

Five Strategies for Protecting Trade Secrets

Article By:

Emma R. Schuering

Eric E. Packel

In a post-Defend Trade Secrets Act world, employers have a host of civil remedies available to them for the misappropriation of trade secrets under both state and federal law. To obtain relief, an employer must establish that the information it claims is subject to trade secret protection is, in fact, protected as confidential and secret. Below we outline five actions an employer might consider to demonstrate it has taken the necessary measures to protect the secrecy of its confidential information.

1. **Written agreements with employees who have access to trade secrets.** These agreements may contain confidentiality, non-disclosure, non-solicitation, or non-competition provisions. To be effective, it is critical that such agreements define clearly what constitutes “confidential information,” and include a clause affirmatively requiring the return of such “confidential information” upon the termination or resignation of the employee.
2. **Written policies governing employee conduct.** Employers should set forth clear rules for marking and maintaining confidential information, such as written instructions related to copying and sharing of confidential information. Employers can also include restrictions on the sharing or disclosure of confidential information in employee handbooks or other policies that are shared with all employees.
3. **Limiting employee access to trade secrets.** This may include limiting physical access to documents stored in hard copy, by, for example, limiting locations where the confidential information is maintained, locking those locations, and tracking individuals accessing the information. Employers should also take care to protect electronically-stored information by, for example, employing password protection on documents and databases containing confidential information, restricting access to such documents on external devices, and implementing security monitoring measures.
4. **Limiting outsiders’ access.** Similarly, employers should limit outsider access to areas housing confidential physical documents and devices with access to electronically stored information. Depending on the information, this may include the use of security guards or cameras, perimeter fencing, visitor badges with log in and out procedures, and security card access to certain areas.
5. **Controls on public dissemination.** Employers may consider designating an employee to review and approve publicly disseminated information, including publications, presentations,

promotional materials, and website content to ensure trade secret information is not inadvertently disclosed. Employers should also carefully evaluate the scope of information shared in meetings with potential partners or customers, and may further consider requiring meeting participants to enter into non-disclosure agreements if confidential information must necessarily be shared.

Employers should remember that any security measures should be regularly monitored, audited, and updated to maintain their effectiveness. Efforts to maintain these procedures may pay dividends should the employer have to pursue a former employee for trade secret theft.

© Polsinelli PC, Polsinelli LLP in California

National Law Review, Volume VII, Number 338

Source URL: <https://natlawreview.com/article/five-strategies-protecting-trade-secrets>