Insights, News & Events

5 TRADE SECRET PROTECTION STEPS EMPLOYERS SHOULD TAKE IN RESPONSE TO NEW CORPORATE ESPIONAGE IN FLORIDA ACT

Insights
Jun 21, 2021

Florida Governor Ron DeSantis recently signed the Combating Corporate Espionage in Florida Act into law, and it will take effect on October 1, 2021. The new law was created to protect intellectual property in Florida from theft by foreign governments and their agents – but the Act also creates important new considerations for employers in their efforts to protect their closely held trade secrets. Likewise, the Act also re-emphasizes considerations for employers who hire employees from their competitors. What do Florida employers need to know about this new law, and what are the five steps you should consider taking to put yourself in the best position to protect your trade secrets?

An Overview of New Florida Law

Most notably, the Act establishes a new second-degree felony for any person who traffics in trade secrets and clarifies that a trade secret can include information or documents stored in electronic form. Therefore, any employee who, without permission, takes trade secrets or confidential business information from their employer now risks far more serious criminal liability.

In addition to enhancing the criminal penalties for trafficking in trade secrets, the Act now requires Florida courts to order restitution when a person steals or traffics a trade secret. The Act specifies that the restitution must include the "value of the benefit derived from the offense, including any expenses for research and design and other costs of reproducing the trade secret that the person has avoided by committing the offense." Therefore, if the development of a

Related People

Justin William McConnell
Partner
407.541.0880

Brett P. Owens
Partner
813.769.7512

trade secret was expensive and time consuming, then the restitution ordered could be substantial in amount and broad in scope. This provides greater protection for the victims of trade secret theft.

The Act also establishes the right for trade secret owners to seek injunctive relief in civil court and, "in exceptional circumstances," the right to recover a reasonable royalty for the use of a trade secret. Although similar remedies are already available under the Florida Uniform Trade Secrets Act and the Florida Valid Restraints of Trade or Commerce statute, employers can now bring claims under all three statutes to stop the use of a stolen trade secret and recover compensation when a trade secret is illegally taken or used.

5 Steps You Can Take to Minimize Risk

Employers can reduce potential claims or disputes over trade secrets by taking the following five steps:

1. *Create Policies and Procedures to Protect Trade Secret Information*
   Review existing policies and make any necessary updates to address issues that arise with using information stored electronically.

   Whether new policies are implemented or existing policies are maintained, you should ensure that employees receive notice of company policies and confirm their receipt and understanding of the policies. Additionally, you should consider whether confidentiality agreements are necessary for employees who routinely have access to confidential, proprietary, and trade secret information.

2. *Restrict Access to Trade Secret and Confidential Information*
   Create policies and procedures to ensure that company data and information are accessible to only necessary individuals and only when needed.

   You may also want to prohibit employees from using their personal devices to access company data. This would enable you to restrict the use of USB devices to those that are company-issued, encrypted, and that will only work on the company computer. From a data collection standpoint, you should also create logs of USB devices issued to employees. If an employee has only been using

Service Focus

Employee Defection and Trade Secrets

Related Offices

Fort Lauderdale

Orlando

Tampa

a company-issued device, doing so will make recovering company information easier when the employee leaves the organization.

3. *Proactively Work with Information Technology and Human Resources Personnel*
   You should work with your Human Resources and Information Technology teams to establish specific procedures for handling the departure of employees. By establishing procedures in advance and ensuring that the human resources and technology teams know how to implement the procedures in the event of a departure, you will restrict the ability of a departing employee to take company data. For example, you should establish a process for immediately disabling the employee's access to the company network, data, and e-mail upon termination of employment.

   Additionally, you should review the company information that is in the employee's possession and determine the process for returning the information prior to the employee's departure.

4. *Be Cautious When Hiring Employees from Other Organizations*
   If you are hiring employees who were privy to trade secrets of their prior employer, you must be especially cautious to ensure that the employee has not taken, used, or disclosed those trade secrets. Florida's new law creates potential liability for employers who employ individuals who bring trade secrets with them.

5. *Review Forensic Activity*
   When an employee leaves the company, you should consider taking steps to review the employee's forensic activity to determine if they were accessing files outside of their normal role; if they were printing excessively, printing outside of the normal business hours, or printing highly confidential company information; and if they were emailing company information to a personal account.

   Likewise, you should review the employee's work devices to determine the employee's access to files stored locally on the devices and whether the employee used flash drives or other external data storage media on the devices. The review and/or examination of an employee's company-issued device after their departure should be performed by a disinterested third-party vendor rather

than the employer's own IT professionals. That will eliminate the employee or their counsel's ability to allege the company doctored or manipulated the data on the device. Typically, an outside vendor will make a copy or "ghost" of the device.

What's Next?

We will be monitoring the new law for any developments that employers should be aware of in regard to the protection of the trade secrets and in mitigating the risk of hiring new employees who are in possession of their former employer's trade secrets. If your business has additional questions regarding the impact of the Combating Corporate Espionage in Florida Act, feel free to reach out to your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Florida offices.

We'll continue to monitor the status of this type of legislation and will provide updates as warranted, so make sure you are signed up for Fisher Phillips' Insight service to receive the latest news directly in your inbox.