KING & SPALDING

Client Alert

International Trade & Litigation Practice Group

May 12, 2016

Third Try is a Charm - Defend Trade Secrets Act of 2015 Enacted Into Law

For the third consecutive year, Congress introduced legislation to create a civil federal cause of action for trade secret misappropriation. Unlike previous years, the identical Defend Trade Secrets Act ("the DTSA")[1] was introduced in both the Senate and House of Representatives. The Senate passed an amended version of the DTSA by a vote of 87-0 on April 4, 2016. The House passed the revised bill by a vote of 410-2 on April 27, 2016. The president signed the bill and it became law on May 11, 2016.

The DTSA was created in response to the increasing importance of trade secrets in today's economy and the increasing theft of trade secrets as global trade expands and critical data become digitized. It has been estimated that trade secret theft exacts a cost on U.S. companies of between $160 and $480 million each year.[2] The DTSA seeks to remedy shortcomings with existing criminal and state laws, including lack of federal resources to investigate trade secret theft, and variations and limitations in state laws that make them not wholly effective in a national and global economy.[3]

The DTSA builds on the existing Economic Espionage Act (18 U.S.C. §§ 1836-1839), and creates a private federal civil action for "an owner of a trade secret that is misappropriated . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." The new federal cause of action is designed to supplement, not pre-empt, already existing state laws relating to trade secrets. It applies to any misappropriation where an act occurred on or after the date of enactment, and provides for a three-year statute of limitations period that runs from date of discovery of the misappropriation or the date it should have been discovered "by the exercise of reasonable diligence."

The DTSA includes provisions similar in many respects to the Uniform Trade Secrets Act ("UTSA"), which has been adopted in various forms by 48 states, as well as several provisions not found in the USTA or most state laws.

Definitions of Trade Secret and Misappropriation

The DTSA provides specific definitions of "trade secret" and "misappropriation." The DTSA modifies the existing definition of "trade secret" found in the Economic Espionage Act, 18 U.S.C. § 1839, in at least one important respect by incorporating familiar language found in the UTSA and state trade secret statutes. The prior definition required a trade secret to

For more information, contact:

William J. Sauers
+1 202 626 2920
wsauers@kslaw.com

Jeffrey M. Telep
+1 202 626 2390
jtelep@kslaw.com

Jeffrey David Mills
+1 512 457 2027
jmills@kslaw.com

Michael W. Johnston
+1 404 572 3581
mjohnston@kslaw.com

Steven T. Snyder
+1 704 503 2630
ssnyder@kslaw.com

Thomas J. Spulak
+1 202 661 7948
tspulak@kslaw.com

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

King & Spalding
Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

derive independent economic value from not being generally known or ascertainable by the "public." The DTSA strikes the term "public" and adopts language similar to most states,[4] and requires a trade secret to derive independent economic value from not being generally known to or ascertainable by, "another person who can obtain economic value from the disclosure or use of the information."

The DTSA definition of "misappropriation" is identical to that provided in the UTSA. This is designed to make clear that the DTSA is not intended to alter the balance of current trade secret law or alter specific court decisions.[5] Misappropriation includes:

(1) "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means," and

(2) "disclosure or use of a trade secret of another without express or implied consent by another" in three specific circumstances.

"Improper means" is defined identically to § 1(1) of the UTSA[6] and includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage. However, reverse engineering and independent derivation of the trade secret are not improper means.

Ex Parte Seizure

Perhaps the most controversial provision of the DTSA is the ability of a trade secret owner to seek expedited relief in the form of an *ex parte* seizure of property. Congress considered the *ex parte* seizure provision "an important remedy for trade secret owners because it enables a trade secret owner under limited controlled conditions, to proactively contain a theft before it progresses and the trade secret is lost."[7]

An *ex parte* seizure is only available "under extraordinary circumstances where necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action." The final version of the DTSA states that an application for an *ex parte* seizure may not be granted unless "the court finds that it clearly appears from specific facts" that:

- An injunction or other form of equitable relief would be inadequate because the party would "evade, avoid, or otherwise not comply" with the order;
- Factors similar to those for temporary injunctive relief are met: the applicant is likely to succeed on the merits of the trade secret claim; the applicant would suffer immediate and irreparable injury absent a seizure order; and the harm to the applicant outweighs the harm to the legitimate interests of the party subject to the order and any third parties that may be harmed by the seizure;
- The person subject to the seizure "has actual possession of the trade secret and property to be seized";
- "The application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized";
- "The person against whom seizure would be ordered, or persons acting in concert with such persons, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person"; and
- "The applicant has not publicized the requested seizure."

