The Protection of Trade Secrets In Canada

Adam Kardash and Rowan Weaver
Heenan Blaikie LLP
Royal Bank Plaza, South Tower
Suite 2600
Toronto, Ontario
M5J 2J4
akardash@heenan.ca

September 11, 2008
American Bar Association
Labor and Employment Law CLE Conference
Denver, Colorado
A. Introduction

This paper provides an overview of Canadian trade secret law. The paper begins with a brief overview of definitional issues with regards to trade secrets in Canada. The paper proceeds with a discussion of the basis for the legal protection of trade secrets, an overview of the sui generis nature of an action for breach of confidence, before examining the protection of trade secrets in the specific context of the employment relationships. We conclude with a brief overview of the remedies available for disclosure of trade secrets as well as practical approaches for organizations to proactively protect their trade secrets information.

B. Trade Secrets

1. Definitional Issues

While numerous Canadian cases have considered the principle of trade secrets, the case law has yet to establish a universally accepted definition of the term. Generally, Canadian trade secret law has developed from the English concept that trade secrets are grounded in the confidential nature of the information in question. When any information is imparted in circumstances of confidentiality, a common law duty may arise to keep such information confidential.

An oft-cited Canadian definition was postulated by the Canadian academic David Vaver.2

“If B acquires information that it agrees, knows, or ought reasonably to know is A’s confidential information, B owes A a duty (redressable by all remedies available for the commission of a common law or equitable wrong) not to use or disclose the information, for at least as long as the information is not generally known, for a purpose other than the one for which A allowed it to be used or disclosed, unless public policy justifies B’s acts or equitable reasons bar A from claiming against B.”

In this vein, an exceptionally broad spectrum of information may potentially fall within the parameters of a trade secret. At minimum, a trade secret consists of “some product of the

---

1 Canadian authorities, in the tradition of the English courts, more often use terminology such as “confidential business information” or “commercial confidences” as opposed to the term “trade secret”. See Julie A. Thorburn & Keith G. Fairbairn, Law of Confidential Business Information (Canada Law Book Inc.: Aurora, ON, Release 9, May 2007) at 3-12 [hereinafter “Fairbairn & Thorburn”]. Furthermore, while some authorities have suggested that a “trade secret” is a particular type or subset of “confidential business information”, others use the terms synonymously. See R. v. Stewart (1988), 50 D.L.R. (4th) 1 (S.C.C.) at para 23 [hereinafter “Stewart”].


3 See also Faccenda Chicken Ltd. V. Fowler, [1986] 1 All E.R. 617 (C.A.) at 627 [hereinafter “Faccenda Chicken”] of Appeal states:

It is clearly impossible to provide a list of matters which will qualify as trade secrets or their equivalent. Secret processes of manufacture provide obvious examples, but innumerable other
human brain which suffices to confer a confidential nature upon the information,” and something for which the creator “has used his brain and thus produced a result which can only be produced by somebody who goes through the same process.” The information is typically “the product of labour, skill and expenditure, and its unauthorized use would undermine productive efforts which ought to be encouraged.” It is not even necessary that an idea be complete and fully formed to constitute a trade secret. The “germ of an idea”, under the right circumstances, may gain protection.

Trade secrets fill the vast grey area of information between that which is typically covered under other recognized areas of intellectual property law and that which is neither “useless information nor trivial.” As noted above, the determining factor is the circumstances of confidence under which the information was imparted. The closer the relationship between the parties and the greater the expectation of confidentiality, the less important the secret need be. Alternatively, the more tightly guarded the secret, the more likely a Canadian court will find that the circumstances of disclosure implied a duty of confidence.

2. Basis for Legal Protection

In trade secret cases, Canadian courts have relied on a mixture of proprietary, contractual, and equitable principles to grant protection to confidential information. One of the leading decisions is the Supreme Court of Canada’s ruling in R. v. Stewart. In this case, the defendant obtained confidential employee information from a hotel company to use in an attempt to unionize, and was charged with counselling to commit theft contrary to the Criminal Code (Canada). The issue before the Supreme Court of Canada was whether the information could be construed as property for the purposes of the Criminal Code. Lamer J. (as he then was) discussed the nature of trade secrets:

“It can be argued – as Professor Weinrib does in “Information and Property” (1998), 38 U.T.L.J. 117 – that confidential information is property for the purposes of civil law. Indeed, it possesses many of the characteristics of other forms of property: for example, a trade secret, which is a particular kind of confidential information, can be sold, licensed or bequeathed, it can be the subject of a trust or passed to a trustee in bankruptcy.... As the term “property” is simply a reference to the cluster of rights assigned to the owner, this protection could be

pieces of information are capable of being trade secrets, though the secrecy of some information may be only short-lived

