

Canadian Trade Secrets: Year in Review 2025

Mark Davis, Claire Stempien

February 6, 2026

In Canada, trade secrets and confidential business information are protected through contract and common law fiduciary obligations. Trade secrets can include:

- formulas and processes (e.g., manufacturing methods);
- business strategies and plans;
- customer lists and pricing models; and
- technical know-how or proprietary algorithms.

Unlike patents, trade secrets are protectable as long as they are kept secret and reasonable measures are taken to maintain confidentiality. Though no single, comprehensive definition of a trade secret exists in Canadian law, it is generally understood that a trade secret must satisfy the following four criteria:

1. it must be secret in an absolute or relative sense (known only to one or a small number of people);
2. the owner must show an intention to treat the information as secret;
3. the information must be capable of industrial or commercial application; and
4. the owner must have an interest worthy of legal protection, typically an economic interest.¹

Significant trade secret litigation in 2025 involved a myriad of subject matters, including algorithms, software, data processing, strategy, pricing and sales information, medical devices, and biotechnology processes. The commercial value of this information compelled the owners to litigate to keep the information secret, or to obtain compensation from wrongdoers when that secrecy had been breached.

The Value of Trade Secrets

Trade secrets can be extremely valuable and trade secret protection is often overlooked. Trade secret law offers broad protection: information may be protected as a trade secret even though it is not patentable.

Recent Canadian cases highlight the significant awards for misuse of trade secrets, including “springboard damages,” which compensate a plaintiff for the head start the defendant gained by misusing confidential information. There were also several notable trade secret cases in the United States last year, showing that misappropriation of trade secrets or confidential information can result in millions of dollars worth of damages. For example, in *Zest Labs Inc v. Walmart Inc*, U.S. District Court for the Eastern District of Arkansas, No. 4:18-cv-00500, a jury in Arkansas awarded technology startup Zest Labs more than \$222

Cassels

million based on allegations that Walmart misappropriated its trade secrets for computer algorithms assessing food preservation and reducing food waste. Further, in *Propel Fuels Inc. v. Phillips 66 Co.*, No. 22CV007179, a California jury awarded Propel Fuels \$604.9 million after finding Phillips misappropriated trade secrets during a failed acquisition. Describing Phillips' conduct as "reprehensible," the Court awarded \$195 million in exemplary damages, calculated by trebling the original \$65 million acquisition price. The total judgment exceeded \$799 million.

These examples show the substantial value of trade secrets and demonstrate that courts regard their misappropriation as a serious commercial wrong. Trade secrets can be multi-million dollar drivers of innovation and corporate strategy.

How to Protect and Enforce Trade Secrets in Canada

Unlike other types of intellectual property, there is no formal registration process for trade secrets. Trade secret protection depends on an owner's ability to maintain secrecy. Once a trade secret is publicly disclosed, the protection is lost.² Therefore, reasonable steps must be taken to protect trade secrets, including the use of confidentiality agreements and security measures to limit access to the trade secrets.

There is no Canadian statute for enforcing trade secrets.³ While there are calls for the Canadian government to provide legislative protection for trade secrets, until this occurs, trade secret protection continues to rely heavily on contract law and common law judicial precedent.

In Canada, the Federal Court has jurisdiction over disputes involving trademarks, copyrights, patents and industrial design, and other forms of intellectual property that are codified by statute, while provincial superior courts have concurrent jurisdiction over enforcement of intellectual property rights and exclusive jurisdiction over cases involving property and civil rights, including trade secrets.

Enforcement of trade secrets is based on common law. Misuse of information communicated in confidence may be enforced through actions for breach of contract, breach of fiduciary duty, and breach of confidence.

To succeed in a breach of confidence action, the plaintiff must prove that:

- the information is confidential;
- that confidential information was conveyed in confidence (or obtained through a breach of confidence); and
- the information was misused by the defendant to the detriment of the plaintiff.⁴

Given the urgency often involved, the potentially serious consequences of misuse, and the difficulty in ascertaining monetary damages in a typical trade secret matter, preliminary injunctions are also a tool that

may be available to prevent the use (and misuse) of trade secrets.

Canadian Cases From 2025

There were several interesting Canadian decisions in 2025 that provide guidance on how a business can protect its trade secrets. The cases also continue to emphasize that courts are reluctant to enforce non-competition covenants.

Prairie Risk Management Inc v Marsh Canada Ltd, [2025 MBCA 6](#) involved an appeal from a damages award of \$1,534,000 against Prairie Risk Management for breach of contract, breach of confidence and breach of fiduciary duty. The Appeal Court found that the defendant misused the plaintiff's confidential information but that the damages award was well in excess of the loss that flowed from the defendant's wrongful conduct. In this case, the plaintiff provided insurance consulting services to a buying group of hog farmers and producers (the "Insured Members"). The list of Insured Members and the details regarding their operations was found to be confidential information. Following termination of the relationship, the defendant almost immediately began contacting the Insured Members directly to retain their insurance business. In reviewing the trial judge's decision on damages, the appeal court found that the advantage that the defendant gained from misusing the confidential information was a springboard that gave it a head start in contacting the Insured Members and gathering the information necessary to place insurance on their behalf. However, there was also evidence that the defendant could have contacted the Insured Members without using the confidential information based on pre-existing relationships. Accordingly, the appeal court reduced the damages award. Overall, the case provides a reminder that while "springboard" damages are often available in trade secret cases, the amount awarded will depend upon the facts, including whether the defendant could have achieved the same result without misusing the confidential information.

In *Total Meter Services Inc. v. GVM Integration*, [2025 ONCA 321](#), a former employee who worked as a software developer and manager copied proprietary software and used confidential information to compete directly with his previous employer. The trial judge found that the former employee was liable for breach of fiduciary duty and breach of confidence and awarded \$750,000 in damages, based on disgorgement of profits. The former employee appealed on two grounds: that the trial judge wrongly drew an adverse inference against him, and that some claims were added too late and were barred by the limitation period. The adverse inference arose because the worker failed to produce complete software documentation during discovery. Although the employer's original software was written in Visual Basic, the worker produced source code almost entirely in C#, which the trial judge found undermined his credibility and supported findings of misconduct. Separately, the employer amended its claim in 2020 (6 years after the claim was commenced) to add new allegations about a 2012 customer opportunity (the "TCS Opportunities claim"), asserting the former employee had secretly pursued work for himself while still employed. The Appeal Court upheld the adverse inference but found that the TCS Opportunities claim was a new cause of action added outside of the limitation period. As a result, the appeal was allowed in part, and the damages were reduced

to remove the portion tied to the time-barred claims. This case serves as a reminder of the significant damages that can be awarded in breach of confidence cases and the importance of ensuring all claims are included before the expiry of any limitation period.

In *Epiroc Rock Drills AB v Zimmerman*, [2025 BCSC 1757](#), the plaintiffs sought broad injunctive relief against three former employees and several companies, alleging breaches of non-competition, non-solicitation, and confidentiality obligations. The British Columbia Supreme Court held that the plaintiff failed to precisely define the confidential information that it claimed was at risk. Although the plaintiff offered an extremely broad definition of “confidential information,” it did not identify any specific information allegedly taken, explain why it met the legal test for confidentiality, or show how it had been misused. At most, the defendants had accessed certain documents, but the plaintiff did not prove those documents were confidential. The Court also found no strong prima facie case that the non-competition clause survived the employment agreement, and the plaintiff failed to demonstrate irreparable harm. The decision underscores a recurring issue in Canadian trade-secret litigation: because trade secrets are not protected by statute, plaintiffs must clearly define the specific confidential information at issue and show it was treated as secret. Many claims fail when plaintiffs rely on vague or overly broad assertions of confidentiality.

Another decision, out of Alberta, is *Occidental Petroleum Corporation v Boguslawski*, [2025 ABKB 578](#). In this case, the applicants sought an interim injunction to enforce a non-competition covenant contained in an employment agreement between one of the applicants (CE) and the respondent. The respondent was formerly employed by CE as a project engineer. The Court emphasized that restrictive covenants are enforceable only if they protect a legitimate proprietary interest, which has been held to include “trade secrets, confidential information, and trade connections of the employer.” It found that CE’s confidential information and trade secrets constituted such an interest, however, the Court also held that CE’s position that this case warrants the extraordinary relief of enforcing a non-competition covenant was not tenable. As a result, the application was dismissed. The Court reached this decision in part because it found that the respondent was neither a fiduciary or key employee (he did not even have any client interactions), nor was he a senior manager or director. The Court stated that as such there was a well-recognized power imbalance between the employee and employer, which required the Court to engage in a more rigorous scrutiny of the non-competition covenant. The Court also found the non-competition clause to be ambiguous and overly broad. The decision serves as a reminder that confidential information and trade secrets should be restricted only to key employees on a need-to-know basis, since it has been held that less scrutiny should be applied to a non-competition clause concerning a key employee.

