ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Harmonize Your Trade Secret Protection To Protect Your Assets

Technology, Privacy, and eCommerce


DTSA


DTSA

CHEAT SHEET

- ***The DTSA.*** Recognizing the importance of protecting trade secrets, Congress recently passed the Defend Trade Secrets Act (DTSA), creating a federal, private civil cause of action for trade secret misappropriation.
- ***EU Directive.*** The European Union has also recently recognized the importance of protecting trade secrets by adopting a Directive that governs and harmonizes trade secret protections throughout the European Union.
- ***Enter Brexit.*** Even in the wake of Brexit, the United Kingdom will likely follow the EU Directive because the country will still be a part of the European Union during the Directive's deadline of June 6, 2018. Many commentators argue that the Directive will be economically beneficial to the United Kingdom and supported by UK businesses.
- ***Protect and fortify.*** To better protect a company's trade secrets, in-house counsel should first identify its trade secrets, demonstrate that they have taken steps to keep the information a secret, remain vigilant in order to protect and preserve the value of the secret, attempt to recover what was lost, and regularly reassess the steps taken to protect and prevent theft.

Trade secrets are the lifeblood of many organizations. From startups to Fortune 100 companies, trade secrets are often among a company's most valuable assets.

A trade secret can include anything from a formula to a customer list. At its essence, a trade secret is something that is secret and has value due to its secrecy. Thus, for example, the formula for Coca-Cola has been a closely guarded trade secret since 1886. For years, only a small group of people knew the formula, which was not written down. Later, in the early 1900s, the formula was written down, but placed in a vault, then a bank, and in 2012, at the World of Coca-Cola in Atlanta. Commentators credit the mystery behind the formula as lending strength and quality to the Coca-Cola brand.

As valuable assets, trade secrets are often targets of theft. Whether by former employees or competitors, trade secret theft can be catastrophic to an organization. In fact, it is estimated that as of 2014, trade secret theft accounted for nearly one to three percent of the GDP of the United States.

Recognizing the importance of protecting trade secrets, Congress recently passed the US Defend Trade Secrets Act (DTSA), creating for the first time a federal, private civil cause of action for trade secret misappropriation.

Like the United States, the European Union has also recently recognized the importance of protecting trade secrets by adopting Directive 2016/943, of the European Parliament and of Council of 8 June 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Directive), which governs and harmonizes trade secret protections throughout the European Union. And, despite Brexit, the United Kingdom appears likely to follow the Directive.

In light of these recent developments, companies now have a more powerful arsenal of weapons to fight trade secret theft. This article provides a brief summary of the recent developments and discusses best practices to help protect trade secrets.

Nuts and bolts of trade secrets

Before the DTSA, a trade secret owner had two avenues to seek redress for misappropriation in federal court: (1) bring a state law misappropriation claim under the court's diversity jurisdiction, or (2) attempt to pursue criminal sanctions under the Economic Espionage Act of 1996.

The problem with the first option is that state law protecting trade secrets varies, both in text and application. For example, state trade secret laws vary in some very fundamental ways; from how "trade secrets" are defined, to the applicable statute of limitations, to remedies. This lack of consistency creates uncertainty that could serve to chill progress and the creation and ownership of IP

The problem with the second option is that the trade secret owner must convince the US Department of Justice (DOJ) to prosecute the case. Then, even if the DOJ agrees to prosecute, the trade secret owner has little ability to influence the proceedings. And, if the trade secret owner files its own separate case under state law, the DOJ prosecution may take priority and the state case can be stayed.

Defend Trade Secrets Act

On May 11, 2016, Congress enacted the DTSA. The DTSA provides trade secret owners with a federal, private, and civil right of action for trade secret misappropriation, but does not preempt state law. In particular, the DTSA allows an owner of a trade secret that is misappropriated to bring an action in federal court "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." The statute of limitations for bringing a case under the DTSA is three years.

