A Lawyer's Confession: Don't Count on Contracts and Courts to Protect Your Company's Confidential Information

Insights
6.01.22

Many people were shocked by the recent leak of a Supreme Court draft opinion. The idea that an employee would subvert confidentiality rules at the nation's highest court on matters of national significance seemed far-fetched. But many companies with confidential business information know that confidentiality violations are commonplace. A breach may be somewhat harmless, such as when an employee emails a sensitive document to a personal account to work on it outside the office. Other times, a violation is deliberate. For example, an employee may violate your confidentiality policy by downloading a list of customer contact information to use for a new competing business. You may not regularly ask yourself what information workers have, where that information is stored, and how it could be stolen. But the answers to these questions could easily change every year. Why is it important to proactively protect your company's data and what steps do you need to take to avoid costly mistakes?

Litigation is Expensive and Unpredictable

While innocuous violations may be dealt with internally, companies spend tens of millions every year on litigation against employees and former employees who have deliberately absconded with confidential information. Many of these employees signed confidentiality agreements and other restrictive covenants prohibiting them from using the information outside of work or competing against their former employer. In some situations, even if an employee didn't sign an agreement, their conduct might violate a law designed to protect information, such as the Defend Trade Secrets Act or the Computer Fraud and Abuse Act. In rare cases, authorities will prosecute trade secret theft under criminal statutes.

But even the best written contracts and laws must be backed by a court order for enforcement, so litigation may be the only resort once information is taken. Note, however, that obtaining money damages is a long and expensive process and rarely provides adequate compensation for the harm caused to your business.

Here are four reasons to proactively avoid litigation:

1. **Judges are people.** The first step in stopping an employee from using improperly obtained confidential information is obtaining injunctive relief from a judge. There are approximately 3,200

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

federal judges and probably ten times as many state judges in America, many of whom have never owned or operated a business. Any particular judge's response to business concerns over the loss of confidential information is impossible to predict. A judge may be ideologically opposed to noncompete agreements. They may believe an employee who claims they will not use the purloined information in an identical job with a new employer. They may not appreciate the significance of the information or conclude it is not confidential. The bottom line is, a judge may not grant the relief your business needs to protect itself, even if the facts and law are on your side.

2. **Evidence is hard to develop.** One of the primary reasons to use a noncompete agreement –when state law allows for it – instead of a less restrictive non-solicitation or confidentiality agreement is that it is hard to determine whether a former employee is living up to contractual obligations at a new employer. The noncompete agreement, if enforced, offers the best protection to curb a former employee's ability or incentive to provide your confidential information to a competitor. Once a former employee is working for a competitor, it becomes difficult to track how the employee is using your confidential information. How will you know if your former employee has a conversation with their new colleagues that reveals your confidential information and results in you losing customers? You cannot count on someone confessing that confidential information was discussed. Even obtaining electronic information is difficult. Accessing your competitor's computer systems to run forensics will require both a court fight, and if successful, a large monetary investment.
3. **Litigation drains resources.** Litigation is not cheap, but attorneys' fees are often a minor expense compared to the time, effort, and stress placed on the employees who must provide information, assist in answering discovery requests, appear for depositions, attend mediations, and ultimately prepare for an appear at trial. Every hour an employee spends on a piece of litigation is an hour they did not spend on building your business.
4. **Good results don't fix all the damage.** Even if they receive a seven-figure award, most businesses would have rather prevented the theft of information and stayed out of court. Even after the judgment, employers may continue to feel the effects of the breach if customers never return, your market share is reduced, or your competitor's reputation improves through the use of your information.

This is not to say that litigation has no value. Businesses can and do win many cases. Courts may block employees from competing with you, and a strong track record of going to court to enforce restrictive covenants and confidentiality agreements can decrease the likelihood of violations. Filing suit can be evidence in a later proceeding of the steps the company has taken to protect its information; an important aspect of proving the existence of a trade secret.

Moreover, the importance of contracts and confidentiality policies should not be downplayed. In the case of many laws, a business's failure to have these tools will in and of itself undermine legal claims. Companies that do not adopt them and ensure they comply with the relevant jurisdiction's laws are playing with fire.

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

Common Mistakes to Avoid

In today's world, many businesses fail to take critical steps to prevent the theft of information. Here are four of the most common mistakes businesses make and tips to avoid them:

1. **Failing to revise cell phone policies.** Too many employers think there is no need to provide employees with phones since everyone has a smart phone. And when asking employees to use their personal cell phones for business, employers may fail to require the use of security software that allows the company to wipe the phone if the employee departs. Allowing employees to use personal cell phones to conduct company business is risky because cell phones are often the first – and sometimes only – place important company information is stored. For example, when a salesperson obtains a new contact's number, it goes in their phone.

   Additionally, employees may receive text messages with key data from customers, which is rarely removed from phones, even after it is uploaded to a company's server. Moreover, cell phones have personal backups. Even if the company owns the phone, if an employee operates it under their personal smartphone ID, the employer's information will be backed up to a cloud database accessible only by the employee. Therefore, you should ensure you control the data on employees' phones and the backups. Otherwise, an employee can walk out with every contact's information, and you might have to seek a court order to have the information deleted.
2. **Leaving remote systems vulnerable.** The pandemic created a demand for remote work that many businesses never expected to see. When remote work was mandatory due to shutdowns, businesses sped through the process of implementing systems. This led to a host of security vulnerabilities from external bad actors, like a hacker, and internal bad actors, like a disgruntled employee who leaves with the algorithm for the business's most important product. Many rudimentary remote systems allow individuals to download reams of data from their work computer while sitting in the comfort of their living room. Remote systems can allow employees to copy data with no evidence it was copied. Therefore, you should take the time to understand how your remote systems work and whether they are protected from external and internal threats.
3. **Failing to use computer tracking tools.** Many computer operating systems offer a host of tools that allow you to track what employees do on their company-issued computers. These tools are invaluable when determining if an employee has copied an important file or maliciously deleted information. But many of these tools are turned off by default or can be turned off by a savvy user. Businesses must understand the tracking settings on the computers they provide to employees, turn on the appropriate options, and control settings through administrator rights to prevent disabling. Software can be added that will provide additional information such as a record of all files copied whenever a thumb drive is inserted.
4. **Forgetting to track printers.** Perhaps it's counterintuitive, but you may have trouble detecting when an employee has printed information and walked away with a paper copy. Most employees do not want to create hard copies because of the additional work involved in re-inputting data

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

electronically. But you should still consider monitoring printers to safeguard sensitive information. Businesses with critical documents can implement software that tracks all the electronic versions of a document and keeps a log of who prints the document and how many copies have been printed. More importantly, you can limit printing capabilities to ensure hard copies of confidential documents are not taken or shared.

Conclusion

We will continue to monitor the latest developments related to confidential business information and restrictive covenants, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have questions, please contact the author of this Insight, your Fisher Phillips attorney, or any attorney in our Employee Defection and Trade Secrets Practice Group.

Related People

Edward F. Harold
Regional Managing Partner
504.592.3801
Email

Service Focus

Counseling and Advice

Employee Defection and Trade Secrets

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.