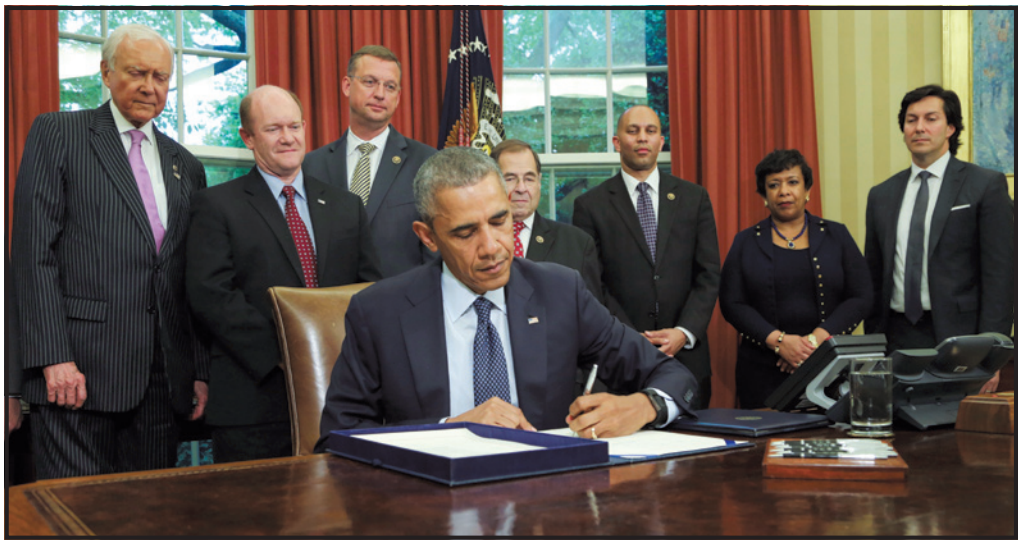
THE NATIONAL LAW JOURNAL
JUNE 27, 2016
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

How to Prepare for Theft of Company Information

Companies should take three steps now to ensure use of the Defend Trade Secrets Act.

BY NICK AKERMAN AND J JACKSON



AUDE GUERRUCCI

Done: President Obama signs the Defend Trade Secrets Act May 11.

In May, President Barack Obama signed into law the Defend Trade Secrets Act that creates a federal civil cause of action for the misappropriation of trade secrets. This new law amends the Economic Espionage Act, which makes it a federal crime to steal and use trade secrets. Title 18 U.S.C. 1831, et. seq. For companies that depend on confidential information to provide them a competitive edge, there are several proactive steps they should take to ensure their use and the full benefits of this statute if their trade secrets are stolen.

Most significantly, the Defend Trade Secrets Act, unlike the state trade secrets laws, provides for an ex parte "order for the seizure of property necessary to prevent the propagation or dissemination of the trade secret," upon a showing of "exceptional circumstance." Traditional state court equitable remedies are limited to a temporary restraining order and a preliminary injunction.

The law also makes the theft, possession and use of trade secrets a predicate act for the Racketeer Influenced and Corrupt Organizations Statue, which can form the basis of a civil RICO action for treble damages and attorney fees. (In the past, federal courts have been reluctant under most circumstances to find a RICO "pattern" for trade secrets theft as part of a scheme to defraud based on the mail and wire fraud statutes. See, e.g., *Bro-Tech Corp. v. Thermax* (E.D. Pa. 2009).

DEFINE TRADE SECRETS

An obvious first step for any company thinking it might use the Defend Trade Secrets Act is to inventory and define its trade secrets and specify them in company policies and employee and third-party confidentiality agreements.

The act follows the classic definition of a trade secret, as defined by state law, to mean "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." It makes no difference whether this information is stored on paper, electronically on a computer or is intangible information committed to memory. Section 1839 (3). The "information" must

"derive economic value, actual or potential, from not being generally known to, and being readily ascertainable through proper means by, the public." Id. at 3(B).

REASONABLE MEASURES

Identifying the company's trade secrets is critical to meeting the next requirement of the statute—"the owner has taken reasonable measures to keep such information secret." Id. At 3(A).

The U.S. Court of Appeals for the Seventh Circuit in *United States v. Lange*, which upheld a criminal conviction under the Economic Espionage Act of a disgruntled former employee who attempted to sell his company's secret manufacturing processes to third parties, is instructive on what constitutes reasonable measures: 1) the processes were physically secured in a designated room "protected by a special lock, an alarm system, and a motion detector"; 2) the documentation describing the process was limited with "surplus copies … shredded"; 3) certain information "in the plan" was "coded" with "few people" knowing the codes; 4) the documentation contained warnings of the company's "intellectual-property rights"; 5) "every employee received a notice that the information with which he works is confidential"; and 6) the company divided work among vendors to ensure "that none can replicate the product."

ADDITIONAL ACTIONS

The *Lange* listing is not exhaustive. Other measures such as confidentiality agreements, employee training programs, password-protected access and access to the confidential information on a "need to know" basis are traditionally relied upon by state courts in finding reasonable measures to protect the information, which measures apply equally to the Economic Espionage Act.

In addition, because most confidential information is maintained in computers or electronic databases, there needs to be an emphasis on policies, procedures and technology to protect such data.

The Defend Trade Secrets Act also provides for "reasonable attorney's fees" and "exemplary damages in an amount not more than 2 times the amount of" the compensatory damages if the theft is willful and malicious.

To be entitled to exemplary damages and attorney fees under the new law, employers must amend their employee agreements and/or policies.

Under the act, an employee "who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding if the individual—(A) files any document containing the trade secret under seal; and (B) does not disclose the trade secret, except pursuant to court order."

For an employer to receive exemplary damages or attorney fees under this statute, it must amend its employee agreements to provide "notice" of this "immunity" "in any contract or agreement with an employee that governs the use of a trade secret or other confidential information." An employer is "considered to be in compliance with the notice requirement," if it provides to its employees "a cross-reference to a policy document" setting "forth the employer's reporting policy for a suspected violation of law."

Taking inventory of trade secrets, reviewing and establishing reasonable measures to protect them, and amending confidentiality agreements will position companies to best utilize the new trade secrets law. The time to start thinking about using this new civil remedy is now, not in the future, when you learn someone has stolen your company's trade secrets.

NICK AKERMAN *and* **J JACKSON** *are partners in the international law firm Dorsey & Whitney. Both are members of the trial group and include among their specialties the protection of competitively sensitive information and trade secrets litigation. Akerman and Jackson can be contacted, respectively, at akerman.nick@dorsey.com and at jackson.j@dorsey.com.*