May 11, 2016

Landmark Trade Secrets Law Creates New Federal Civil Cause of Action and Compliance Obligations for All Employers

Earlier today, President Obama signed into law the Defend Trade Secrets Act (DTSA). The landmark legislation is significant. For the first time, federal civil protection is afforded to trade secrets alongside copyrights, patents and trademarks.

What is a Trade Secret?

A "trade secret," as the phrase implies, is a form of intellectual property that is unknown to the public and that provides a competitive advantage due to reasonable measures to keep it confidential. Trade secrets have no expiration date and are not examined, issued or registered by any government office. Common examples of trade secrets include customer lists, customer contract details, data, business plans, business strategies, formulas, methods, software codes, processes, procedures and techniques.

Past Legal Landscape and Shortcomings

Economic Espionage Act: Prior to passage of the new federal trade secrets law, companies could only seek relief under federal law for trade secret theft by convincing government lawyers to bring claims under the criminal provisions of the Economic Espionage Act (EEA)(18 U.S.C. § 1831 *et seq*.), which makes it a crime to steal a trade secret "for the economic benefit of anyone other than the owner . . . while intending or knowing that the offense will injure any owner of that secret." The EEA does not provide a civil cause of action for trade secret misappropriation.

State Laws: Although some thieves of trade secrets (especially thieves of computer code) went to prison under the EEA, companies previously had to seek civil relief for trade secret theft exclusively under state laws. Statutes modeled upon the Uniform Trade Secrets Act (UTSA) have been adopted by 47 states, the District of Columbia, Puerto Rico and the US Virgin Islands, but there are variations among the statutory language from state to state. Moreover, there are meaningful differences in how the various state courts have interpreted these laws, with decisions often being informed by separate bodies of state common law that predate the enactment of trade secret statutes. The result is a patchwork quilt of unpredictable and differing definitions, standards, remedies, statutes of limitation, and procedures. The new law aims to bring uniformity and reliability to this situation and harmonize civil trade secret litigation.

Computer Fraud and Abuse Act: Additionally, before passage of the new federal trade secrets law, the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030), which targets individuals and entities who access or use a computer without proper permission, was the closest equivalent to a federal civil cause of action for cyberespionage. Like the EEA,

For more information and an in-depth look at how the law might affect your organization, please contact any of the following members of Katten's **Intellectual Property** practice, or a member of Katten's **White Collar, Investigations and Compliance**; **Privacy, Data and Cybersecurity**; or **Employment Law and Litigation** practices.

Peter J. Riebling
+1.202.625.3598
peter.riebling@kattenlaw.com

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Thomas J. Maas
+1.312.902.5258
thomas.maas@kattenlaw.com

Julia L. Mazur
+1.312.902.5280
julia.mazur@kattenlaw.com

Jeffrey A. Wakolbinger
+1.312.902.5570
jeff.wakolbinger@kattenlaw.com

the CFAA is a federal criminal statute, but the CFAA was designed specifically to address malicious computer hacking. Although the CFAA provides a potential federal civil cause of action in cases involving trade secrets misappropriated by hacking, liability under the CFAA requires accessing a protected computer without authorization, or exceeding authorized access, with an intent to defraud, and actually obtaining something of value. But under the CFAA, an employee only "exceeds authorized access" to company computers when he or she violates the company's computer access and use restrictions about which he or she has actual notice.

International Trade Commission: The International Trade Commission (ITC) also provides means to remedy harm caused by cyberespionage. The ITC is authorized under 19 U.S.C. § 1337 to prevent the importation of products that incorporate misappropriated trade secrets where the misappropriation took place overseas. But the ITC's remedial cease-and-desist power is limited only to imported articles, and no damages are available.

Key Points of New Federal Trade Secrets Law Everyone Should Know

Effective Date: It applies to the misappropriation of trade secrets that occurs on or after May 11, the date President Obama signed the DTSA into law. It does not apply retroactively.

Statute of limitations: Three years.

Non-Preemption: Existing state laws are not pre-empted, thus allowing plaintiffs the choice between federal or state court, and federal or state law, for claims involving misappropriation of trade secrets related to a product or service used, or intended for use, in interstate or foreign commerce. Because the DTSA was enacted pursuant to Congress's Commerce Clause power, it does not confer federal jurisdiction over purely intrastate activities.

