DTSA Review for Inside Counsel

This summary highlights the important features of the Defend Trade Secrets Act of 2016 (DTSA), the potential impact of the legislation, and recommended actions and strategies.

Effective May 11, the DTSA amends the Economic Espionage Act (18 U.S.C. §§ 1831-39) and creates for the first time an optional federal civil remedy for trade secret misappropriation, providing some distinct advantages:

- a single statute, rather than variable state laws
- nationwide service of process
- consistency through application of the Federal Rules of Civil Procedure
- a judiciary experienced in cross-border issues

Most definitions and remedies are the same as the Uniform Trade Secrets Act (UTSA), which applies (in varying form) in forty-seven states. But the DTSA adds special provisions:

- ex parte seizure by federal marshals of property containing a trade secret, if it is about to be destroyed or removed from the jurisdiction
- injunctions against departing employees whose behavior indicates that they cannot be trusted to keep information confidential when moving to a competitor; but this "threatened" misappropriation must be based on bad behavior and not just on the sensitivity of what they know
- corporate whistleblower immunity for disclosures in confidence to law enforcement or in a sealed pleading; this applies to employees, contractors and consultants, and notice has to be included in new or updated confidentiality agreements

Industry had long been pressing for a federal civil law, to accommodate the increasing importance of data assets in all their forms, as well as the heightened risk to those assets due to networks and mobile technology. The DTSA should cause recalibration of strategic thinking in this area, not only about possible litigation but also about how companies act to protect valuable information against loss or contamination.

The new law requires that trade secret owners exercise "reasonable efforts" to protect their data, and although this generally means restricting access to those with a need to know, judges will expect a sophisticated approach that begins with knowing, at least by category, what should be protected, and then considers:

- the value of the trade secrets: what harm would the organization suffer if the information becomes known to competitors
- the risks of loss or contamination: external threats from cyberattacks, weak system controls, and sloppy management of business transactions; but note that the internal threat of careless behavior by staff is the most common vector for loss
- the costs of various mitigation measures: technology is important for electronic security, but people and processes (including training and monitoring) can have as large an impact

Because of the pervasive importance to the business of intangible assets, you should ensure review of relevant programs, not only to protect the integrity of the company's own trade secrets, but also to prevent contamination by unwanted information from third parties, for example through onboarding new employees or carrying out competitive intelligence.

As a matter of litigation strategy, the DTSA raises these considerations:

- cases involving actors in multiple states, or in other countries, are very good candidates for federal filing
- in New York or Massachusetts, where the UTSA has not yet been adopted, the DTSA may provide broader protection, and the same may be true in some states where the UTSA has been significantly amended
- when there is clear evidence of an imminent misappropriation by a known actor, ex parte seizure may be an effective remedy
- whether to assert collateral state law claims, including under the UTSA, since the DTSA is not preemptive
- where the case is not very strong, it may make more sense to file in state court, where judges generally are less likely to demand detailed specification of secrets and to grant summary judgment

For now, we suggest taking these steps:

- amend all new and revised confidentiality agreements with employees, contractors and consultants to include notice of whistleblower immunity as required by the DTSA
- review existing external confidentiality agreements, particularly involving non-U.S. entities, to determine how they might be enforced in U.S. courts, and consider steps to require or encourage dispute resolution in the U.S. for future transactions involving exchange of confidential data
- consider implementing a comprehensive review of the company's information protection strategy and risk management procedures, to conform with best practices

Contact:

For further information please contact Jim Pooley at jpooley@orrick.com or 650-285-8520.