Chatters Limited Partnership v Chatters Deerfoot Meadows Limited, [2025 ABKB 536](#) provided guidance for franchisors in protecting their trade secrets. The franchisor/plaintiff (Chatters) sought to stop its former franchisee/defendant from operating a new, competing salon. The franchise agreement contained a non-competition clause for a two-year period and 10-mile geographic scope from the location of the franchisor salon. The Court dismissed the plaintiff’s application for an interlocutory injunction finding, among other things, that in the franchising context, it is dangerous to assume that the courts will accept that a franchise

system (such as confidential information relating to sales and promotional and marketing techniques) contains trade secrets that are worthy of protection through restrictive covenants without robust supporting evidence. The Court found that, overall, there was insufficient evidence that the defendants were using trade or business connections from the plaintiff or that the defendants were using, or would damage, any goodwill in the plaintiff's name or brand. The Court found the non-competition clause to be unenforceable as it was not sufficiently limited in scope, duration or geography. The Court found that since the average distance between the franchisor's own salons is approximately three miles, the 10-mile restriction was not reasonable. This case serves as an important reminder to franchisors that robust agreements should be entered into prior to sharing trade secrets with any potential franchisee. It also reinforces the principle that non-competition clauses should be drafted to be reasonable if they are to be upheld.

Amendments to the Ontario Employment Standards Act 2021

Historically, restrictive covenants in employment contracts such as non-solicitation covenants and non-competition covenants were used to protect trade secrets. Courts have been historically hesitant to enforce these covenants, especially non-competition covenants and, as shown in recent decisions, courts generally continue to find these clauses unenforceable in the employment context.

Ontario was the first province in Canada to legislate restrictions on non-compete agreements in the employment context. The *Working for Workers Act 2021* prohibits employers from including non-compete clauses in employment contracts or other agreements with employees. In Ontario, non-competition covenants were generally unenforceable and are now clearly prohibited, with minor exceptions expressly provided for in the new legislation.

Whether other Canadian jurisdictions will follow Ontario's lead will remain to be seen, but businesses should hesitate before relying on non-competition clauses in employment contracts to protect their valuable trade secrets. Businesses in Ontario must now rely on other mechanisms that are more targeted and enforceable to protect their trade secrets. We discuss some of these mechanisms in the section below.

Recommendations for Protecting Trade Secrets

To obtain trade secret protection, it is imperative that the information remain secret. Businesses should create a robust strategy to protect their trade secrets, by, for example adopting the following measures:

- **Identify and document trade secrets:** Businesses should conduct an audit to identify information that should be protected as a trade secret. This audit should aim to identify all forms of protectable intellectual property so that a strategy can be implemented for protecting those rights.
- **Create, maintain, and update internal trade secret policies:** Detailed internal policies should be

created, regularly reviewed, and updated with respect to trade secrets, including for example:

- Information-handling procedures such as restrictions and/or guidance on accessing, printing, copying and storing confidential documents;
 - employee training and awareness, including mandatory onboarding training on confidentiality obligations with regular refresher sessions and signed acknowledgments; and
 - incident response plans, including steps for responding to an unauthorized disclosure of trade secrets and assigning responsibility to a specific internal team.
- **Use of strong agreements:** Non-disclosure or confidentiality agreements should be signed by all employees, independent contractors, and business partners who are given access to trade secrets before any disclosure. It is important to seek legal advice to ensure these agreements are adequately drafted. At a minimum, the agreements should include a clear definition of the confidential information, clear boundaries on appropriate use of such information, return/destruction obligations, and these obligations should continue after termination.
 - **Restrict access:** Courts in Canada will look for evidence that the information was indeed confidential, including factors such as the extent to which the information was shared.^[5] As such it is advisable to ensure that trade secrets are shared only with individuals on a *need-to-know* basis, restricting access to those that rise to the level of key employees or fiduciaries if practicable. For employees that need not and should not gain access to trade secrets of the business, both physical and electronic measures should be implemented and monitored to ensure access is limited (for example multi-factor authentication, keycard access, and visitor logs). It is also crucial to ensure that exiting employees have access disabled immediately upon departure, return all devices and documents, and are reminded of their ongoing obligations at exit interviews.
 - **Limit external disclosure:** Avoid disclosing trade secrets in marketing, pitches, or investor materials. If such information must be shared externally, then businesses should ensure robust agreements are entered into with all individuals that the information will be shared with prior to disclosure. Share only what is necessary and restrict access to the information as much as possible.
 - **Maintain documents:** If there is a misuse of confidential information and enforcement measures are taken, Canadian courts will require evidence as to how the information was treated. It is important to have documentary support for training sessions, signed non-disclosure agreements, access logs, security audits, internal policies and updates, incident reports, and related correspondence. An individual or team within the business should be responsible for ensuring these documents are maintained.

Recommendations to Businesses on How to Protect Themselves Against Allegations of Misappropriation of Confidential Information

In addition to protecting their own trade secrets, businesses need to protect themselves from accusations that they have assisted in, or benefited from, a misappropriation of someone else's confidential information.