6 Stewart supra, at 10.
7 Seager v. Copydex Ltd., [1967] 1 W.L.R. 923 (C.A.) at 936, see Fairbairn & Thorburn at 3-16.
10 See generally Barry B. Sookman, Computer, Internet and Electronic Commerce Law (Toronto, On.: Carswell, Release 2, 2008) at 4-7 [hereinafter “Sookman”] and Hughes in “Trade Secrets and Confidential Information” supra at 24-33.
11 Stewart supra, at 10.
13 Stewart supra at 23.
given in the form of proprietary rights. The cases demonstrate that English and
Canadian civil law protect confidential information. However, the legal basis for
doing so has not been established by the courts... It appears that the protection
afforded to confidential information in most civil cases arises more from an
obligation of good faith or a fiduciary relationship than from a proprietary
interest.”

The Supreme Court of Canada further developed the basis for the protection of trade secrets in
*International Corona Resources Ltd. v. LAC Minerals Ltd.*14 (“LAC”). In this case, two parties
were negotiating a possible joint venture to develop a mining property. In the course of the
negotiations, one party disclosed information to the other regarding the location of a valuable
mineral deposit. The party receiving the information decided to develop the property alone,
purchased the property unbeknownst to the disclosing party, and ended the negotiations. In the
*LAC* decision, the Supreme Court of Canada set out the common elements of a breach of
confidence action, adopting the test set out in the *Coco v. A.N. Engineers* decision.15 The three
main elements of the cause of action, which have been applied consistently in Canadian breach
of confidence cases, are as follows:

(i) The information at issue must be confidential;
(ii) The information must have been communicated in confidence; and
(iii) The information was misused by the party to whom it was communicated.

To establish the cause of action, each of the elements (which are discussed below) must meet the
objective standard set forth in the English Court of Appeal decision in *Coco v. A.N. (Engineers)
Ltd.*16 The following standard was adopted in Canada in *LAC*, and has been cited with approval
in many subsequent cases:17

“...if the circumstances are such that any reasonable man standing in the shoes of
the recipient of the information would have realized that upon reasonable
grounds the information was being given to him in confidence, then this should
suffice to impose upon him the equitable obligation of confidence. In particular,
where information of commercial or industrial value is given on a business-like
basis and with some avowed common object in mind... I would regard the
recipient as carrying a heavy burden if he seeks to repel a contention that he was
bound by an obligation of confidence.”

The objective standard does not require that a term of confidentiality be explicit. Rather, the
nature of the relationship and circumstances of disclosure may reasonably imply confidence. If a
person should have realized that the information was to remain secret, an obligation to maintain
secrecy may arise.18

---

15 *Coco* supra.
16 *Ibid.* at 47.
17 *LAC* supra at 613. See also Fairbairn & Thorburn *supra* at 3-10.
18 Fairbairn & Thorburn *supra* at 3-11.
(i) **Quality of Confidence**

The person who is claiming an unauthorized disclosure or use of confidential information has the burden of proving, on the objective standard identified above, that the information was in fact confidential and that there is some significant commercial value in protecting the information or some loss of market advantage through its disclosure and use. All the circumstances in each particular case will be examined to make this determination, but there are three specific factors the Canadian courts will consider in determining that the information has the requisite quality of confidence and considered valuable by the owner. These factors are as follows:

1. Whether the information is public or unknown to others within that business or specific industry;
2. Whether the information is capable of acquisition elsewhere by those outside the business entity; and
3. Whether measures were in place to ensure the secrecy of the information.

Each of the factors is discussed below.

**Public or Generally Unknown Information**

Trade secrets differ from other forms of intellectual property protection in that the rights to confidential information dissolve upon discovery. Public knowledge won’t gain trade secret protection. As stated by the English Court of Appeal in *Saltman Engineering Co. v. Campbell Engineering Co.*:

> "I think that it shall not be stating the principle wrongly, if I say this with regard to the use of confidential information. The information, to be confidential, must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge"

Information which is revealed in the media, in published patents, public files, published annual reports, and even in advertising or other promotional materials cannot be considered confidential information and will not gain trade secret protection. There is also an obligation on the defending party to show that only public information was relied upon where partly public and partly private information is available. As stated by the English Court of Appeal in *Seager v. Copydex Ltd.*:

---

20 See Fairbairn & Thorburn *supra*, at 3-5.
21 [1963] 3 All E.R. 413 at 415.
23 As in LAC, *supra*.
24 *Eldon Industries Inc. v. Reliable Toy Co.* (1964), 44 C.P.R. 239 (Ont. H.C.J.) at 249 [herinafter "Eldon Industries"]). See also Fairbairn & Thorburn, *supra* at 3-12.
“When the information is mixed, being partly public and partly private, then the recipient must take special care to use only the material which is in the public domain. He should go to the public source to get it: or, at any rate, not be in a better position than if he had gone to the public source. He should not get a start over others by using the information which he received in confidence. At any rate, he should not get a start without paying for it.”

Public information, however, can be used in developing imitation products. For example, in Eldon Industries Inc. v. Reliable Toy Co., a toy company was sued for imitating the design of a toy dump truck that had been marketed and sold in Canada and the United States. The court determined that since the toy company had not based its truck design on technical drawings, but rather on publicly available advertising and marketing material, there was no breach of confidence.

Voluntary communication, such as intentional public disclosure for advertisement purposes, will negate the quality of confidence in the information and destroy the basis of a claim to secrecy. But minor, isolated disclosures of insignificant material, limited demonstration or promotional literature that does not give technical details will not put the information in the public domain. Disclosure of more substantial information, however, such as the technical capacities or details of a computer program, will destroy confidentiality.

As well, if the information is known in the industry outside the particular business in question, there will be no duty to maintain confidentiality. If, however, constituent parts of an idea are known in an industry, but a particular combination is not known, then the unique combination may constitute a trade secret. For example, the constituent parts of a secret formula or recipe may be readily known or ascertainable by the public, but as long as the whole result is not known, the information may still be secret.

Notwithstanding the foregoing circumstance, a company should still show that the information was only known to its employees. The exact number of people who may know the information before it will lose the quality of secrecy depends on the situation. For instance, if a small number of principal people to whom the secret is valuable know the information, like a competitor, the trade secret will lose protection. But if the confidential information is known to a great many people in a company but not to the competitors, it may still retain the quality of secrecy. As stated in Stevens v. Avery:

---

26 Eldon Industries supra.
27 Fairbairn & Thorburn supra, at 3-12.
28 Ibid. at 3-9.
29 See Sookman at 4-40.
30 Ibid. at 4-40.
31 Fairbairn & Thorburn, supra, at 3-8.
32 See FBI supra.
33 See Sookman supra, at 4-37.
34 See R. L. Crain supra, where the claim was dismissed because the judge found too many people knew the information.
35 See Sookman supra, at 4-38 to 4-39.
“The mere fact that two people know a secret does not mean that it is not confidential. If in fact information is secret... it is capable of being kept secret by the imposition of a duty of confidence on any person to whom it is communicated. Information only ceases to be capable of protection as confidential when it is in fact known to a substantial number of people.”

Absolute secrecy, then, is not required, nor is secrecy lost through limited communications that are made without a view to publication. However, the line between confidential information and public information is not precise and will be drawn by the courts based on the circumstances of the case.

**Information Capable of Acquisition**

Even if the information was not in the public domain, the courts will also consider whether the information could have been obtained from non-confidential sources. Persons charged with using confidential information in developing similar products can defend against such accusations by showing the product was developed through reverse engineering or that the secret was ascertained using public sources. In *Molnar Lithographic Supplies Ltd. v. Sikatory*, for example, the court found that former employees had discovered a secret formula from trial and error and reliance on trade manuals, rather than from confidential information obtained during employment.

But just because a comparable product could be developed using public information does not necessarily relieve the defendant of all liability. The courts may award damages based on any advantage a person gained through the use of confidential information. The test is to compare the actual time the defendant took in developing the product with the estimated time that would be required to develop such a product without access to confidential information. For example, in *Cadbury Schweppes Inc. v. FBI Foods Ltd.* (“FBI”), protection was still extended to a formula for “clamato juice” even though the court recognized that juice mixing wasn’t “rocket science” and determined that a suitable imitation formula could have been easily developed. Nevertheless, the court determined that the use of confidential information gave FBI Foods a twelve month head-start. The court extended protection to the formula, but only granted a remedy for damages based on the “springboard” advantage gained through the use of confidential information.