The DTSA — consistent with the Uniform Trade Secrets Act (UTSA) on which state law protecting trade secrets is often based — provides that a trade secret must not be generally known to, or readily ascertainable by, "another person who can obtain economic value from the disclosure or use of the information." Also similar to the UTSA, the DTSA defines "misappropriation" of a trade secret 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." "Misappropriation" under the DTSA additionally includes:

- "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;
    - at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was:
        - Derived from or through a person who had used improper means to acquire the trade secret;
        - Acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or,
        - Derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret.
    - before a material change of the position of the person, knew or had reason to know that:
        - The trade secret was a trade secret; and,
        - Knowledge of the trade secret had been acquired by accident or

> mistake." Thus, under the DTSA, a former employer or distributor who was under a duty to maintain the secrecy of the trade secret and nonetheless disclosed it without consent, could be liable under the DTSA."

The DTSA also includes a whistleblower provision, which provides protection from liability for confidential disclosure of a trade secret to the government or in a court filing. It also protects employees from retaliation by an employer for reporting a suspected violation of law and allows the employee to disclose the trade secret information under seal in the court proceeding.

As for remedies, the DTSA allows for injunctive relief, monetary damages for actual loss, unjust enrichment, and a potential for reasonable royalties in lieu of other monetary damages. Trade secret owners also have the chance to recover exemplary damages up to two times the damages awarded (and attorneys' fees) if the trade secret is willfully and maliciously misappropriated.

One of the most controversial aspects of the DTSA is the *ex parte* seizure provision that allows a trade secret owner to request, without notice, the seizure of property to prevent the dissemination of trade secrets. But, in cases since its enactment, courts have seemingly limited the remedy to extraordinary circumstances. Trade secret owners, thus, may not rely too heavily on the ex parte seizure provision as such relief has not been routinely granted.

Another interesting issue that has arisen since the enactment of the DTSA is whether it can be applied to misappropriation that took place before the DTSA's effective date of May 11, 2016. Courts have largely concluded that a trade secret owner can proceed with a DTSA claim even if the misappropriation occurred before May 11, 2016, if at least some of the wrongful conduct took place after that date.

The first DTSA case to verdict, *Dalmatia Import Group v. Foodmatch, Inc.,* No. 16-cv-02767 (E.D. Pa.), provides additional clarity regarding the importance of timing to a DTSA cause of action. On February 27, 2017, the jury in Dalmatia awarded the plaintiff US$2.5 million in damages, including US$500,000 for misappropriation of trade secrets. The complaint alleged that the defendants misappropriated the plaintiff's proprietary recipe and production process for the company's fig jam, including claims for misappropriation of trade secrets, trademark infringement, trademark counterfeiting, conversion, and breach of contract.

Following the jury verdict, the defendants asked the court to decline to enforce it because the jury was not properly instructed regarding the differences between the state and federal trade secret claims and that the verdict included damages before the enactment date of the DTSA. Ultimately, on May 3, 2017, the court entered judgment and awarded treble damages on the trademark counterfeiting claim, bringing the final award to US$5.2 million. The parties are now in the midst of post-trial briefing. In any future appeal, the court may need to address how to adequately plead the federal and state claims for trade secret misappropriation, as well as how to appropriately instruct the jury on the differences.

In addition to *Dalmatia Import,* there have been numerous other cases under the DTSA. Recently, trade secret owners have used the DTSA to pursue misappropriation claims involving various types of intellectual property, including self-driving cars. For example, Waymo — a subsidiary of Google's parent company, Alphabet — sued Uber, claiming that one of Waymo's former employees stole key technology that he used to start his own competing self-driving car company, which Uber acquired.

This relatively new enforcement vehicle is on the upswing. Both with high-tech and low-tech

companies, the fierce search for talent that accompanies development efforts and the public attention generated by companies like Apple and Google, we should expect more DTSA cases filed as employees move from company to company.

