Stikeman Elliott

Bank Secrecy Laws (Canada)

By Shawn Smith, Wesley Ng, Stikeman Elliott LLP,
with Practical Law Data Privacy Advisor

THOMSON REUTERS
PRACTICAL LAW

Bank Secrecy Laws (Canada)

SHAWN SMITH AND WESLEY NG, STIKEMAN ELLIOTT LLP, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

Search the Resource ID numbers in blue on Westlaw for more.

A Practice Note discussing the laws, regulations, and guidance governing bank secrecy in Canada under the common law, the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (PIPEDA), and the Bank Act. This Note provides general guidance for a banking institution handling customer data in Canada on complying with bank secrecy obligations, the circumstances in which it can disclose customer data to third parties, and required steps to permit disclosure.

Bank secrecy laws generally prohibit banking institutions, and their officers and employees, from disclosing customer data to third parties. However, banks commonly need to disclose customer data for routine business purposes including:

- Providing products or services to customers.
- Making inter-company transfers.
- Outsourcing to third-party service providers.
- Responding to litigation and regulatory inquiries.

Global banks operating in jurisdictions with bank secrecy laws must find practical solutions to perform business functions or face sanctions including fines, regulatory actions, private lawsuits, and, in severe cases criminal sanctions for disclosing customer data in violation of bank secrecy laws.

This Note discusses the laws, regulations, and guidance governing bank secrecy in Canada. It provides guidance for a banking institution handling customer data collected in Canada on complying with bank secrecy and outsourcing obligations, the circumstances in which it can disclose customer data to third parties, and required steps to permit disclosure.

For information on global bank secrecy laws, see Practice Note, Global Bank Secrecy Laws: Overview (W-002-8052).

CANADA BANK SECRECY LEGAL FRAMEWORK

Unlike many other jurisdictions, Canada does not have specific legislation governing bank secrecy. However, banks collecting customer data in Canada are subject to certain laws that collectively establish a legal framework for the collection, use, and disclosure of customer data including:

- The common law duty of confidentiality, which banks owe to their customers (see Common Law Duty).
- The Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (PIPEDA) (see PIPEDA).
- Certain provisions of the Canada Bank Act (Bank Act, S.C. 1991, c. 46) (Bank Act) (see Bank Act).

COMMON LAW DUTY

Canadian courts have followed the English Court of Appeal's decision in *Tournier v. National Provincial and Union Bank of England* [1924]1 K.B. 461 (C.A.), which is the leading authority on a banker's common law duties owed to a customer. *Tournier* held that a banker owes a customer an implied contractual duty not to disclose the customer's data to third parties except under certain circumstances (see Exceptions Permitting Disclosure).

COVERED PERSONS AND ENTITIES

The common law duty to protect customer data applies to the relationship between the bank and the customer. A bank includes banks identified under the Bank Act and any person acting in the capacity of a banker in Canada.

The duty generally lies with the bank, as an institution, to protect customer data. Banks must therefore take steps to ensure that their employees, directors, officers, agents, and other representatives maintain customer data under the common law duty.

The common law duty to protect customer data continues even after termination of the relationship between the bank and the customer (*Tournier*, 1 K.B. at 473).

PROTECTED CUSTOMER DATA

The common law duty to protect customer data applies to all data obtained by the bank from any source that relates to a customer (individual or corporate), except for information that is or becomes public (other than due to the fault of the bank). This includes data relating to:

- The customer's identity.
- Investments maintained and the value of the investments.
- Deposits and withdrawals.
- Loan information.
- Value of investments.
- Information given by the customer about the customer's financial circumstances.
- The customer's relationship with other banks, if any.

The common law duty to protect customer data from disclosure protects information relating to the applicable customer. Banks seeking to anonymize or aggregate customer data before disclosure so that the customer is not identified should ensure that they comply with PIPEDA (see PIPEDA: Disclosing Anonymized Personal Data).

EXCEPTIONS PERMITTING DISCLOSURE

Under *Tournier*, a bank's common law duty of confidentiality to its customers is not absolute and is subject to exceptions where:

- Applicable law requires disclosure (see Disclosure Required by Law).
- There is a duty to the public to disclose (see Duty to the Public to Disclose Customer Data).
- The interests of the bank require disclosure (see Bank's Interests Require Disclosure).
- The customer provides express or implied consent (see Customer Express or Implied Consent).

(See *Haughton v. Haughton* (1964), [1965] 1 O.R. 481 (Ont. S.C.); *Guertin v. Royal Bank*, (1983) 43 O.R. (2d) 363 (Ont. S.C.).)

The *Tournier* exceptions (other than consent) do not allow for many disclosures that banks typically need to make to third parties including to third-party service providers and related corporate entities. Banks should seek to rely on written customer consent rather than the other *Tournier* exceptions to disclose customer data to make necessary disclosures and avoid customers challenging the bank's grounds for disclosure (see Customer Express or Implied Consent).

Disclosure Required by Law

Canadian courts invoking *Tournier* have allowed banks to disclose customer data when the disclosure is required by law, which generally means under court orders and legislation (see, for example, *Haughton*, [1965] 1 O.R. 481 (the court held that a bank manager may only be compelled to testify by a specific order of the court and that a subpoena is insufficient to override the banker's duty of confidentiality); *Royal Bank of Canada v. Art's Welding & Machine Shop (1980) