3 Reminders for Employers Mitigating the Risk of Trade Secret Misappropriation in the Face of Mounting Layoffs

Insights
5.08.23

While economists continue to debate the prospects for a recession, layoffs are impacting employees across the U.S., and not just in the technology sector. Given the greater potential for trade secret misappropriation in the current economic climate, what can employers do to mitigate the risks? As a threshold matter, you must ensure that all trade secrets – including confidential and proprietary information – are subject to reasonable security measures to prevent unauthorized disclosure. As a quick refresher, here are three additional steps you should consider taking to protect your information, particularly in a time of economic uncertainty when you may be facing difficult decisions, including a reduction in force.

1. **Review and Potentially Revise Key Policies and Practices**

   Review your current policies that prohibit the unauthorized use or disclosure of trade secrets and restrict use of personal devices, such as external drives to store, download, or transfer confidential company information. You should also assess your physical security measures that restrict access to facilities and areas where confidential information is used and stored. Additionally, you should consider providing training to all employees that reinforces relevant policies and procedures and explains the disciplinary consequences for their violation.

   Consider requiring employees with access to confidential and proprietary information to sign nondisclosure agreements. Additionally, you may want to utilize restrictive covenants – such as non-competition and non-solicitation provisions – as appropriate and where authorized by applicable law.

2. **Manage Access to Data and Devices**

   Ensure all employees with computer access are provided with unique passwords (that are regularly changed). Furthermore, access to confidential and proprietary information should be limited to a need-to-know basis, and you should consider utilizing data loss prevention software to detect and promptly investigate suspicious employee computer activity. Additionally, company-issued devices of departing employees should be imaged and retained when there is a reasonable suspicion that trade secret misappropriation has occurred.

3. **Remind Departing Employees of Their Obligations**

   You should also consider adopting contractual provisions and policies that require departing employees to immediately return company property, allow an inspection of personal devices used for work, and participate in an exit interview.
   Departing employees should be provided with a letter reminding them of their contractual obligations – and you should attach a copy of any non-disclosure, non-solicitation, or non-competition agreement signed during employment. If trade secret misappropriation or breach of restrictive covenants is discovered, promptly send cease and desist letters to former employees and their new employers. Injunctive relief should be sought without delay when pre-litigation efforts to secure compliance fail.

Conclusion

We will continue to monitor the latest developments and provide updates as warranted, so you should ensure you are subscribed to Fisher Phillips' Insight System to gather the most up-to-date information directly to your inbox. If you have questions, please contact the authors of this Insight, your Fisher Phillips attorney, or any attorney in our Employee Defection and Trade Secrets Practice Group.

Related People

William E. Altman
Regional Managing Partner
248.433.8710
Email

Greg Grisham
Partner
901.333.2076
Email

Service Focus

Employee Defection and Trade Secrets

Litigation and Trials