Cassels

Allegations can arise during hiring, partnerships, joint ventures or even routine customer interactions. Businesses can dramatically reduce their risk of having to defend against such allegations with the right governance, documentation, and training.

Businesses should implement policies to show they take confidentiality seriously and have systems in place to prevent misuse. At a minimum, such policies should prohibit employees from bringing or using confidential competitor documents that they obtained in confidence, customer lists, source code, and pricing information and require employees to disclose any potential conflicts. Many misappropriation claims arise when employees move between competitors. As such, asking new hires to confirm in writing that they will not use or bring any confidential information from prior employers will help reduce the risk that new employees are bringing trade secrets of their former employer with them.

One of the best defenses in a trade secret case is proving that your product or process was developed independently. It is therefore crucial to document research and development work.

Trade Secrets and Artificial Intelligence

The rapid adoption of artificial intelligence (AI) presents challenges for trade secret protection. AI tools are transforming how information is created, shared, and stored—and with that transformation comes a new set of risks and obligations that businesses must manage.

Risks arise through the increasing use of generative AI by employees. When employees share confidential information with AI systems, they can lose control over the information and destroy its confidentiality. The information may be stored on public and foreign servers, used to train future AI models, and potentially be accessible to or shared with third parties. As noted, the key to maintaining a trade secret is to keep it secret. AI creates a trade secret leakage risk, which in addition to the risk of misappropriation, may pose issues to enforceability. Canadian courts may refuse to provide remedies where a business cannot show that it took reasonable steps to protect the secrecy of its information. It is important for businesses to adopt specific AI-policies prohibiting employees from entering confidential information into public AI tools.

AI may also require additional disclosure mechanisms that are directly in contrast to maintaining the secrecy of trade secrets. For example, Canada's proposed *Artificial Intelligence and Data Act* (AIDA) was introduced in 2022 as Canada's first federal attempt to regulate "high-impact" AI systems, including requirements for transparency and the publication of certain information related to AI systems. Unfortunately, the legislative process for AIDA ended in early 2025, so there is still no AI-specific regulatory framework in force in Canada. Nevertheless, it seems inevitable that legislation regulating AI will be passed in the future and that it will likely impose obligations on AI developers and deployers to reveal information about how their AI systems work creating tension between regulatory transparency and trade secret protection.

Cassels

Despite these risks, AI may also be beneficial, for example in detecting misuse of trade secrets. Companies can use AI to help detect suspicious employee behaviours, including downloads or data transfer and track competitor filings or public disclosures for signs of misuse. If employed properly, AI can provide businesses with additional mechanisms to protect their internal confidential information and to avoid inadvertently misappropriating the confidential information of others.

Overall, AI brings additional considerations for businesses in protecting and enforcing their trade secrets. To stay protected, businesses should take additional measures to modernize their confidentiality policies, adopt AI-specific governance and train employees on the safe use of AI. The companies that adapt early will be far better positioned to protect their intellectual assets in an AI-driven economy.

The [Cassels Intellectual Property](#) team is a leader in all aspects of trade secret protection, management, and enforcement. We understand the strategic value that confidential business information holds, and we are highly experienced in helping organizations safeguard their most sensitive assets. We would be pleased to speak with you if you need guidance on protecting your trade secrets or addressing a potential breach.

To receive timely and insightful updates on developments in Canadian IP law, including trade secrets, trademarks, patents and copyright, we invite you to subscribe to our Intellectual Property publications by following this [link](#). If you have any questions about the contents of this article, please reach out to the authors of this article or any member of the [Cassels Intellectual Property](#) team.

Special thanks to [Summer Tan](#) and [Sky Shin](#), articling students at Cassels, who helped prepare this article.

¹ *Merck Frosst Canada Ltd v Canada (Health)*, 2012 SCC 3 at para 109 citing Phelan J. in *AstraZeneca Canada Inc. v. Canada (Minister of Health)*, 2005 FC 189, who referred with approval to Health Canada's *Access to Information Act — Third Party Information — Operational Guidelines*, which sets out the four criteria to be met by a trade secret (para 64). The Supreme Court held this definition appropriately captures the traditional legal meaning and is consistent with the common law definition of "trade secrets."

² Even if all the components of a trade secret are public, this does not preclude the protection for a combination of the individual elements, as a trade secret.

³ Except for the provision in the Criminal Code for violating or unlawfully communicating a trade secrets.

⁴ *Lac Minerals Ltd. v. International Corona Resources Ltd.*, 1989 CarswellOnt 126 (S.C.C.), at para 10.

⁵ *Pharand Ski Corp. v. Alberta*, 1991 CarswellAlta 85 (Alta. Q.B.), at para 144.