akerman

Practice Update

Federal "Defend Trade Secrets Act of 2016" Passes in Congress Today: How the DTSA Affects Your Business

April 27, 2016

Over the past decade, as companies moved into a digital world, so too moved their most valuable assets and proprietary information. As a result, the United States witnessed a significant uptick in data theft and misappropriation as companies scrambled to protect their information, not only from outside theft, but also from internal employee misconduct. A law review article in 2010 assessed that trade secret theft cost companies as much as $300 billion per year. To assist in the battle, additional states began adopting the Uniform Trade Secrets Act (UTSA), with 48 states currently having adopted some version of the UTSA. Concern existed that the variation among the state laws, however, caused inconsistent outcomes. Congress sought to resolve this through S. 1890, starting in 2014, and, with amendments, became what is now known as the Defend Trade Secrets Act of 2016 (DTSA). On April 4, 2016, the Senate Judiciary Committee passed S. 1890, on April 20, 2016, the House Committee approved S. 1890 by voice vote, and on April 27, 2016, the bill was passed.

The provisions and remedies found in the DTSA closely mirror those in the UTSA. Specifically, the DTSA provides for:

- a universal definition of a trade secret, requiring that: a corporation take reasonable efforts to protect the information and the information

Related Work

Intellectual Property
Labor and Employment
Litigation
Trade Secrets, Restrictive Covenants, and Unfair Competition

Related Offices

Chicago

provides independent economic value from not generally being known

- actual damages, restitution, exemplary relief (up to two times the award of actual damages), and attorneys' fees
- injunctive relief for both actual and threatened misappropriation

The DTSA also, however, provides numerous unique tools for companies to protect its assets not otherwise found in state counterparts. Those provisions include:

- federal jurisdiction, allowing cases to be brought directly in federal court
- the allowance for ex parte property seizures (with certain limitations); this provision allows a plaintiff to pursue government assistance in recovering misappropriated trade secrets before providing notice of litigation to a defendant
- an immunity provision to protect whistleblowers who report a violation of law
- the ability to pursue criminal penalties
- an amendment to the Racketeer Influenced and Corrupt Organizations Act to add a violation of the Economic Espionage Act as a predicate act for a RICO violation

Notably, the DTSA does not preempt any state trade secret laws, allowing aggrieved parties to still pursue claims under both state and, now, federal law. Also notable is that the DTSA does not specifically preempt other causes of action that may arise under the same common nucleus of facts, like several state statutes.

What Does this Mean for Your Business

First, as true whenever a change in the law occurs, you should have qualified counsel review your policies and contracts to ensure they are properly crafted to comply with the change in the law. Such

review should include determining whether your contracts and policies contain the necessary language regarding immunity, as failure to include such language may preclude the recovery of exemplary damages and/or attorneys' fees. Specifically, the DTSA places an affirmative duty on employers to provide employees notice of the new immunity provision in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information." Compliance includes providing a "cross-reference" to a policy given to the relevant employee that identifies the reporting policy for suspected violations of law. The review should also include considering whether the definition in your agreements matches that found in the DTSA, and tailoring any definition to avoid claims of overbreadth.

Second, the passage of the DTSA provides an opportune occasion to conduct an audit of your confidential and proprietary information to ensure that proper steps are being undertaken to fully and completely protect that information. Such audits should include not only identifying your most important assets, but also a review of security policies and procedures related to protecting such information.

Third, your company should review its employee policies, such as hiring, termination, and training. The most common form of misappropriation occurs via departing employees. Creating simple consistent steps during the on-boarding and off-boarding of employees, in addition to periodic training, will greatly reduce the risk of such theft.

Finally, you should review company contracts with contractors and vendors and assure adequate protections exist in those relationships to guard your trade secrets.