New Federal Law Offers Different Avenue for Trade Secret Protection

Carl E. Woock, Esq. In almost every industry, companies big and small rely on trade secrets to maintain an edge in a competitive marketplace. Trade secrets occupy a broad category of information that is commercially beneficial to a business and not generally known to the public. Some famous examples readily come to mind: the formula for Coca Cola or the secret behind the “nooks and crannies” in Thomas’ English Muffins. Other trade secrets are more conventional (and less tasty): for example, a customer list for a Kennebunk plumbing company, purchasing information for a Bangor hardware store, or a consumer market analysis performed by a local credit union, all of which may be protected by trade secret law. Unlike patent, trademark, or copyright protections, which eventually expire, trade secrets last for as long as the secret is kept. Once that secret is lost, though, it is lost forever. Until very recently, trade secrets were also different from trademark, copyright and patent law for another reason: trade secrets were primarily an object of state law. That is no longer the case. On May 11, 2016 President Barack Obama signed into law the federal Defend Trade Secrets Act of 2016 (“DTSA”). DTSA gives trade secret owners a new option to bring lawsuits for trade secret misappropriation using federal law and the federal courts. It has been called “most important piece of intellectual property legislation that Congress has passed in several years.” That might overstate the law’s significance, but this is certainly a development that businesses should take seriously. What are the practical implications of this new law? Well, if a former employee marches over to a competitor with a confidential list of clients, a business owner might now bring a misappropriation of trade secrets claim in federal, rather than state, court. There are some conditions. The business can only make use of the federal remedies if “the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.” DTSA uses an existing definition of “trade secret “ from the Economic Espionage Act—that is, "all forms and types of" various categories of information, regardless of how stored, if “the owner thereof has taken reasonable measures to keep such information secret” and “the information derives independent economic value, actual or potential, from not being generally known” to the public. From there, the definition of “misappropriation” is borrowed from the Uniform Trade Secrets Act adopted in most states, primarily defined as the “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,” or the “disclosure or use of a trade secret of another without express or implied consent by a person” who “used improper means to acquire knowledge of the trade secret.” If these conditions apply to the employee hawking a confidential list of clients, federal remedies may be on the table. Federal Remedies Are Both Familiar and New DTSA largely tracks with the remedies provided by the Uniform Trade Secret Act. Specifically, DTSA’s remedies include injunctive relief, actual damages, restitution, and exemplary damages of up to two times the actual damages, as well as attorneys’ fees. In contrast to the uniform state laws, DTSA permits *ex parte* civil seizure of property to prohibit the dissemination of a trade secret without advance notice to the other side in “extraordinary circumstances.” If prosecuted by the federal government, an offender also faces penalties from $5 million to the greater of $5 million or three times the value of the stolen trade secret. The headline, though, is that these remedies are available in federal court, which offers an intuitive upside. Without a uniform federal law, a company seeking to curtail the misappropriation of trade secrets would rely on one set of law in Maine (i.e., the Uniform Trade Secrets Act, which Maine has adopted), but an entirely different set of laws in Massachusetts (which is one of just two states that has

©2026 Norman Hanson DeTroy LLC All Rights Reserved

not adopted Uniform Trade Secrets Act). Under that scheme, it is possible that the same misuse of company secrets would result in inconsistent outcomes depending on which state hears the case. Ideally, DTSA will provide more predictability to businesses bringing this claim, while still permitting companies to use those long-standing state remedies when preferable. Holding Back High Praise On the other hand, DTSA is in some ways less wave-making than it could have been. For starters, one could argue that the law does not improve the legal landscape in a substantive way. The federal government already had the power to enforce trade secret laws through criminal and civil actions, and state laws are mostly uniform and consistent in offering private remedies. In that sense, the immediate consequence of DTSA is to complicate and disrupt existing trade secret law. Trade secret litigation was already capable of being tedious and expensive, but with dual layers of state and federal law, cases are bound to become more complicated, as well as more costly. Further, DTSA missed an opportunity to tailor protections for victims of cyber-hacking and cyber-espionage, a growing area of concern among some companies. Recent high-profile corporate hacks and espionage exploits have targeted Sony Pictures, DuPont, and Lockheed Martin, but smaller companies (often with comparatively less cyber-security) are also vulnerable to these types of attacks. A cynic might suggest that DTSA is merely the result of a dysfunctional Congress coming together to needlessly federalize legal protections already covered in near-uniformity by the states. What Business Owners Need to Know Today The main reason DTSA is generating some buzz is not because of what the law says, but rather the fact that it is going to affect many businesses. Exactly how it will affect businesses is less clear. Like with any new law, opinion is divided as to how DTSA's provisions will operate in the real world. For example, the *ex parte* civil seizure provision has the potential to offer swift and decisive justice to a victim of trade secret misappropriation, but it can also become a controversial weapon for bad faith actors who seek to unsettle their competitors. Hopefully, most businesses will not need to discover first-hand how the federal law plays out in practice. But two things are certain: first, DTSA will usher more claims into federal courts, either as a standalone claim or as related breach of contract or unfair competition claims (which are state law matters) make it to federal court via supplemental jurisdiction when attached to a federal law claim. Second, DTSA reaches almost every business, from your brother-in-law's general contracting company to your uncle's accounting firm. Arguably every business has methods, data, or information that might be considered trade secrets, and every business with trade secrets can be economically harmed if that information is stolen or misused. Business owners must therefore act in advance if they hope to take full advantage of the law. On that note, DTSA protects employees who disclose trade secrets in response to a court order or government investigation. In order to be eligible for all of the remedies created by DTSA, employers must provide notice of the statute's whistleblower immunity in any "contract or agreement with an employee that governs the use of a trade secret or other confidential information." That means confidentiality, non-disclosure, and non-compete agreements must be updated accordingly. Failure to do so may mean that a successful plaintiff cannot recover exemplary damages or attorneys' fees as otherwise allowed by the statute. Any business that may be affected by DTSA should also take this time to update policy manuals to include the appropriate immunity language. Form employment agreements used with employees who handle confidential business information will need to be modified. While agreements executed prior to May 12, 2016 are not required to have the whistleblower notice language, any businesses that entered into an employment agreement after May 12, 2016 will need to go back and amend those agreements to enjoy the full protection of DTSA. After all, if a company finds itself in the unfortunate situation of needing to use DTSA, it probably wants to have all of those brand new federal remedies at its disposal.

©2026 Norman Hanson DeTroy LLC All Rights Reserved