EU Directive

Like the United States, the European Union has recently attempted to unify its regime for protecting trade secrets. In November 2013, the European Parliament and the Council of the European Union proposed the adoption of a new Directive governing and harmonizing trade secret protections throughout the European Union. Nearly three years later, on June 8, 2016, the EU formally adopted the Directive. The Directive requires member states to adapt their national laws to conform to the Directive's provisions by June 9, 2018.

The Directive provides uniform, baseline standards on several different aspects of law: what constitutes a "trade secret," a framework for judicial proceedings regarding trade secret protection cases, and remedies for trade secret owners whose rights are infringed. For example, the Directive defines a "trade secret" as "information that meets all of the following requirements:

- Is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- It has commercial value because it is secret; and,
- It has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

The Directive also describes what constitutes an unauthorized disclosure of trade secrets, including "unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder" without the holder's consent. Even if the trade secret thief received the trade secret from another source, the Directive — like the DTSA — imposes liability if the infringer "knew or ought, under the circumstances, to have known" that the trade secret had originally been acquired or used unlawfully by direct or indirect means. Unlike the DTSA, however, the Directive expressly provides for several methods by which the acquisition of a trade secret should not be considered unlawful, such as where it is independently created; discovered through investigation of publically available information; or uncovered through the "exercise of the right of workers . . . to information and consultation."-Finally, the Directive includes a "catch-all" provision that exempts disclosure through practices "in conformity with honest commercial practices."

> **A trade secret owner must remain vigilant in order to protect and preserve the value of its trade secrets. When appropriate, an owner must assess when a threat is present and investigate whether a theft has occurred. Once an owner has confirmed that a theft has occurred, the owner must determine exactly what was taken.**

The Directive creates two distinct avenues for trade secret owners to use the judicial process to enforce their rights: provisional measures that can be implemented before a hearing on the merits (Articles X and XI); and post-hearing remedies, including injunctions (Article XII) and damages (Article XIV). Even before the trade secret owner receives a hearing, the Directive requires its member states to develop temporary, stop-gap mechanisms by which trade secret owners can protect the use and disclosure of their trade secrets while the case is pending. Similar to the DTSA,

the Directive authorizes judicial authorities to order the seizure of any “suspected infringing goods,” or require that these goods be delivered elsewhere in order “to prevent their entry into, or circulation on, the market.”

A number of remedies are available to trade secret holders after a hearing on the merits. First, the trade secret owner may receive “damages appropriate to the actual prejudice suffered” by the infringer’s disclosure. Second, the court has an arsenal of injunctive relief awards it can impose on the defendant: cessation or prohibition of trade secret use, disclosure, or acquisition; prohibition on importation or production of goods utilizing the trade secret; and, perhaps most significantly, the destruction of “all or part of any document, object, material, substance, or electronic file containing or embodying the trade secret.” Third, judicial authorities can impose “corrective measures” regarding any goods produced that incorporate the trade secrets, including the goods’ recall, destruction, or alteration to remove the infringing elements.

United Kingdom adoption of the EU Directive

Most commentators agree that even in the aftermath of “Brexit,” the United Kingdom will likely follow the Directive first and foremost because the United Kingdom will still be part of the European Union when the Directive’s deadline of June 6, 2018. Further, even if no legal obligation existed for the United Kingdom to follow the Directive, many commentators argue that the Directive will still be economically beneficial to the United Kingdom and supported by UK businesses. Before the Directive, the United Kingdom had already constructed “a well-developed and relatively sophisticated framework for the handling of trade secrets,” but the framework lacked definitions of “trade secrets” and other important elements that the Directive provides. For this reason, commentators argue that “the Directive is likely to be helpful in that it will codify and clarify aspects of the existing law without fundamentally altering the legal landscape and categories of protection available to companies.”

