers should strive to protect their business relationships, employees, and confidential information by continuing to use non-solicitation agreements with their employees. These agreements will not only prevent your former employees from contacting and poaching your business' clients, but also prevent them from trying to poach your other employees, which can be invaluable, especially in situations involving hostile departures.

(3) Implement written confidential business information policies

Every business should develop and immediately implement written policies regarding their confidential business information and business relationships and distribute these writings to all employees, either in the form of an employee handbook or as a separate policy. By placing these policies in writing, you not only instruct employees on how to identify and protect sensitive information but also aid management in enforcing those policies and demonstrate your commitment to protecting that information, which can be extremely valuable in litigation. Indeed, during litigation, courts will typically give significant weight to how much time and effort an employer put into designating and protecting its sensitive information and client relationships. It never hurts to be overly-cautious.

(4) Restrict access to confidential business information to employees with legitimate, business-related need to know

Employers should restrict the number of employees with access to sensitive company information. Employers are encouraged to limit disclosure to employees who require that information to perform their duties for the company. If an employee can perform his/her duties with limited information, he/she should only be given the amount of information needed. Remember, the more people who are in on a secret, the harder it is to keep.

(5) Use confidentiality agreements with third parties

All too often, companies risk exposing their confidential business information and business relationships when engaging with third-parties without the necessary protections in place.

Communications with consultants, media outlets, financial advisers and other professionals should be heavily scrutinized and employers should consider the following:

- Require signed confidentiality agreements with all outsiders before providing access to sensitive information;
- Mark all confidential documents given to outsiders;
- Disclose the least amount of information necessary; and
- Before entering into joint ventures, mergers, or similar arrangements, clearly set forth and identify ownership and protection of confidential business information.

(6) Limit public/outsider access to buildings

Employers should be especially careful in limiting outsider access to buildings and systems housing sensitive company information and trade secrets. Depending on the level and sensitivity of the information, employers should consider the use of security guards or cameras, visitor badges with check-in and check-out procedures, and required security card access to certain areas and systems. By physically limiting the amount of individuals with access to certain information, employers can increase their chances of safeguarding their confidential business information.

(7) Monitor departing employees

Lastly, employers should strive to monitor their employees' use of company property, especially when an employee is preparing to leave the company. Oftentimes, employees departing a company will take with them – either consciously or subconsciously – sensitive company information and fail to return all company-issued documents and property. To prevent this, employers should conduct exit interviews with all departing employees to ensure that: (1) all company-issued documents and property are returned prior to departure; (2) the employee is aware of his/her legal and/or ethical obligation to maintain the company's confidential business information; and (3) the departing employee's access to company databases is terminated. It is also advised that departing employees' sign acknowledgements of their continuing secrecy obligations.

Although no system is fool-proof, by following the above tips, employers can continue to improve their chances of keeping their sensitive information and business relationships safeguarded from prying eyes, competitors, and disgruntled ex-employees. If you have any questions regarding how to protect your business's confidential information and business relationships, or how the proposed Act may affect your business, contact **Christopher Nana-Sinkam**.