**Measures in Place to Ensure Secrecy**

The final factor the courts consider in determining whether information has the requisite confidentiality to gain trade secret protection, is the measures that were in place to protect the information. While an owner of confidential information does not have to protect the

---

37 See Sookman *supra*, at 4-39.
39 Fairbairn & Thorburn *supra*, at 3-13 to 3-14.
40 FBI *supra*.
41 Hughes *supra*, at 23.
information against “unanticipated, undetectable, or unpreventable methods of discovery,” it is necessary for the business to have made some attempt to protect the secret to establish that it considered the information valuable enough to warrant protection. The circumstances of the particular case will determine if a corporation has sufficiently protected the information at issue. Please see the discussion at the end of this paper regarding practical approaches in this regard.

(ii) Information Imparted in Circumstances Implying Confidence

The second requirement of the LAC test is that the information must be imparted in circumstances that imply confidence. The factors courts will consider in determining if the information was imparted in confidence include whether the information was given gratuitously or for consideration, past practice and industry standard, the warnings and/or instructions given upon disclosure, and what commercial obligations may be applicable. Information that is imparted expressly as non-confidential will obviously not gain protection. Neither will information that is imparted to a party without the opportunity to reject the disclosure. Further, if the party didn't understand the information was imparted in confidence or didn't understand the purpose for which the disclosure was made, there will be no liability.

Confidence may also be implicit in a relationship, such as between partners in a business or joint-venturers or those intending to enter such a relationship. In such cases, the court can impose an expectation of confidence even where one does not explicitly exist. In LAC, for example, the fact that the parties were part of a joint venture was sufficient for the court to determine there was a reasonable expectation of confidence in the relationship. Third parties can also be held responsible for a breach where they understand that they are receiving information that was communicated in confidence between the original parties.

If information is conveyed in a business-like manner with some common objective in mind, this will generally generate a reasonable expectation of confidence. Corporations cannot take confidential information of a third party and use such information in a different application, even for an eventuality that was not originally contemplated. For example, in Ticketnet Corp. v. Air Canada, two corporations held negotiations to enter a common ticketing arrangement. The negotiations fell through, however, and Air Canada used the information gained from the plaintiff to pursue the opportunity alone. The court found that while no contract had been

42 Sookman supra, at 4-39.
43 See LAC supra, at 604, FBI supra, at 115, and Fairbairn & Thorburn supra, at 3-18.
44 Sookman at 4-95 for additional examples.
45 Ibid.
46 Ibid.
47 Chris G. Paliare, “When Will Confidential Obligations be Imposed by the Common Law?” in Trade Secrets and Confidential Information supra at 3 [hereinafter “Paliare”].
48 LAC supra.
49 See FBI supra, at 155, Fairbairn & Thorburn suora, at 5-14 to 5-14.1, and Paliare supra, at 2.
50 See Sookman supra, at 4-15.
concluded, a mutual duty of confidentiality had arisen between the parties not to use information disclosed in the negotiations to the detriment of the other party.\textsuperscript{52}

Other relationships that impose an expectation of confidence include manufacturers and distributors, manufacturers and designers, consultants and independent contractors who are handling a corporation's confidential information, licensors and licensees of technology, and designers and the manufacturers of technology.\textsuperscript{53}

In \textit{LAC}, breach of fiduciary duty was pled in addition to breach of confidence. While it is a well established principle that a fiduciary relationship automatically imposes a duty of trust and confidence,\textsuperscript{54} Canadian courts have been reluctant to impose fiduciary obligations in arms length commercial relationships. Sopinka, J. stated in \textit{LAC}:\textsuperscript{55}

\begin{quote}
\textit{“...the fact that confidential information is obtained and misused cannot itself create a fiduciary obligation. No doubt one of the possible incidents of a fiduciary relationship is the exchange of confidential information and restrictions on its use. Where, however, the essence of the complaint is misuse of confidential information, the appropriate cause of action in favour of the party aggrieved is breach of confidence and not breach of fiduciary duty.”}
\end{quote}

The court has refused to impose a fiduciary duty to arm’s length commercial transactions in two recent Ontario decisions.\textsuperscript{56} However, directors and officers of a corporation do stand in a fiduciary position with respect to a company’s confidential information, as discussed below.

(iii) Misuse of Confidential Information

The third and final element of a breach of confidence action is whether the information was misused by the party it was communicated to. The case law suggests that the standard for this element is not very difficult to meet. It appears that where a duty of confidence exists between parties to use information for a specific purpose, virtually any use, other than for that purpose, may likely be considered an inappropriate use.\textsuperscript{57} Proof of monetary detriment is not required, as equity will enforce the obligation of confidentiality. Where a duty of confidence has been established, the courts have not barred a remedy for want of an inappropriate use.\textsuperscript{58}

\textsuperscript{52} See Sookman \textit{supra}, at 4-17.