Definition of Trade Secret: The definition of a "trade secret" in the EEA has been amended. Previously, a trade secret was defined, in part, as information deriving independent economic value from not being generally known to (or readily ascertainable through proper means by) the *public*. Now that definition has been amended, such that the question is whether that information derives value from not being generally known to (or readily ascertainable by) another *person who can obtain economic value from such information*. The revised definition of a "trade secret" is thus: "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."

Definition of Misappropriation: The newly defined term "misappropriation " means either: (1) the acquisition of a trade secret of another by "improper means" (with knowledge or reason to know that this acquisition was by improper means) or (2) a number of scenarios involving the disclosure or use of such a trade secret without consent, which involve knowledge (or reason to know) that the trade secrets had been acquired by improper means, accident, or mistake, or that there had been a duty to maintain the secrecy of the trade secret or limit its use. Thus, liability can extend, not only to the original bad actor, but also to certain individuals who knowingly continue to use or disclose the trade secret. This definition is largely the same as what is provided in the UTSA.

Definition of Improper Means: "Improper means" includes "theft, bribery, misrepresentation, breach or inducement of breach of a duty to maintain secrecy, or espionage through electronic or other means." This definition matches the definition provided in the UTSA but it also goes on to provide that "improper means" does *not* include "reverse engineering, independent derivation, or any other lawful means of acquisition."

Jurisdiction: No diversity of citizenship is required. Federal courts have original federal jurisdiction over claims brought, so long as the trade secrets at issue are "related to a product or service used in, or intended for use in, interstate or foreign commerce."

Seizures: The law contains an important remedy that is not normally granted under state trade secret laws—*ex parte* seizures of property in "extraordinary circumstances" to prevent the propagation or dissemination of the trade secret that is the subject of the action, giving plaintiffs the ability to move quickly with tremendous early leverage in litigation.

Determining Extraordinary Circumstances Necessary for a Seizure: Before a court will issue an *ex parte seizure*, the trade secret owner applying for a seizure must show "extraordinary circumstances" exist. To do so, the applicant must establish each of the following eight factors: (1) a temporary restraining order (TRO), preliminary injunction or another form of equitable relief would be inadequate because the party to which the order would be issued would evade, avoid or otherwise not comply with such an order; (2) an immediate and irreparable injury will occur if a seizure is not ordered; (3) the harm to the applicant of denying the seizure outweighs the harm to the legitimate interests of the person against whom seizure would be ordered, and substantially outweighs any harm to third parties; (4) the applicant is likely to succeed in showing that the information is a trade secret and the person against whom seizure would be ordered misappropriated the trade secret of the applicant by improper means or conspired to use improper means to misappropriate the trade secret of the applicant; (5) the person against whom seizure would be ordered has actual possession of the trade secret and any property to be seized; (6) 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; (7) the person against whom seizure would be ordered, or persons acting in concert with such person, 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 (8) the applicant has not publicized the requested seizure.

10 Additional Checks Against Seizure Abuse: (1) Seizure orders may only be issued upon submission of an affidavit or verified complaint; (2) the order must be the narrowest necessary to achieve the purpose; (3) the order must direct that the seizure be conducted in a way to minimize any business operations of third parties and, to the extent possible, not interrupt the legitimate business operations of the person accused of misappropriation; (4) the person obtaining the order must provide the security amount determined by the court for the payment of damages for a wrongful seizure; (5) the requestor of the seizure may not participate in the seizure; (6) the court must protect the seized property from disclosure and access until a hearing; (7) the court must hold a hearing no later than the seventh day after issuance of the order; (8) at the hearing, the applicant has the burden of proving that seizure was necessary under the circumstances; (9) upon request, courts must take appropriate action to protect from publicity the person against whom the seizure order is directed; and (10) anyone claiming an interest in the seized subject matter may move at any time (including *ex parte*) to encrypt that material.

Seizure a Double-Edged Sword: A seizure order will be a helpful tool when a TRO or preliminary injunction may not avoid irreparable harm, for example, when a defendant is seeking to flee the country or on the cusp of imminently disclosing the trade secret to others. But companies should beware that such provisions in the law can be used against them, too. Your company's biggest competitor, believing your company stole their trade secrets, can now potentially convince a federal judge to seize competitive plans, strategies, data and information in your company's possession—without prior notice.

Litigation Discovery Benefit: By bringing civil actions for trade secrets theft in federal court, plaintiffs can take advantage of nationwide subpoena power.