Best practices for protecting trade secrets

Identify

A trade secret owner must first identify its trade secrets. Trade secrets can be almost anything that is secret and has value by virtue of its secrecy. Common examples of trade secrets include customer lists, pricing information, marketing plans, manufacturing methods, designs, computer code, customer buying preferences, business plans, and formulas. Trade secrets can even include failed attempts at manufacturing a product and unsuccessful attempts to sell products.

A trade secret owner must also identify the value of its trade secrets. For example, in certain circumstances, a company may wish to hire an expert to provide a formal valuation of the company’s trade secrets. In other cases, a company may identify a trade secret’s value by reference to its own books and records.

Protect

In order to maintain confidential information as a trade secret, a trade secret owner must demonstrate that they have taken steps to keep the information secret. Common steps include restricting access to trade secrets to only those who need to know this information, requiring execution of a non-disclosure agreement before disclosing the trade secret, labeling documents (and the containers in which they are stored) as confidential trade secrets, password-protecting access to electronic copies

of trade secret information, requiring employees to change their passwords monthly in order to access trade secret information, surveillance of areas in which trade secrets are disclosed, monitoring of computer activity of employees with access to trade secrets, restricting access to areas in which trade secrets are stored and disclosed, requiring employees to sign-in and sign-out when entering areas where trade secrets are disclosed or housed, shredding paper copies of trade secret information, employee training identifying trade secrets and how to protect them, entrance and exit interviews, and post-employment letters confirming continuing confidentiality obligations.

The level of security measures taken to protect trade secrets will, of course, depend on the resources of the trade secret owner and nature of the secrets. But even simple security measures can be effective at helping protect trade secrets. Take the example of cell phones — a company may wish to restrict the use of cell phones in areas where trade secrets are disclosed. This will help prevent the cell phone photos containing trade secrets from being posted on social media sites, thereby destroying the secrecy of this information. In a recent incident, a photo of the Orlando Magic's offseason plans was leaked when a player's agent tweeted a photo of his client signing a contract with the Magic — but a list of the Magic's potential trade possibilities and free-agent targets was featured in the background.

A company can also guard against its employees using a former employer's trade secrets. Common steps include execution of confirmation of non-use of former employer's trade secrets during on boarding, counseling new employees regarding non-use of former employer's trade secrets, restricting the use of non-approved methods to upload information onto company computers (i.e., external hard drives, online data sharing sites), and monitoring large data transmissions involving new employees.

Investigate

A trade secret owner must remain vigilant in order to protect and preserve the value of its trade secrets. When appropriate, an owner must assess when a threat is present and investigate whether a theft has occurred. Once an owner has confirmed that a theft has occurred, the owner must determine exactly what was taken. Often, when dealing with electronic information, companies rely on their information technology departments to assist in the investigation of the theft, including compiling evidence of the identity of the thief and the extent of the theft.

Recover

A trade secret owner should, when appropriate, attempt to recover what was lost and take immediate steps to prevent further loss. Common examples of recovery are cease and desist letters and lawsuits. On this front, delay can be fatal. In a noteworthy case, a Florida district court denied a preliminary injunction in a trade secret misappropriation case because, among other things, the plaintiff waited over four months from discovery of the misappropriation to file suit.

Reassess

After an owner experiences a loss, it should reassess the steps it is taking to protect its trade secrets in light of the loss. Often, there are many lessons to be learned from a loss and unlearned lessons are bound to lead to future exposure.

Conclusion

The increasing rate at which innovation occurs and the reach of new innovations into every corner of business and personal life are obvious, from facial recognition technology to unlock your iPhone X to Oracle SaaS licenses to power a business's finance operations. This increases the rate of creation of proprietary trade secrets. But even in non-high tech industries, the mobility of employees, fluidity of business relationships, and the ease and faster speed at which information can be exchanged add to the need for increased vigilance in protecting company's trade secrets. The DTSA and EU Directive are ways in which the law is keeping up with these realities and providing new tools to fight misappropriation of trade secrets. The examples of best practices above identify ways companies attempt to safeguard their trade secret assets and aid in pursuing potential trade secret claims.

