pharmaceutical COMPLIANCE MONITOR

How New Trade Secret Legislation Impacts Pharma Compliance Programs

March 29, 2013

Jose P. Sierra

Two recently enacted criminal statutes have raised the stakes not only for individuals and corporations that misappropriate another company's trade secrets, but also for the companies responsible for safeguarding those trade secrets from theft. For the legal, human resources, and compliance departments of a pharmaceutical company, these statutes create both risks and opportunities and underscore the importance of re-assessing the company's policies, training, and internal controls relating to trade secrets and other proprietary information.

On December 28, 2012, the Theft of Trade Secrets Clarification Act of 2012 (Clarification Act) was enacted in response to the Second Circuit's ruling in U.S. v. Aleynikov, 676 F.3d 71 (2nd Cir. 2012). In that case, Sergey Aleynikov, a former computer programmer at Goldman Sachs & Co., developed a computer source code for Goldman's high-frequency trading (HFT) system that permitted large volume trading decisions in a fraction of a second. Before leaving his employer to work for a Chicago-based start-up seeking to develop and implement its own HFT system, Aleynikov uploaded over 500,000 lines of source code to a German server. After downloading the source code at home and sharing the information with his new colleagues, Aleynikov was arrested, charged, and convicted under the Economic Espionage Act (EEA) and National Stolen Property Act (NSPA). He was sentenced to more than eight years in prison, fined $12,500 and denied bail pending appeal.

Approximately one year into his sentence, the Second Circuit reversed Aleynikov's conviction and ordered the charges dismissed. Although unsympathetic to Aleynikov, the Court determined that Goldman's source code did not constitute physical or tangible property (and, therefore, was not a "good" under the NSPA) and was neither "produced for" nor "placed in" interstate or foreign commerce, (and, therefore, was not covered under the EEA), since it was designed only for internal use, created no good for interstate commerce, and was never sold or licensed to third parties. As a result, Aleynikov was released from prison (although he was later re-arrested and charged under New York state law).

In response to Judge Calabresi's concurring opinion, in which he essentially invited Congress to amend the EEA to cover the kind of conduct in which Aleynikov engaged, Congress swiftly passed the Clarification Act, and a little more than two weeks later, passed the Foreign and Economic Espionage Penalty Enhancement Act of 2012 (Penalty Enhancement Act). The Clarification Act amends the EEA to cover internal trade secrets "related" to both products and services "used in or intended for use in interstate or foreign commerce, to the economic benefit to anyone other than the owner thereof." The Penalty Enhancement Act, in turn, significantly increases the financial penalties where the trade secret misappropriation benefits a foreign entity. Under the Penalty Enhancement Act, the maximum fines were raised from $500,000 to $5 million for individuals and from $10 million or "three times the value of the stolen trade secret" for organizations, "including expenses for research and design and other costs of reproducing the secret that the [misappropriating] organization has thereby avoided." The latter provision is particularly significant for foreign entities engaged in or suborning trade secret theft, since the value of the stolen trade secret can easily exceed the previous $10 million cap.

Implications and Risks for Compliance Programs

It would be a mistake for U.S. based pharmaceutical companies to view the Clarification Act and the Penalty Enhancement Act amendments to the EEA as merely expanding a prosecutor's "criminal tools" to go after trade secret thieves and foreign companies and governments primarily engaged in economic espionage in the defense and high-tech industries. In fact, only months before Aleynikov, Yuan Li, a Chinese national and former Sanofi-Aventis research chemist, pled guilty to one count of trade secrets theft under the EEA after she was caught downloading information about drug compounds to her home computer by email or a USB thumb drive and then attempting to sell the data to Abby Pharmatech LLC, the U.S. unit of a Chinese company. Li was later sentenced to 18 months in prison, directed to pay Sanofi $131,000 in restitution and ordered deported after completing her sentence. Although Li was apprehended before she could sell the drug compound data to a willing buyer, observers have noted that it was Li's incompetence, not Sanofi's security system, which led to the crime's discovery before Sanofi could be harmed.

The Li case confirms not only that pharmaceutical companies are prime targets for trade secret theft (both foreign and domestic), but underscores the need to regularly reassess the adequacy of a company's firewalls for safeguarding intellectual property, such as trade secrets, and other proprietary information. The risks of not doing so can be severe and can include millions of lost dollars in research and development and an even greater loss in competitive advantage. Indeed, companies that risk and lose hard-earned competitive advantages as a result of inadequate safeguards may need to disclose such security "breaches" to shareholders in securities filings, particularly if the company is required to take legal action against the thief and/or the company that acquired the information. Moreover, although somewhat of a stretch, it is not inconceivable to imagine an aggressive plaintiffs' attorney filing suit against a company's board of directors for failing to exercise appropriate oversight over their company's policies and internal controls (i.e., compliance program) related to protecting the company's intellectual property, trade secrets, and other proprietary information.

Preventing Future Problems

Although the Clarification Act and the Penalty Enhancement Act amendments to the EEA provide federal prosecutors with new weapons in fighting trade secret theft – and provide companies with the potent option of making a criminal referral to a local federal prosecutor – these laws also provide compliance officers with a more immediate and practical opportunity (and statutory justification) to reassess and upgrade relevant policies and internal controls. There are several steps pharmaceutical companies can and should undertake in the wake of the Clarification Act and the Penalty Enhancement Act amendments.

First, while it is standard for all employees to sign confidentiality and non-compete agreements, companies should update these agreements and include warnings about the civil and criminal penalties under the EEA for misappropriating trade secret and other proprietary information. Vendors should also be required to sign similarly updated confidentiality/non-disclosure agreements. Second, to the extent not already in place, the company's code of conduct, policies, and procedures should all reflect that confidentiality is a core company value and reinforce the importance of identifying and classifying trade secret and other proprietary information (e.g., by marking such as "confidential"). Third, annual training on the importance of maintaining the company's confidential and proprietary information should be updated – or undertaken if not in place – to include the EEA's provisions and penalties, using the Li case as a prime example. Employee signatures or certifications (written or electronic) on all relevant agreements, policies, and training materials should also be obtained and maintained in personnel files and training logs.

Fourth, with respect to beefing up internal controls, companies should, among other things, (a) map identified trade secrets and other proprietary information to their business owners and, using state-of-the-art security techniques, restrict access to the information to these employees and, if

necessary, to others on a “need to know basis” only; (b) improve security to detect large or unusual data exports via email, download or other means; (c) require individuals who have or have had access to proprietary information to submit for review and approval any written materials that are intended for external use (e.g., articles, manuscripts, abstracts, papers, slides for conferences and seminars, etc.); and (d) conduct annual or periodic audits designed to test the adequacy of the company’s policies, training, and internal controls.

Conclusion

By taking proactive measures such as the ones described above, pharmaceutical companies can leverage the newly strengthened EEA to improve an often neglected but increasingly important area of compliance that is tied directly to enterprise risk management. Although no set of policies, degree of training, or system of internal controls can guarantee that a cunning employee will never succeed in stealing trade secrets or other valuable proprietary information, a solid compliance program in this regard should go a long way towards protecting a company’s trade secrets and avoiding either civil litigation against the trade secret thief and/or misappropriating organization or referring the matter to a federal prosecutor.