The Rise of Trade Secret Litigation: Are You Prepared to Stop Your Trade Secrets from Walking Out the Door? (Part Two)

Related Professionals

Charles F. Billington III

George L. Stevens

Aaron M. Williams

Related Services

Intellectual Property

Labor and Employment

CLIENT ALERT | 3.9.2026

Part one of this series highlighted the historic high that trade secret litigation hit in 2025 with more than 1,550 cases filed in courts across the United States and suggested proactive, common-sense steps that businesses could take with respect to trade secret governance. But even businesses that take those steps will, at some point, face an attempt by departing employees to take their trade secret, confidential, and proprietary information as they leave. This edition addresses what businesses can do before, while, and after that happens.

Exfiltration of trade secrets (or generally confidential and proprietary information) can be accomplished in a number of ways. While instances involving "old school" methods of theft such as printing and taking documents or taking unauthorized photos of documents still occur, most methods are electronic in nature: emailing documents to a non-company address; uploading documents to a non-company cloud application; or copying documents onto a non-company external flash or hard drive. And however effectuated, exfiltration tends to occur in a narrow window between when an employee is in the process of interviewing for a new job and the last day an employee has access to the company's systems.

So, what can businesses do? Proactively:

- To prevent theft **before** it potentially occurs—and throwing back to Part One—businesses should identify trade secret, confidential, and proprietary information and secure it appropriately. This should include limiting access to those who need it and implementing a system that tracks who accesses what document and when they do so. Businesses should also consider deploying robust confidentiality and/or non-disclosure agreements that provide contractual rights protecting information that may fall short of trade secrets but are nonetheless valuable, proprietary, and confidential.
- To catch theft **while** it is potentially occurring, businesses should implement systems that flag suspicious activity to appropriate information security personnel. This could include instances of an employee accessing third-party cloud storage sites; sending email

correspondence to common personal domains like “Gmail” or “yahoo;” and connecting unapproved external storage devices.

- To catch theft **after** it potentially occurs—and ensure critical evidence to any trade secret case is available—businesses should implement a standing policy of preserving departing employees email folders and system user accounts for a period of time following their departure and implement a standing policy of gathering and holding departing employee devices before resetting and putting them back into circulation.

All of the above will position a business well should it discover, after departure, that an employee left to join a competitor and may have taken trade secret, confidential, or proprietary information with them. In the event of such a suspicion, a business should:

- Immediately place the employee’s already-preserved email folders and user account on an indefinite hold, beyond the automatic hold implemented by policy;
- Immediately ensure that the employee’s devices are not tampered with or placed back into circulation, and consider whether they should be forensically imaged; and
- Work with information security professionals and counsel to search the employee’s email and user accounts (and devices, if applicable) for suspicious activity.

Trade secrets cases are won or lost on the evidence businesses can muster when it finds out that a former employee was a bad actor. Speedy preservation of evidence is critical. Employees will often delete emails or wipe devices in efforts to cover their tracks, to varying degrees of success. Having a robust, uniformly applied policy automatically preserving potential sources of evidence for all departing employees will help ensure a business does not lack the ability to gather important evidence if it is blindsided. Taking swift, deliberate action to search those sources when a business is given reason to be suspicious will ensure that a business is walking into litigation with potentially decisive, overwhelming evidence rather than trying to piece it together on the fly.

This is the conclusion of a two-part series by our intellectual property and labor and employment groups designed to cover best practices related to trade secrets and your business. You can read part one here.

Upcoming Webinar:

The authors of this series will be hosting a webinar on Wednesday, April 8, 2026 at 12pm ET to further dive into these issues. Learn more and register.