\textsuperscript{54} Fairbairn & Thorburn at 5-9.

\textsuperscript{55} \textit{LAC supra}, at 600.


\textsuperscript{57} See \textit{LAC supra} and \textit{Paliare supra}, at 7.

\textsuperscript{58} See Sookman \textit{supra}, at 4-93 to 4-98 for a complete discussion.
3. **The Sui Generis Nature of an Action for Breach of Confidence**

The *LAC* decision highlights the *sui generis* nature of an action for breach of confidence. As Sopinka J. commented:

“The foundation of action for breach of confidence does not rest solely on one of the traditional jurisdictional bases for action of contract, equity or property. The action is *sui generis* relying on all three to enforce the policy that confidences be respected.”

The *sui generis* doctrine has been elaborated in several cases since *LAC*. These decisions characterize actions for breach of confidential information in a flexible manner, thus allowing the courts to provide an appropriate remedy in the circumstances. As stated in *Apotex Fermentation Inc. v. Novopharm Ltd.*:

“The courts’ attitude to jurisdictional sources has thus been a pragmatic one. Their principle concern has been, not to classify the breach of confidential action into an existing conceptual category, but to use existing categories to enforce the more fundamental notion of confidence.”

The pragmatic approach of treating trade secrets in a *sui generis* fashion was also addressed in *FBI*. In that case, Binnie J. agreed with the lower courts that the basis of the liability lay in equity. Since the information was transmitted in confidence to Caesar Canning, the party to the original licence, an obligation of confidentiality followed the transmission to FBI Foods, a third party. Binnie J. stated:

“Equity, as a court of conscience, directs itself to the behaviour of the person who has come into possession of information that is in fact confidential, and was accepted on that basis, either expressly or by implication. Equity will pursue the information into the hands of a third party who receives it with the knowledge that it was communicated in breach of confidence (or afterwards acquires notice of that fact even if innocent at the time of acquisition) and impose its remedies.”

With respect to the *sui generis* nature of the action, Binnie J. acknowledged that the “reference to anything as *sui generis* tends to create a frisson of apprehension or uncertainty amongst lawyers” but reaffirmed that the *sui generis* approach was adopted to recognize the flexibility that has been shown by courts in the past to uphold confidentiality and in crafting remedies for its protection.

---

59 *LAC* supra, at 157.
62 *FBI* supra, at para. 19.
4. Protection of Trade Secrets in the Employment Context

Depending on the nature of the employment relationship, trade secret obligations between employees and employers may arise in a number of ways:

1. They may arise from an implied duty of good faith which exists during the term of employment, and to a lesser extent, after employment ends;

2. They may arise from fiduciary obligations which arise particularly when the employee is occupies a position of power within the employer company;

3. They may be specified in an employment contract or a non-competition agreement between employer and employee.64

Each of these obligations will be considered briefly below.

1. Implied Duty of Good Faith

Generally, employees owe a common law duty of “good faith and fidelity” to employers.65 On the basis of this duty, an employee is bound not to disclose or use for purposes that are adverse to his employer’s interests, confidential information received by him in his capacity as employee. An employee is also bound by the duty of good faith not compete with his employer during the employment relationship, even in the employee’s spare time. Furthermore, the employee is also bound to disclose to his employer valuable information which he receives from another employee and which is unknown to his employer.66 Employees must fulfil this duty faithfully, deal with an employer’s property (including confidential information) appropriately, and not interfere with these duties in the course of his or her employment.67 Such obligations are diminished, however, upon termination of employment. Depending on the circumstances, some information that the employee had a duty to protect while employed, may be disclosed in good faith after termination of employment.

Generally, former employees may pursue customers of their former employers, so long as they do not use customer lists or other confidential information of the employer.68 However, in RBC Dominion Securities Inc. v. Merrill Lynch Canada Inc (“RBC”), the British Columbia Court of Appeal held that the duty of confidentiality owed by former employees extends to client records but not to client lists.69 In RBC there was a mass defection by employees of one securities brokerage firm to another. The former employer sued the new employer and its former employees for breach of confidence in respect of client files and information that the departing employees took with them and used in their new positions. The majority of the Court held that as a matter of law, departing employees do not owe an implied duty to their former employer not to

---

66 Sookman supra, at 4-57.
67 Ibid. at 4-57.
68 Sookman supra, at 4-59.
compete unfairly. Furthermore, while the former employees had a duty not to take away confidential documents and trade secrets, this duty was limited. The former employees were allowed to take a list of his or her own client lists and contacts but could not take information for other advisors’ clients or copies of account statements. The majority further found that, while the defendant employees had strayed across the line, there was no causal connection between the breach of confidence and the plaintiff’s loss of customers to the defendant brokerage.

