thepharmaletter
Up to date news for the Pharmaceutical and Biotechnology industries

Rogue employees and protecting your company trade secrets and confidential information

By David Prange & Chris Pinahs

19-12-2017 Comments (0)

In light of a recent case, David Prange (pictured above, left) and Christopher Pinahs, from USA-based law firm Robins Kaplan, provide an Expert View piece containing potentially crucial insights into improving trade secret protection.

In recent years, a greater awareness has emerged for protecting company intellectual property (IP) with complimentary trade secret and patent-protection plans. This awareness is driven in part by the Defend Trade Secrets Act of 2016, which created a federal civil cause of action for trade secret misappropriation, and the increased scrutiny being placed on patents by the America Invents Act and case law addressing patent eligibility.

While trade secret protection is not new, the increased scrutiny on patent protection should push companies to consider a more holistic approach to protecting its IP. Companies should consider developing protection policies for trade secrets and have an action plan in place if a dispute arises. Although patent rights may not be lost by unauthorized use or disclosure, trade secrets potentially are lost if quick action is not taken when an unauthorized disclosure occurs.

The recent lawsuit filed by Par Pharmaceutical against QuVa Pharma in federal court in New Jersey should provide additional incentive to develop a readiness action plan. Par sued QuVa and three former Par employees for trade secret misappropriation. Par alleges that QuVa engaged in a 'poaching campaign' to hire key Par employees, who supposedly misappropriated confidential and proprietary information relating to manufacturing/storage methods, operating details, and business strategies for Par’s injectable Vasostrict (vasopressin injection) drug product.

Despite claiming robust security measures, Par asserted that trade secrets were stolen for almost a year leading up to the former Par employees’ exit, including through direct email correspondence among the former employees and QuVa, and by downloading numerous Par documents to personal hard drives just prior to departure.

Assuming the allegations as true, the Par v QuVa lawsuit illustrates how difficult it can be to prevent employees with malicious intent from circumventing company confidentiality and protection policies.

Still, by implementing a trade secret protection plan and moving quickly upon discovery of a defecting employee’s potential misappropriation, companies can mitigate the risk of the potential loss of trade secret or confidential information.

A protection plan may include expressly identifying an individual responsible for trade secret protection and tracking; minimizing access to trade secret and confidential information when an employee departs; and developing an action plan to use if a misappropriation is discovered.

Having a plan in place, and educating employees of company trade secrets protection and consequences associated with breaching company rights, can have a deterrent effect.

Make someone responsible

Identifying an individual accountable for developing and implementing a trade secret protection policy should be a first step. Individual tasks may include implementing reasonable protection measures to prevent uncontrolled dissemination of trade secret and confidential information, and may extend to cataloging trade secrets for protection. Those responsibilities may also include leading periodic presentations to educate employees on company confidential information and trade secret procedures. If there is later litigation involving a trade secret, these protection procedures may be used as evidence to meet a company's burden of demonstrating that it took reasonable steps to preserve the secrecy of its trade secrets.

Take action when an employee leaves

When an employee gives notice of departure, a company should move quickly to limit continued access to sensitive company information. After receiving an employee notice, the company should consider monitoring workplace computer and email usage for signs that the employee may be downloading or emailing proprietary company information. A company should also consider discontinuing employee access to confidential information altogether. The scope of limitation will depend on the employee's role and responsibilities, and the nature of the termination. Following a notice of termination, a company should also consider conducting an employee exit interview, one purpose of which is to provide the departing employee with notice of the types of information the company considers to be proprietary.

Companies should further consider performing an immediate review of any computer activity that occurred prior to the employee providing notice. For example, in the Par case, days before giving notice, one departing employee downloaded numerous Par documents concerning Vasostrict, including Food and Drug Administration inspection protocols, accounting spreadsheets, and board of directors presentations. A quick survey of employee computing activity may spot potential misconduct that can be addressed before an employee leaves the company, and before valuable trade secret and confidential information is disseminated to others.

Have a plan

A company should have a plan in place to address any potential misuse of company trade secret or confidential information. Knowing who to call and when such a call is warranted may reduce any potential dispute resolution timeline and limit the financial impact of any misappropriation. The Par case serves as a cautionary reminder that quick action is needed to preserve a company's competitive advantage in the marketplace, and potentially preserve profits.

There, Par filed for a preliminary injunction seven months after the former employee-defendants left the company, and four months after Par filed its lawsuit. Delay in seeking a preliminary injunction usually does not favor the party seeking the injunction. Presumably, Par engaged in an investigation of its former employees' conduct, leading to the discoveries giving rise to the case. But even if Par's injunction motion is successful, QuVa will have had months of unfettered access to Par's trade secret information concerning its Vasostrict product prior to any court- issued remedial action. Having a defined readiness plan in the event a company discovers a misappropriation allows for quick action, potentially saving a trade secret from public disclosure, and maintaining any marketplace advantage a company may have.

Being prepared and acting quickly upon the occurrence of employee misappropriation of company trade secret or other confidential information is integral when trying to maintain company market position and profitability. Companies should consider designating an individual responsible for implementing a protection plan, and addressing the ownership of proprietary information with departing employees. Failing to do so may result in a scramble when trying to prevent further harm, once a misappropriation of trade secret information is discovered.

Expert View | Focus On | In Depth | Legal | Management | Par Pharmaceutical | Pharmaceutical | QuVa Pharma | ROBINS KAPLAN LLP