Gregory Lewis provided assistance for this article.

Further Reading

18 U.S.C. § 1836(b)(1).

18 U.S.C. § 1836.

18 U.S.C. § 1836(d).

18 U.S.C. § 1839(3)(B). Courts have relied on UTSA precedent to interpret the DTSA. See, e.g., Kuryakyn Holdings, LLC v. Ciro, LLC, No. 15-cv-703-jdp (W.D. Wish. Mar. 15, 2017); Henry Schein v. Cook, No. 15-cv-03166-JST (N.D. Cal. June 22, 2016).

18 U.S.C. § 1839(5)(A).

18 U.S.C. § 1839(5)(B).

See 18 U.S.C. § 1833(b).

See 18 U.S.C. § 1833(b)(2).

See, e.g., OOO *Brunswick Rail Mgt. v. Sultanov,* No. 5:17-cv-00017-EJD, 2017 WL 67119 (N.D. Cal. Jan. 6, 2017); *Balearia Caribbean Ltd. Corp. v. Calvo,* No. 1:16-cv-23300-KMV (S.D. Fla. Aug. 5, 2016).

See, e.g., Adams Arms, LLC v. Unified Weapons Sys., No. 16-cv-01503, 2016 WL 5391394 (M.D. Fla. Sep. 27, 2016); Syntel Sterling Best Shores Mauritius Ltd v. Trizetto Group, Inc., No. 15-CV-211 (S.D.N.Y. Sept. 23, 2016).

Dalmatia Import Group v. Foodmatch, Inc., No. 16-cv-02767, Dkt. No. 280 (E.D. Pa. Feb. 27, 2017).

Dalmatia, Dkt. No. 321 (May 3, 2017).

Directive 2016/943, of the European Parliament and of Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure 2016 O.J. (L 157).

Id. at art. IXX, § 1.

Id. at art. II, § 1(a)–(c).

Id. at art. III, § 2(a).

Compare id. at art. III, § 4, with 8 U.S.C. § 1839(5)(B).

Directive, supra, art. III, § 1(a)–(c).

Id. at art. III, § 1(d).

Id. at art. X, § 1(c).

Id. at art. XIV, § 1.

Id. at art. XII, § 1(a)-(b),(d).

Id. at art. XII, § 2.

Froud & Samuels, supra.

Id.; see also Exten-Wright, supra (noting that the Directive will codify much of the UK's existing practice, but will still require the country to update its contractual protections and policies).

See *Dyncorp International LLC v. AAR Airlift Group, Inc.*¸ 2015 WL 5923630, Case No. 6:15-cv-01454-GAP-GJK (M.D. Fla. Oct. 9, 2015). The district court later granted the defendant's motion to dismiss, which was subsequently reversed on appeal to the 11th Circuit Court of Appeals. See DynCorp International v. AAR Airlift Group, Inc., 664 Fed. Appx. 844, 2016 WL 6833333 (11th Cir. Nov. 21, 2016).