Generally, customer information can be used post employment unless the information could only be gained through employment rather than through general public information known to all competitors. For example, in *Barton Insurance Brokers Ltd. v. Irwin* a former employee solicited her former employer’s customers using client contact information that she had memorized. The British Columbia Court of Appeal upheld the trial judge’s finding that as a “mere employee” she did not have a fiduciary duty to refrain from using the confidential information. Absent an enforceable non-competition agreement, she was entitled to recall the names of former clients and use a telephone book to contact them to solicit their business. As Hall J.A. explained for the Court:

...Absent an enforceable agreement to refrain from soliciting former customers, I am not of the view that any duty, fiduciary or otherwise, should have been found to prevent Ms. Irwin from canvassing former clients...the general interest of the public in free competition and the consideration that in general citizens should be free to pursue new opportunities, in my opinion, requires courts to exercise caution when imposing restrictive duties on former employees in less than clear circumstances. Generally speaking, as I noted from the earlier authorities referred to, the law favours the granting of freedom to individuals to pursue economic advantage through mobility in employment.

The Canadian case law reflects a constant tension in the employment law context between the information which belongs to the company, and the information which forms part of the employee’s “know-how” – the particular aptitudes, skills, mental and physical abilities of the individual. Whereas the former belongs to the company, the employee is free to use the latter in competition with the former employer. The “know-how” employees gain is often called the “subjective knowledge” that remains the individual’s property. Only “objective knowledge”, being the trade secrets of the corporation, cannot be used once employment has been terminated. Objective knowledge is defined as what a person of ordinary honesty and intelligence would recognize to be the property of the former employer and not his own. Though many cases have been decided on the distinction between objective and subjective knowledge, the courts have expressed concern that this distinction is hard to define and, in fact, almost meaningless.

---

70 Sookman supra, at 4-59.
72 Ibid. at para 39.
73 Sookman supra, at 4-54.2. See also Paliare supra, at 17 to 21 and Thorburn & Fairbairn supra, at 4-7 to 4-9.
74 Thorburn & Fairbairn supra, at 4-9 to 4-10.1. For a discussion of this distinction see *Genesta Mfg. Ltd. v. Babey* (1984) 2 C.P.R. (3d) (Ont. H.C.) [hereinafter “Genesta”].
75 Sookman supra, at 4-65.
76 Ibid. at 4-67.
2. **Fiduciary Duty**

Officers, directors, and senior management owe a fiduciary duty to act in the best interests of the corporation, which is a more stringent duty than generally required of other employees. The test for a fiduciary relationship is well established. To determine if a fiduciary relationship exists, the courts generally look at three factors:

a. Whether the fiduciary has scope for the exercise of some discretion or power;

b. Whether the fiduciary can unilaterally exercise that power or discretion to affect the beneficiary’s interests; and

c. Whether the beneficiary is vulnerable to or at the mercy of the fiduciary exercising the discretion of power.

A fiduciary is not allowed to take an opportunity from the corporation, even after the termination of employment. The various factors considered include:

...the position or office held, the nature of the corporate opportunity, its ripeness, its specificity and the director’s or managerial officer’s familiarity with it, the amount of knowledge possessed, the circumstances in which it was obtained and whether it was special or, indeed, even private, the factor of time in the continuation of fiduciary duty where the alleged breach occurs after termination of the relationship with the company, and the circumstances under which the relationship was terminated.

3. **Contracts and Non-Competition Agreements**

In addition to the common law duty, confidentiality is often addressed in contractual agreements between employers and employees to avoid any dispute concerning use of confidential information.

Non-disclosure covenants (whether included in employment agreements or on a stand-alone basis) are commonly used to prevent disclosure of trade secrets for a reasonable period after the termination of employment. In determining whether such a covenant is unreasonable, the court will balance the commercial interests of the corporation in the information with the interests of the former employee to use the knowledge and skills gained in employment. Information that is in the public domain, or otherwise not protected as a trade secret, cannot be protected merely

---

78 See *LAC supra*, at 599.
80 *Sookman supra*, at 4-61.
82 *Sookman supra*, at 4-74.
through its express inclusion in an agreement. However, the inclusion of express terms of non-
disclosure in an employment contract makes it more likely that the court will find the
information to be a trade secret and not the subjective knowledge of the employee.

