WINSTON & STRAWN LLP

2019 Trade Secrets Year in Review

Top 10 Takeaways in Trade Secrets

2019 was another interesting year in the world of trade secret breaches and theft. Throughout 2019 there was a focus on protecting and prosecuting trade secrets by individuals, governments, and law enforcement agencies worldwide. **Winston & Strawn's Global Privacy & Data Security Task Force** has assembled a top 10 list of notable developments and trends that occurred over the past year relating to trade secret theft, litigation, and protection, as well as our observations and predictions for 2020.

Top 10 Takeaways in Trade Secrets

1 The Department of Justice maintained its focus on Chinese theft of trade secrets

As we reported in our **2018 Year in Review,** the United States Department of Justice (DOJ) created a "China Initiative" in 2018 to prioritize economic espionage and theft of American trade secrets by Chinese actors.

Throughout 2019, several cases showed that the DOJ is pursuing this focus. Highlights include:

- In January 2019, **a grand jury indicted Huawei Technologies**, two of its affiliates, and the company's CFO with theft of trade secrets, fraud, and other crimes. According to the DOJ, the indictment traces a long-running scheme by Huawei "to deceive numerous global financial institutions and the U.S. government regarding [its] business activities in Iran."

- One month later, **the DOJ indicted former Coca-Cola scientist Xiaorong You** of Lansing, Michigan, and alleged co-conspirator Liu Xiangchen of Shadong Providence, China, for conspiring to steal trade secrets concerning BPA-free linings in soda cans.

- In November, a Chinese national and former scientist for Phillips 66, **Honjin Tan, pled guilty to trying to steal trade secret information from his former employer**. The information was related to the development of a product worth more than $1 billion.

We expect to see more cases brought against Chinese companies and Chinese nationals in the coming months and years as the DOJ's initiative proceeds.

2 Theft by company employees continues to be a significant risk area and focus of litigation

Theft by insiders, like employees, continues to be a significant risk point for companies when it comes to protecting their trade secrets. As in 2018, numerous companies across industries filed civil lawsuits against current or former employees who stole the companies' trade secrets, with the Department of Justice also indicting some cases of theft by employees. For example:

- In April, **the parent company of Chicago-based Garrett Popcorn (CarmelCrisp LLC) brought suit against an ex-employee for stealing trade secrets**. The suit claimed that the ex-employee was one of only three people with access to the secret formula and that she stole 5,400 related files from the company. CarmelCrisp asked the court for both preliminary and permanent injunctive relief under the federal Defend Trade Secrets Act (DTSA). *CarmelCrisp LLC v. Aisha Putnam*, No. 19-CV-02699 (N.D. Ill. filed Apr. 22, 2019).

- In June, **a grand jury in Louisiana indicted two scientists for conspiring to steal trade secrets related to The Water Institute of the Gulf**. Allegedly, the scientists conspired to steal a scientific model that projects how the natural environment of the Mississippi Delta would change over time. The U.S. Attorney emphasized that theft of proprietary information will not be tolerated, "especially where the theft is from a research institution whose purpose is to study environmental impacts[.]…"

- Also in June, a **Lexington, Massachusetts, man was indicted for stealing trade secrets from his former employer, Analog Devices, Inc**. The man allegedly downloaded hundreds of highly confidential schematic design files and uploaded them to his own Google drive to benefit his own new business venture.

- In September, **final judgment was entered against a former employee of Atlas Biologicals and his new companies** for stealing Atlas' customer contact lists, a supplier agreement, the quality manual, an organizational chart, and other key business items. The court awarded Atlas a permanent injunction and damages over $2 million. *Atlas Biologicals, Inc. v. Kutrubes*, 2019 WL 4594274, at *23 (D. Colo. Sept. 23, 2019).

As more and more data is stored electronically and employees continue to be highly mobile, switching jobs with frequency, theft by insiders will continue to be a risk point for companies in the coming year—a risk that will only grow if companies do not take proactive measures to protect their trade secrets, starting with conducting an audit of their practices, policies, and protocols.

3 Trade secret cases end in large damages claims, verdicts, and settlements

As in 2018, this year there were again significant damages claims, jury verdicts, and settlement outcomes in theft-of-trade-secrets cases, highlighting the significance of taking precautions before litigation ensues.

- **One judge in California affirmed a jury's $845 million verdict in a theft-of-trade-secrets suit between two competitor companies**. *ASML US Inc. v. XTAL,* No. 16-cv-295051 (Santa Clara Sup. Ct. May 3, 2019). The jury trial found the company XTAL liable for stealing lithography technology from ASML, a semiconductor company. Although XTAL was in bankruptcy, ASML is expected to receive most, if not all, of the $845 million under a bankruptcy settlement agreement.

- **Another jury returned a $91.3 million verdict against beauty giant L'Oreal after, beauty company Olaplex sued, claiming that L'Oreal stole its trade secrets**. Olaplex claimed that L'Oreal entered into an agreement with Olaplex pending a contemplated acquisition, but after the deal went south, stole the proprietary technology at issue. The court reduced the amount to just under $50 million. *Liqwd Inc. v. L'Oreal USA Inc.*, 17-CV-00014 (D. Del.).

- In a case involving trade secrets for designing data rooms, one jury found Emerson Electric liable for $30 million to Bladeroom Group Limited. *Bladeroom Grp. Ltd. v. Emerson Electric Co.*, 2019 WL 1117538 (N.D. Cal. Mar. 11, 2019). In that case, the plaintiff's expert determined the damages to be around $100 million, but the jury returned a verdict of $30 million. The court refused, however, to issue a permanent injunction against Emerson Electric, stating that since the expert could calculate damages, they could be quantified and an injunction would be like double recovery.

In short, in addition to causing uncertainty and creating disruption, trade secret theft can be extremely costly. This highlights the importance for companies to make sure they have practices and protocols in place to prevent new employees from bringing trade secrets from their former employers as the company will end up being the deep pockets named as a defendant in litigation.

4 Courts continue to scrutinize whether trade secret owners have taken sufficient "reasonable measures" to allow a DTSA claim to proceed

As we noted in our **2019 Mid-Year Review**, our **2018 Year in Review**, and **a recent Law360 article**, the requirement of the DTSA that a trade secret owner take "reasonable measures" to protect its information has been the downfall for many plaintiffs. Both the DTSA and the Uniform Trade Secrets Act (UTSA) (adopted in some form by 49 states) require a trade secret owner to take reasonable measures to protect its data. A study Winston conducted of cases filed from 2009 through 2018 showed that courts dismissed claims in 11% of disputed trade secret cases because the plaintiff-company failed to take "reasonable measures" to protect the stolen information, as is required to meet the definition of a "trade secret." In 2019, many courts continued this alarming trend and dismissed theft-of-trade-secrets claims and/or denied injunctive relief because the victim-companies failed to take "reasonable measures" to protect their trade secrets. By way of example:

- In February, **a district court in Alabama allowed a trade secrets case to progress past the motion-to-dismiss stage**, holding that the plaintiff had taken "reasonable measures" to protect the stolen trade secrets, even though the plaintiff company had not marked the document at issue as "confidential." *S. Field Maint. & Fabrication LLC v. Kilough*, No. 2:18-cv-581-GMB (M.D. Ala. Jan. 29, 2019). The court looked at the overall protections that the company took to protect its information to determine whether "reasonable measures" were achieved. The court held, "under all the circumstances, if the employee knows or has reason to know that the owner intends or expects the information to be secret, confidentiality measures are sufficient."

- In *Zoppas Indus. De Mexico, S.A. de C.V. v. Backer EHP Inc.*, a District of Delaware court held that a non-disclosure agreement between parties in conjunction with the plaintiff's continued request "to either return or destroy [the] information" after the relationship between the parties soured was "sufficient to make out a plausible

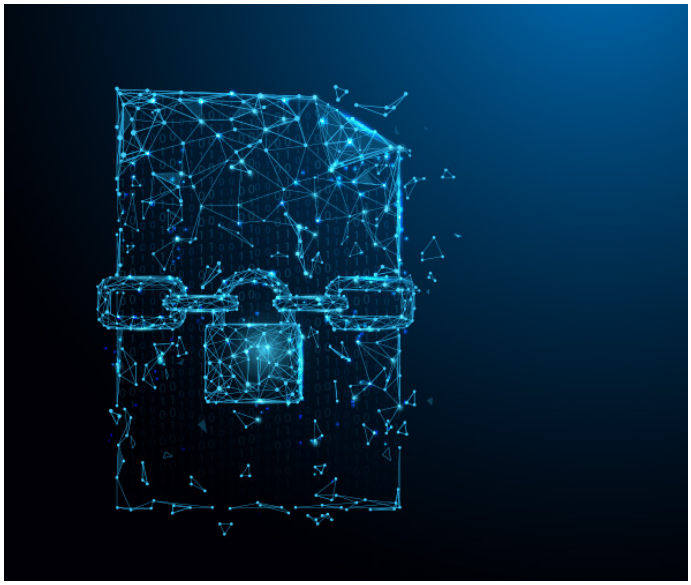
claim that the information" was a legally protectable trade secret under the DTSA. 2019 WL 6615421 at *3 (D. Del. Dec. 5, 2019). The defendant's motion to dismiss was denied in part.

- Also this year, **a Northern District of Illinois court found** that where a victim-company did not require its employees to sign non-disclosure agreements, did not tell the employees that the information was confidential, and did not password protect or encrypt the files (among others things), "reasonable measures" to protect the information had not been achieved. *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F.Supp.3d 888, 898-99 (N.D. Ill. Mar. 4, 2019).

- Similarly, in December 2019, a Pennsylvania District Court held that secret recipes for a sandwich shop were not "trade secrets" under the DTSA because they were posted "in the sandwich preparation room in the store, visible to all employees…and accessible to any vendor who had access to that area." *Revzip, LLC v. McDonnell*, 2019 WL 6701835, at *6 (W.D. Penn. Dec. 9, 2019). The plaintiff's request for a preliminary injunction was denied.

- Finally, in *Mastronardi Int'l Ltd. v. SunSelect Produce (Cal.), Inc.*, an Eastern District of California district court found that whether reasonable measures had been taken was not an issue that could be determined at the motion-to-dismiss stage of the litigation. 2019 WL 3996608, at *9 (E.D. Cal. Aug. 23, 2019). There, the court found that it was a question of fact "whether…SunSelect took reasonable measures to keep [its information] confidential," and cited several cases from 2018 and 2019 to support its position.

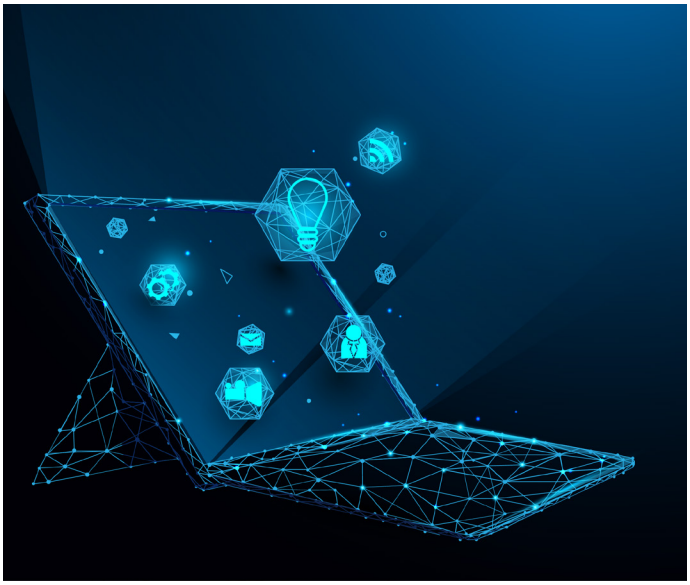
We expect defendants to continue to challenge the measures taken by plaintiffs and for courts to delve further into the nuances of the fact-specific question of what measures are "reasonable." Companies should be aware that whether they can prevail on a theft-of-trade-secrets claim may be determined by actions they take long before the theft ever occurs. Companies must give critical thought to how to ensure their actions will be considered "reasonable" by a court, especially for the company's most valuable trade secrets.



5 Whether to mark documents "confidential" or not has become increasingly important

As we analyzed in an article earlier this year, how a company crafts and deploys a policy regarding marking confidential and trade secret documents as such can significantly impact the company's ability to protect its trade secrets. Courts repeatedly look to whether a document has been marked and what type of policy a company deploys when assessing whether (1) the company took "reasonable measures" to protect the secret and (2) the defendant was on notice that he had an obligation to protect the information at issue. Two recent cases highlight the nuances companies need to consider when utilizing a marking policy. First, in *Call One, Inc. v. Anzine*, 2018 WL 2735089 (N.D. Ill. June 7, 2018), the court granted summary judgment in favor of the defendant because the company-plaintiff had a policy to mark confidential and trade secret documents as such, yet the information purportedly stolen was not marked. However, in the 2019 *Kilough* case (also mentioned above), the company failed to mark the document at issue as confidential, yet still received trade secret protection.

The difference between these cases in a short period of time underscores that there is no one-size-fits-all approach to marking documents as confidential.



6 Courts analyzed how much information a victim-company must divulge to adequately allege misappropriation

One challenging issue in trade secret cases is how much detail a plaintiff must divulge to define and identify the trade secrets at issue. This is an issue that some courts addressed head-on in 2019 and that has received differing treatment by courts in different jurisdictions.

For example, in *Magnestia Refractories, Co. v. Tianjin New Century Refractories, Co.*, 2019 WL 1003623, at *9 (M.D. Pa. Feb. 28, 2019), a court conflated the Pennsylvania Uniform Trade Secrets Act's (PUTSA) standard for sufficient description, to the same requirement in the DTSA. The PUTSA does not require trade secrets to be described "with particularity." This court found that "[i]n the two years since the DTSA's enactment, district courts across the country have applied a similar standard to federal misappropriation claims" and therefore chose to do the same. *Id.* Description with particularity was not required.

Conversely, in November**, a California district court dismissed a case because the plaintiff company's description of its trade secret was too vague.** *Zoom Imaging Sols., Inc. v. Roe,* 2019 WL 5862594, at *5 (E.D. Cal. Nov. 8, 2019). There, the company listed information categories that it considered to be trade secrets. Yet, "because the list…[was] not exhaustive, and because trade secrets [were] an unknown subset" of the information stolen, the court determined that the information was not "sufficiently identified." *Id.*

We expect to see more disagreement and nuance among district courts as they continue interpreting the definitions and parameters of both state and federal trade-secret-theft claims. Companies should be aware of these nuances when considering in what jurisdiction to file a trade secret claim.

7 China revised an unfair competition law to better protect companies' trade secrets

The National People's Congress of China **amended the Anti-Unfair Competition Law (AUCL) in April 2019 to protect the trade secrets of companies doing business in China**. The three main changes were as follows:

- The law now covers misappropriation by more than just "non-business operators." This means employees and former employees can now be found responsible under the AUCL for trade secret misappropriation.
- Punitive damages against trade secret infringement is now allowed (if "malicious intent" is present), and the maximum statutory compensation was raised from 3 million RMB to 5 million RMB where the loss suffered cannot be determined.
- Newly added Article 32 requires that a trade secret owner only provide "preliminary" evidence on the protection measures taken to protect the trade secret and is only required to show to a "reasonable extent" the trade secret is actually infringed. This lessens the burden on the trade secret owner.

We consider these changes to be major improvements to Chinese trade secret law, giving more protection to companies doing business in China. Although Chinese courts have yet to review and interpret the revisions, as written, the changes demonstrate a positive shift.

8 EU member states continued to roll out their implementation of the EU directive

Throughout 2019, **additional European Union (EU) member states implemented the EU's Trade Secrets Directive.** Spain, Germany, Luxembourg, Greece, **and Portugal** all adopted laws implementing the Directive. The laws of Spain, Germany, and Luxembourg each require the trade secret owner to maintain the secret's confidentiality to maintain protection. Notably, similar to the DTSA, none of the laws define what types of measures a company must take to receive protection under the laws, which will require development through future jurisprudence.

9 Breaches by state actors and breaches against corporate executives are on the rise

This year **Verizon published its 2019 Data Breach Investigations Report,** which found (among other things) that year-over-year trends show that data breaches aimed at companies by state actors are rising, while breaches by organized crime groups are falling. **Our team analyzed** the report and determined that these findings may signal that attackers' sophistication and resources are increasing, that the priorities of hackers are shifting, and that political motivation may be a factor when hackers choose where and how to strike.

The Verizon Report also found that security incidents and data breaches "that compromised [individual] executives" of companies and corporations "rose from single digits" last year "to dozens" this year. "C-level executives were twelve times more likely to be the target of social incidents…than in years past." The Verizon Report highlights the importance of data protection training for executives and assuring that there are high-tech security mechanisms on executives' devices.

As explained in detail above, in 2019, the DOJ continued its "China Initiative" priority to target Chinese hackers that attack American businesses. This led to a number of indictments against Chinese nationals and companies, including: **Huawei Technologies** (one of the world's largest communications equipment manufacturers), **a Coca-Cola scientist**, and **a former Phillips 66 scientist.**

10 The United States Supreme Court weighed in on sharing confidential information with the government

During the summer of 2019, **the Supreme Court reversed an Eighth Circuit opinion** and gave more parameters to the Freedom of Information Act (FOIA) Exemption 4, which allows businesses to withhold information from FOIA if it is "confidential business information." *Food Mkt. Inst. v. Argus Leader Media,* 139 S. Ct. 2356 (2019). Specifically, the Court held that a showing of "competitive harm" is *not* required to establish the confidentiality of business information. So long as commercial or financial information is "both customarily and actually treated as private by its owner," and "provided to the government under an assurance of privacy," the Court held that the information can qualify for Exemption 4 and companies and businesses do not have to disclose it. *Id.* at 2366.

This opinion may make it easier for businesses to protect their sensitive information from disclosure to the public. It also signals to business owners that they should "customarily and actually" treat the information as private if they want to take advantage of FOIA Exemption 4.

Key Contacts

Gino Cheng
Partner, Hong Kong and
Los Angeles
+ (852) 2292 2218
gcheng@winston.com

Sheryl Falk
Partner, Houston
+1 (713) 651-2615
sfalk@winston.com

Sara Susnjar
Partner, Paris
+ 33 1 53 64 81 33
ssusnjar@winston.com

Shannon Murphy
Partner, Chicago
+1 (312) 558-5285
stmurphy@winston.com

David P. Enzminger
Partner, Los Angeles and
Silicon Valley
+1 (213) 615-1780
+1 (650) 858-6580
denzminger@winston.com

Steve Grimes
Partner, Hong Kong and Chicago
+852 2292 2138
+1 (312) 558-8317
sgrimes@winston.com

About Winston & Strawn

Winston & Strawn LLP is an international law firm with 1,000 attorneys across 16 offices in Brussels, Charlotte, Chicago, Dallas, Dubai, Hong Kong, Houston, London, Los Angeles, Moscow, New York, Paris, San Francisco, Shanghai, Silicon Valley, and Washington, D.C. The exceptional depth and geographic reach of our resources enable Winston & Strawn to manage virtually every type of business-related legal issue. We serve the needs of enterprises of all types and sizes, in both the private and the public sector. We understand that clients are looking for value beyond just legal talent. With this in mind, we work hard to understand the level of involvement our clients want from us. We take time to learn about our clients' organizations and their business objectives. And, we place significant emphasis on technology and teamwork in an effort to respond quickly and effectively to our clients' needs.

Visit **winston.com** if you would like more information about our legal services, our experience, or the industries we serve.