Injunctive Relief: Injunctive relief may be issued to prevent both actual and threatened misappropriation. Courts, however, may not issue injunctions that prevent a person from entering into an employment relationship or that otherwise conflict with state laws on employee mobility, "without evidence of actual or threatened misappropriation." In others words, the law does not follow the "inevitable disclosure" doctrine; i.e., it does not allow injunctions against employment merely because a departing employee has knowledge of a trade secret in his or her head.

Damages: A plaintiff may claim its actual damages plus any unjust enrichment, or in the alternative, damages measured by a reasonably royalty. In cases of willful or malicious misappropriation, exemplary damages also are available up to twice the amount of actual/reasonable royalty damages, as are attorney's fees. Attorney's fees are available to a defendant as well, but only if a claim is brought in bad faith.

Heightened Criminal Penalties: In addition to the new, independent, private cause of action, the federal criminal penalties for theft of trade secrets also have been increased. Previously capped by statute at $5 million, these criminal damages may now be as much as three times the value of the stolen trade secret to the offending organization (including the costs avoided by that organization for legitimate research, design and reproduction of the trade secret). Economic espionage and theft of trade secrets have also been added to the list of "racketeering activities" under the Racketeer Influenced and Corrupt Organizations Act (RICO, 18 USC 1961 *et. seq.*), which opens up potential federal criminal liability (and civil actions with treble damages) against conspiracies to misappropriate trade secrets.

Immunity for Whistle Blowers and Disclosures in Pleadings: No individual may be held civilly or criminally liable for the disclosure of a trade secret in confidence to federal, state or local government officials or to government attorneys when made to investigate or report a suspected violation of law, or when made in a complaint or other document filed in a lawsuit if such filing is made under seal.

New Employer Compliance Obligations: Employers are *required* to include notice of the whistle blower immunity described above under the new federal trade secrets law in any contracts with individual employees, contractors or consultants that govern the use of a trade secret or other confidential information that are entered into or updated after May 11. If an employer does not provide the above notice, the employer may not be awarded exemplary damages or attorney's fees in a federal trade secret litigation against such persons. Notice obligations may be satisfied by cross-referencing a separate policy document.

What You Should Do Now

Recent developments in patent law have raised significant questions about whether patents can protect certain valuable intellectual property assets. For example, the US Supreme Court's decision in *Alice Corp. v. CLS Bank International*, and its progeny, have led to the increased scrutiny of patent claims directed to business methods, business processes and computer-implemented inventions. The America Invents Act has provided patent challengers new ways to invalidate or narrow patents, as well as instituting many other changes whose effects may not yet be fully appreciated. These factors are forcing more and more companies to evaluate how they can leverage the trade secrets laws to effectively protect their most valuable competitive assets. The passage of the new federal trade secrets law will only fuel the increase of trade secret litigation. Thus, successful navigation of this new legislation will be critical to the success of many companies.

Although trade secret theft often happens quickly and quietly with the single click of a cell phone or computer key, trade secret litigation is often lengthy and highly disruptive. Such cases usually present complex, highly technical factual issues. Being mindful of a few simple guidelines in advance can help you avoid trade secret theft before it happens, not to mention save your company significant expense.

Trade secret claims most frequently are the result of: (1) conduct of current or former employees and consultants; (2) disclosures by persons outside the company after confidential business discussions; or (3) conduct of foreign or domestic hackers. Therefore, companies should initially review and comply with the following "best practices" checklist:

- Require confidentiality agreements as a condition of employment (or of continued employment) and as a condition of engagement of any contractors or consultants.
- *Immediately* include notice of whistle blower immunity under the new federal law in any contracts or confidentiality agreements with employees, contractors or consultants that govern the use of a trade secret or other confidential information that are entered into or updated after May 11, so the company is in compliance with federal law and may avail itself of exemplary damages or attorney's fees in a federal trade secret misappropriation action against such persons.
- Require that a non-disclosure agreement (NDA) that carefully defines what is "confidential" be signed by persons outside the company before any discussions about confidential information take place.
- Inventory competitive data, information and materials to determine what likely falls within the definition of a "trade secret."

- Conduct an internal audit to confirm "reasonable measures" and protocols are in use to store and protect and prevent valuable information identified as a trade secret from dissemination, disclosure, theft, hacking/data breach or other inappropriate use.
- Provide employees with educational training and seminars about established policies and laws for trade secrets and confidential information.