Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Trade Secrets 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

USA: Trends & Developments

Steven Blonder
Much Shelist, P.C.

Trends and Developments

Contributed by:
Steven Blonder
Much Shelist, P.C.

Much Shelist, P.C. is a firm of approximately 100 attorneys who focus on business counselling, transactional law and litigation for businesses of all sizes. The firm has offices in Chicago, Illinois and Newport Beach, California. Clients include financial institutions, private equity groups, public and private companies with a global presence, middle-market businesses, families and high net worth individuals. Its attorneys help clients identify and correct potential gaps in their trade secrets protection strategies. This includes audits of existing trade secrets and intellectual property as well as non-compete, non-disclosure and confidentiality agreements. Much Shelist also reviews licensing agreements, database and other electronic information protection systems, and other policies and employee training practices. Following this analysis, the firm recommends strategies designed to shore up weak or non-existent firewalls and to negotiate more effective agreements with business partners and allies.

Author

Steven Blonder is a member of Much's Management Committee. A valued legal and business counsellor who focuses on complex business litigation, Steve has argued successfully before the federal and state appellate courts as well as the Illinois Supreme Court. He possesses a record of consistent success in motion and trial practice (both jury and non-jury) in state and federal courts and in arbitration. His clients range from Fortune 500 companies and government entities to small businesses and entrepreneurs in a variety of industries, including gaming, food and beverage, financial services and real estate.

Much Shelist, P.C.

191 North Wacker Drive
Suite 1800
Chicago
Illinois
USA
60606

Tel: +1 312 521 2000
Fax: +1 312 521 2100
Email: info@muchlaw.com
Web: www.muchlaw.com

Trade Secret Litigation Continues to Rise

The odds today are substantially increased that a company will unwittingly find another company's trade secret on its computer system or experience an unplanned disclosure of its own trade secret. This stems from a variety of reasons, ranging from employee mobility being on the rise, reductions in force, workplaces that are remote or hybrid and workers increasingly bringing their own devices to the workplace. The number of lawsuits filed alleging the misappropriation of trade secrets has been continually increasing over the past several years, and 2023 is so far no exception to this trend.

However, any discussion of trends relating to trade secret claims needs to start with the legislatures in various states passing laws restricting, if not banning, non-compete agreements, with the federal government poised to follow suit. As a result, a company's only avenue for protection may be to enforce its rights in its trade secrets more aggressively than in the past. In recent years, litigation involving trade secrets has increased in sophistication, and clients have become more aware of the legal protections available under state and federal law.

Additionally, as competition has intensified in many industries, companies are often turning to trade secret protection for their core economic business drivers instead of seeking protection under the patent laws. Financial drivers such as customer lists, algorithms and other proprietary technology or business methods enjoy better protection as a trade secret, which essentially enables companies to continue to derive economic value from their protected secrets in perpetuity. As workforces with access to confidential and proprietary information remain increasingly remote, and workers display an increased willingness to speak out about business practices they do not agree with, the necessity for businesses to protect their confidential information is magnified.

Trade secrets are often core to a business' economic viability, if not its success, and rank among a company's most valuable assets; put another way, they are often a company's "crown jewels". Well-known examples include the formula for Coca-Cola, Google's search algorithm, and the secret sauce recipe of McDonald's. None of these examples enjoy patent, copyright or trademark protection – rather, each is a protected trade secret. A trade secret enjoys significant advantages over the other forms of IP protections in that disclosure is not required and the "secret" can be protected for an unlimited period. While many of the big IP litigation battles historically involved patent challenges, that is no longer the case. Many well-known companies are or have been involved in costly trade secret litigation in recent years.

Claims alleging a misappropriation of trade secrets have continued their rapid rise in the past few years. In federal court alone, there were over 700 trade secret claims filed in 2022, with the largest numbers being filed in federal courts sitting in New York and California. By comparison, in 2016 there were 476 such claims filed. During the first few months of 2023, litigants had filed nearly 140 federal trade secret complaints.

This litigation in the trade secret space cut across a wide swathe of industries ranging from cannabis to fashion and retail, e-commerce and consumer products. Historically, trade secret claims had been brought in state courts, but since the 2016 passage of the federal Defend Trade Secrets Act (DTSA) which created a federal cause of action for trade secret theft, claims are now routinely brought in the federal courts.

On the recovery side, successful plaintiffs in trade secret cases have continued to see courts make substantial damages awards. While most claims are resolved prior to trial, federal court trade secret claims over the past five years have resulted in large jury verdicts. During the past year, one Virginia court entered judgment in excess of USD2 billion in a trade secret misappropriation case. If nothing else, the past few years serve as a stark reminder that the damages that are being awarded for trade secret claims remain staggering.

So what trends are likely to define trade secret litigation in 2023? What follows are a few takeaways.

Non-compete policy will impact trade secret claims

In January 2023, the Federal Trade Commission proposed a ban on most employee non-compete agreements. Existing non-competes would need to be rescinded under the proposed rule and future agreements would be prohibited. The growing trend among states (ie, Massachusetts and Illinois that recently enacted new laws and states like New Jersey in which legislation is under consideration) is likewise to limit non-compete agreements. As a result, trade secret protection will be increasingly important in the future.

New technologies and increasing employee mobility present new challenges to trade secret protection

Since early 2020, many businesses have transitioned to working environments that involve remote working or hybrid models combining in-office and remote opportunities. Videoconferencing technologies (such as Zoom and Microsoft Teams) have emerged as the new primary vehicle for communications, both internally at companies and in their external relations with third parties, and employees are changing jobs with increasing frequency. The "great resignation" that began in 2021 creates more opportunities for departing employees to retain or misuse confidential information that they had access to with their prior employer. These shifts have significant implications for how companies protect their trade secret information.

Beware of the statute of limitation and when it begins to run

The federal statute provides for a three-year statute of limitation for a trade secret claim. While certain states allow four or even five years within which a claim must be brought, most states enforce a three-year statute of limitation. Regardless of the length of time to assert a claim, the most critical issue relates to when the statute of limitation begins to run.

If a company believes that its trade secrets have been misappropriated, it potentially forfeits its trade secret protection unless it acts to protect its trade secrets. The law says that a claim arises when the injured party has actual notice of the potential misappropriation of its trade secret, or when that party should have discovered the misappropriation through the exercise of reasonable diligence. In other words, when would a reasonable person investigate whether their trade secrets had been stolen?

At least one court has held that the statute of limitation may begin to run when a company warns a former employee that the disclosing of its trade secrets to a new employer would constitute a crime. Other courts have noted that, in the context of a failed business transaction, an enquiry notice exists when one party fails to return the other's confidential information according to the terms of a non-disclosure agreement that the

parties signed. The question of when a statute of limitation begins to run is likely to continue to be a major source of dispute in 2023.

The question as to when the trade secret theft occurred is important for other reasons as well. For example, one change brought by the 2016 federal legislation was that trade secret misappropriation can constitute a predicate act under the RICO statute. To qualify, a plaintiff must show that the trade secret theft occurred after 11 May 2016 – the date that the DTSA was enacted.

The kinds of trade secret continue to expand

The definition of a trade secret can be quite broad. Simply put, a trade secret is defined as information used in a company's business that is not known or readily accessible by competitors, that is protected from disclosure through reasonable efforts to maintain its secrecy, and that provides either a competitive advantage in the marketplace or has commercial value.

Many trade secret claims revolve around computer codes, algorithms and customer lists. However, recent cases span the gamut from OSHA data summarising warehouse worker illnesses and injuries, the manufacture of Botox, advertising plans for exercise equipment, proprietary information about cannabis platforms supporting a telehealth service, methods for bleaching hair and repairing hair damage, and the process of adding aromas as a perceived taste-enhancer to beverage bottles. The bottom line is that any type of information that meets the broad criteria of a trade secret can be protected.

Where exactly did the theft occur?

DTSA was enacted as a part of the response to the theft of trade secrets by Chinese companies and other foreign actors. Moreover, in the USA, courts have recently held that a civil action under DTSA can arise from wrongful conduct occurring completely outside the USA. The only catch is that the wrongful activities have some nexus with activities that took place within the country.

Who took the trade secret?

In January 2023, President Biden signed the Protecting American Intellectual Property Act. This statute provides for the imposition of sanctions on foreign companies and individuals involved in the theft of significant trade secrets from United States companies and individuals. What is significant is not defined in the statute. This statute provides for sanctions against not only those who steal trade secrets, but also against others including board members and executives of a foreign company that stole the trade secrets regardless of the knowledge of the theft by those individuals. The only catch is that the statute only allows sanctions against foreign persons.

The sanctions that may be imposed can prove crippling. They range from limiting loans from US financial institutions to blocking all transactions in property and excluding corporate officers from the United States.