The requirement for actual possession of the trade secret was included to protect third parties from seizure. For instance, the operator of a server on which another party has stored a misappropriated trade secret, or an online intermediary such as an internet service provider, would not be subject to seizure because their servers, and the data stored upon them, would not be in actual possession of the defendant.[8]

The DTSA also provides specific requirements for any seizure order entered. A seizure order must (1) set out findings of fact and conclusions of law, (2) provide for narrowest seizure of property necessary to achieve the purpose of the order, (3) be conducted in a manner that minimizes any interruption of business of third parties and – to the extent possible – the defendant, (4) prohibit access or disclosure until the parties are heard in court, (5) after the hearing, limit access to the seized materials as necessary, (6) provide guidance to law enforcement regarding the execution of the seizure; (7) be raised in a hearing no later than seven days after the order; and (8) require the party seeking the seizure to provide security adequate to compensate for damages resulting from a wrongful or excessive seizure or attempted seizure. At the required hearing, the party who requested the order has the burden to show that the findings of fact and conclusions of law necessary to support the order are still in effect.

The DTSA further includes specific provisions pertaining to execution of *ex parte* seizure orders. For example, the seizure order must be carried out by a Federal law enforcement officer. The Court can allow state and local law enforcement officials to participate in the seizure, as well as an approved technical expert who is unaffiliated with the applicant. However, neither the applicant nor its agent may participate. Any information seized is taken into the custody of the Court, and appropriate measures must be taken to protect the confidentiality of seized material unrelated to the trade secret information seized. A person who claims to have an interest in the seized materials may make a motion, which may be heard *ex parte*, to encrypt any materials seized or to be seized.

As a further protection for parties subject to an *ex parte* seizure order, the DTSA provides a cause of action for damages caused by a wrongful or excessive seizure. Any "person who suffers damage by reason of a wrongful or excessive seizure" has a cause of action against the applicant and may seek the same relief provided for wrongful seizures under 15 U.S.C. § 1116(d)(11) of the Trademark Act.

Remedies

The remedies available under the DTSA are similar to state law remedies in many respects and are intended to coexist with, not preempt, influence, or modify applicable state laws. Injunctive relief is available to prevent any actual or threatened misappropriation, and may require affirmative actions to be taken to protect the trade secret. Where injunctive relief would be inequitable, future use of the trade secret may be conditioned on a reasonable royalty payment for no longer than the period of time for which the use could have been prohibited (*e.g.* the time it would take to independently develop the trade secret).

The DTSA also permits injunctive relief to prevent "threatened misappropriation," more commonly referred to as the "inevitable disclosure doctrine." Courts interpreting state trade secret laws have reached different conclusions on the applicability of the inevitable disclosure doctrine.[9] Many jurisdictions have declined to recognize, or have rejected, this doctrine when interpreting state trade secret laws. The DTSA includes provisions that seek to mitigate concerns with respect to the doctrine. For example, the DTSA provides that an injunction may not "prevent a person from entering into an employment relationship" and may not "otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business." In addition, any conditions placed on such employment "shall be based on evidence of threatened misappropriation and not merely on the information the person knows."

The DTSA also identifies specific damages that may be obtained. Damages can be obtained for actual loss caused by the misappropriation and for unjust enrichment not accounted for by actual loss. In lieu of damages measured by any other method, damages can be measured by a reasonable royalty for the unauthorized use or disclosure.

For the successful plaintiff, the DTSA allows for up to double damages and attorney fees where there is a finding of willful and malicious misappropriation. The availability and amount of enhanced damages differs among the various state trade secret laws. In addition, the prevailing party can seek attorney fees where claims or motions to terminate an injunction were made in bad faith.

Immunity for Disclosing or Using Trade Secrets

The DTSA provides for immunity from criminal or civil liability for disclosing or using a trade secret in certain circumstances. Immunity is provided to those who disclose a trade secret in confidence to government officials for the purpose of reporting or investigating a suspected violation of the law. Immunity is also accorded to those who disclose a trade secret in a complaint or other document filed in a lawsuit or proceeding if filed under seal. Finally, anyone who files a lawsuit for retaliation by an employer may disclose the trade secret to his or her attorney and use the trade secret in the court proceeding in limited circumstances.

The DTSA requires employers to provide notice of the immunities set forth in the DTSA in any employment contract that governs the use of a trade secret or confidential information entered into or updated after the effective date of the DTSA. The employer can fulfill this notice requirement by providing a cross-reference to a policy document that sets forth the employer's reporting policy for suspected violations of the law. If an employer fails to comply with the notice requirement, it may not obtain exemplary damages or attorney fees in any action against an employee who was not provided notice.

* * *

---

1 H.R. 3326 introduced in the House on July 29, 2015; S. 1890 introduced in the Senate on July 29, 2015.
2 "Defend Trade Secrets Act of 2016," House Report 114-529 issued April 26, 2016 ("House Report") at 3-4.
3 *Id.* at 3-4.
4 New York state law follows the Restatement (First) definition of a trade secret that additionally requires that information be in use to qualify as a trade secret.
5 "Defend Trade Secrets Act of 2016," Senate Report 114-220 issued March 7, 2016 ("Senate Report") at 10.
6 *Id.*
7 *Id.* at 3.
8 Senate Report at 6.
9 Senate Report at 8 n.16.