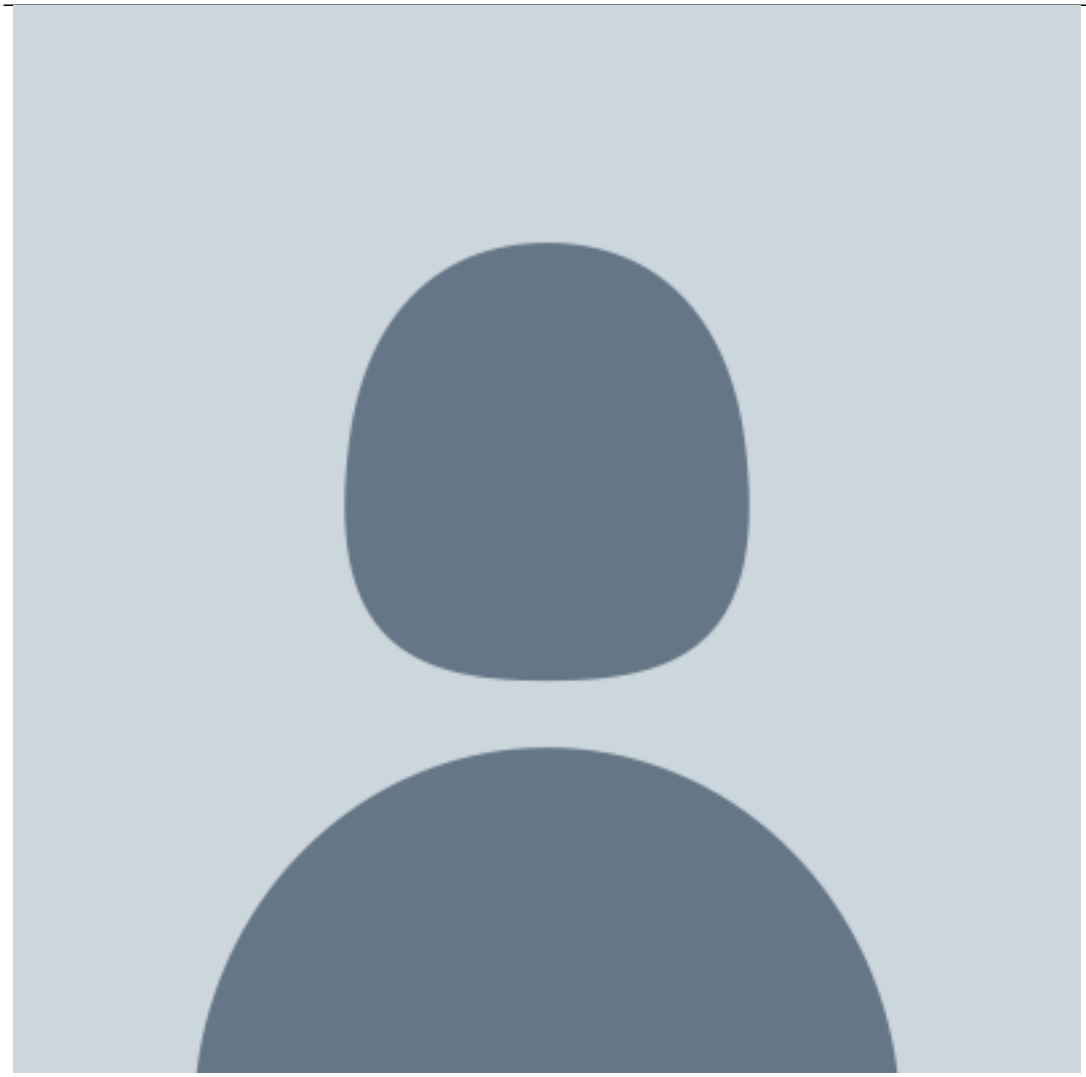
Elizabeth E. Atlee

Senior Legal Manager

CBRE

She manages more than 300 active cases globally and is also responsible for outside counsel management, legal spend containment, and other essential responsibilities as a senior legal manager at CBRE.

Devon C. Beane



IP litigator

the Chicago office of K&L Gates LLP

She has been involved in litigation matters across the country, including district courts, the Federal Circuit, and the International Trade Commission.

Christina N. Goodrich

Litigation Partner

the Los Angeles office of K&L Gates LLP

She has litigated intellectual property and complex commercial disputes in federal district and appellate courts, along with California trial and appellate courts.

Christine Lawton

Christine Lawton provides strategic business advice to retail, entertainment, tech, and consumer brand companies driving revenue by innovating consumer experiences, and held senior executive home entertainment positions at Universal and Fox.