Steps taken to maintain information as confidential can have implications for trade secret litigation years down the road

The DTSA and various state statutes require that a trade secret owner take "reasonable measures" to protect its trade secret information. What constitutes "reasonable measures" is not defined, and the actions that a company takes to protect its trade secret information up front can impact the likelihood of a successful trade secret claim years later.

Coca-Cola is widely known for the efforts it undertakes to maintain secrecy of the formu-

la for its popular soft drink, but this is not the benchmark for what is required.

Numerous courts have dismissed trade secret claims based on the failure of the plaintiff to enact "reasonable measures" to protect its trade secrets. In some of these cases, the party seeking trade secret protection had not adequately marked the information as "confidential". Other indicia of reasonable measures may include storing the information in a password-protected, limited-access server, having employees sign written acknowledgements of their obligation to keep sensitive business information confidential, and telling employees that the information was confidential.

In today's world where companies use cloud applications allowing employees to work more flexibly, the issue becomes more difficult. The ease with which data can be transferred in a cloud-centric world significantly changes a company's ability to maintain the secrecy of its information. For example, when an employee downloads information from the cloud to a personal device outside of the company's control, the company may lose track of its data and not be able to maintain the secrecy or confidentiality that it thought that it had.

A party seeking to enforce a trade secret bears the burden of properly identifying and disclosing the trade secrets being protected at the outset of the litigation. Indeed, federal courts clarified the need for specific disclosures to be made at the outset of litigation and before extensive discovery takes place so as to preclude parties from "retroactive stamping" of trade secrets. Likewise, parties cannot use industry practices to identify their trade secrets.

Whether or not a company has undertaken "reasonable measures" to protect its confidential information is necessarily a fact-based enquiry; in all likelihood, this will continue to be a hot issue in trade secret litigation in 2023.

Trade secret claims may involve large actual and punitive damages

In addition to increases in the number of cases being filed, the recoveries in trade secret claims for successful plaintiffs continue to be significant, even eye-popping. This is often true whether the recovery results from settlement or comes in the form of a verdict after a full-blown trial. Reported decisions in state and federal courts evidence damage awards in the eight and nine-figure range, and now extending into ten figures. Sometimes these include punitive damages, while at other times they do not. Most remarkable is that often the damage awards entered reflect the asserted unjust enrichment of the defendants which significantly outpaces the actual losses suffered by the plaintiffs.

Litigants in trade secret cases have flexibility in fashioning their damage theories. This is exemplified by a recent appellate court decision affirming an arbitration award containing "head start" damages. These damages represented the benefit to the defendant for the research and development and operational head start that it received through the misuse of the information. The "head start" damages were a means to quantify the benefit of the increase in value in the defendant's business resulting from its being several years ahead of where it would have been without the wrongful conduct. These damages were distinct from the saved development costs which provided an additional benefit to the defendant. The policy underlying these damage awards is to prevent a company from keeping ill-gotten gains. Remarkably, under this

"unjust enrichment" approach, any actual loss to a plaintiff becomes irrelevant.

Regardless of the theory of damages, the bottom line is that – assuming a litigant can prove misappropriation occurred – recoveries for plaintiffs in trade secret cases continue to be large, with juries showing little mercy. For companies, taking precautions to ensure that new employees do not bring with them trade secrets owned by their former employer can prevent costly litigation down the road.

Other trends to watch out for

A common defence raised in trade secret cases is "unclean hands". In asserting this defence, a defendant seeks to shift the enquiry away from the alleged misappropriation toward the complaining party's conduct in order to invalidate a claim. For example, employees often access their social media accounts from work computers or other devices. Employers routinely monitor such access but, depending on how employers monitor this information and what they do with it, the facts can give rise to an unclean hands affirmative defence. As always, in investigating potential trade secret misappropriation, a company needs to consider the implications of its actions on its potential lawsuit.

Another issue is the interplay between patents and trade secrets. At least one case held that a plaintiff lacked standing to pursue trade secret claims because the alleged trade secrets were "extinguished" by the publication of patent applications involving the same technology. Other cases address the question of whether ownership or inventorship of a patent impact on ownership of a trade secret.

Trade secrets remain essential to the competitive success and financial viability of many businesses. Claims alleging trade secret misappropriation are likely to continue to rise. Companies would be well advised to examine their policies and procedures regarding their confidential information and the protections in place to maintain that information in confidence. Looking at these issues on the front end can lead to increased success on the back end if a claim needs to be pursued.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com