Non-competition agreements are another measure used by companies to help protect their trade
secrets. Such agreements, however, are presumed to be void on the policy basis that any such
restrictions are an illegal restraint on trade. The presumption can be rebutted, however, with
proof that the restraint protects the legitimate interests of the corporation without unduly
restricting the rights of the employee. More generally, employers can restrain employees from
using confidential information as a “springboard” to get a head-start in development of a
competitive product. However, all covenants must be reasonable and cannot go beyond the
time and scope necessary to protect the information. This requires that the covenant be specific
enough that the employee can determine with certainty where and when he or she can work in
the future.

5. Remedies for Disclosure of Trade Secrets

Methods of enforcement in Canada, whether in the employment context or more generally,
include both civil action and criminal prosecution.

1. Civil Action

The equitable, sui generis nature of actions in breach of confidence is most apparent in the
flexibility in remedies that courts have awarded in these circumstances. There is some authority
to state that the remedy may be dependant on the nature of the confidence and the breach.
Leading case law, such as the FBI decision, suggest that the nature of equity means that all
remedies should be available and fashioned on a case-by-case basis. As Binnie J. stated in FBI:

“The result of LAC Minerals is to confirm jurisdiction in the courts in a breach of
confidence action to grant a remedy dictated by the facts of the case rather than
strict jurisdictional or doctrinal considerations”.

---

83 Ibid. at 4-75.
84 See for example Matrox Electronic, supra.
85 Ibid. at 4-80 to 4-81. See also Elsley v. J.G. Collins Insurance Agencies Ltd., [1978] 2 S.C.R. 916 at 923-924
[hereinafter “Elsley”].
86 Ibid. at 4-80. This principle was recently reaffirmed by the Ontario Court of Appeal in H.L. Staebler Company
Limited v. Allan, 2008 ONCA 576 at paras. 33-36 [hereinafter “Staebler”]. Specifically, the Court reiterated that:

While an overly broad restraint on an individual’s freedom to compete will generally be unenforceable, the
courts must recognize and afford “reasonable protection to trade secrets, confidential information, and
trade connections of the employer.”

87 Ibid. at 4-82. See also Matrox Electronic, supra.
88 Ibid. at 4-83 and Staebler, supra at para. 36.
89 Ibid. at 4-84; see for example Wilson Learning Corp. v. Hurley (1990), 33 C.P.R. (3d) 172 (Ont. H.C.) and
90 FBI supra, at para 24.
As such, the plaintiff in a breach of confidence action has a wide range of remedies available and may elect whichever is appropriate.91

Breach of confidence is most commonly remedied through injunction, damages, or an Anton Piller order.92 Remedies can also be found, though less commonly, in an accounting for profits or constructive trusts.93

The measure of damages in breach of confidence cases remains controversial.94 Damages in breach of confidence actions are meant to compensate for loss or injury and to try to place the injured party in the same position as they would have been but for the disclosure of the trade secret.95 But when dealing with an intangible such as information, it is typically very difficult to determine what damages are appropriate. Several measures have been used based on the defendant’s net profits, the development costs of the information, the market value of the information if it were sold, or loss of profit.96

Accounting for profits has also been applied to breach of confidence cases where the wrong can be characterized as an unjust enrichment.97 In Canada, though, the courts have made clear that accounting for profits will not be applied in cases where the information was of limited value, and will be limited in situations where the “springboard” principle is applied.98 This latter principle, which was applied in the FBI decision, essentially provides that where a competitor, be it a former employer or third party, is able to develop a competitive product quicker than they would have done without the use of that information, such persons should not be allowed to profit from this unfair advantage.99 In these circumstances, the case law suggests damages will be awarded based on the profits earned for this period.100

2. **Criminal Prosecution**

While any number of civil remedies are available to a person who has been aggrieved with respect to the disclosure of confidential information, in Canada, criminal prosecution for the misappropriation of a trade secret is a more tenuous proposition.

As noted above, the application of the Criminal Code to trade secrets was considered by the Supreme Court of Canada in Stewart.101 Speaking for the Court, Lamer J. found that confidential information is not capable of being “stolen” because it does not qualify as property for the

91 M.B. Gehlen, “Remedies for Misuse of Confidential Information” in Trade Secrets and Confidential Information, supra, at 4 [hereinafter “Gehlen”].
92 See Sookman supra, at 4-96 for a complete list. See also Fairbairn & Thorburn supra, at 7-1 to 7-20 and Gehlen supra.
93 See LAC supra, at 4-109 for a complete list of the basis for compensation that have been used by the courts.
94 See Gehlen supra, at 5 to 9, and Fairbairn & Thorburn supra, at 7-18.
95 See LAC supra, at 619.
96 See Sookman supra, at 4-109 for a complete list of the basis for compensation that have been used by the courts.
97 See Sookman supra, at 4-110. See also Fairbairn & Thorburn supra, at 7-14.
98 See Gehlen supra, at 10.
99 See Paliare supra, at 22, Fairbairn & Thorburn supra, at 3-16.1.
100 FBI supra, at para. 101.
101 Stewart, supra..
purposes of the theft provisions of the *Criminal Code*. Lamer J. further found that except in very unusual circumstances, confidential information is not of a nature such that it can be taken or “converted” as required by the definition of “theft” in the *Criminal Code*. In *Stewart*, Lamer J. also considered the applicability of the fraud provisions of the *Criminal Code*. He found that the accused’s conduct did not amount to fraud as the hotel did not suffer an “economic loss” which resulted in the requisite “deprivation” necessary to establish fraud. However, in the context of making this assertion, Lamer J. endorsed the finding of the dissenting judge at the Ontario Court of Appeal who stated that:

*The deprivation would be clear if the confidential information had been in the nature of a trade secret or copyrighted material having a commercial value intended to be exploited by the victim.*

Thus, the availability of criminal enforcement remains uncertain in Canada. While it would appear that prosecution for theft is not possible, it may still be feasible to pursue criminal prosecution on the basis of fraud.

6. **Practical Approaches to the Protection of Trade Secrets and Other Confidential Information**

There are a number of practical steps organizations can take in an effort to proactively protect its trade secret information.

Typically, and as noted above, prudent organizations ensure that employees are bound by appropriately comprehensive contractual obligations regarding the confidential information of the employer, as well as reasonably drafted restrictive covenants addressing the post-employment context. Ideally, these obligations would be formalized as part of the employment agreement entered into prior to the commencement of the employment relationship or, if not appropriately addressed at that time, as early as possible in the employment relationship.

Notably, in Canada, these steps are increasingly being undertaken as part of broader legal compliance and information management initiatives designed to address all of the information in an organization’s custody and control.

For instance, all Canadian private sector privacy statutes contain specific provisions relating to the safeguarding of personal information, and obligations to develop specific written policies, practices and procedures for the implementation of technical, administrative and organizational safeguarding measures. Notably, evidence of such written security policies, practices and procedures—as part of an information security governance structure—is a key factor considered

---

by privacy regulatory authorities in the course of their investigations of security breach incidents and their determination of whether an organization established reasonable safeguards. Similarly, organizations that deal with payment card information are required under the Payment Card Industry (“PCI”) Data Security Standards to establish an information security governance structure for the protection of payment card information under their custody and control. More generally, many companies are addressing these issues in connection with the formulation of document retention policies and/or knowledge management initiatives.

As such, in addition to standard provisions of employment contracts, organizations seeking a robust information security governance program to protect trade secrets, personal information and payment card information are relying on an emerging standard of security guidelines and principles, such as those contemplated in the International Standards Organization’s Information technology – Security techniques – Code of practice for information security management ISO/IEC 17799:2005 standard. These guidelines set out best practices of information security control objectives and controls for information security management.

By way of reference, ISO 17799 addresses the following are the principal components of an information security governance structure:

- Risk assessment;
- overall security policy;
- organization of information security (information security governance);
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access controls;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management; and
- compliance.

The implementation of a robust information governance structure will involve, among other things, a detailed set of written security policies and procedures as well as the development and
implementation of specific and regular training and awareness programs for information security in connection with the roll-out and ongoing compliance of the information security requirements. Notably, the majority of security incidents involving the misuse of data (including personal information) are caused by internal employees, and regular training and awareness is a key factor considered by privacy regulatory authorities in the course of their investigations of security breach incidents and their determination of whether an organization established reasonable safeguards. Another critical component to effective information security is regular third party and internal threat and risk assessment/penetration and vulnerability testing, and other processes to assess and address technical, physical, and administrative security risks and identify solutions.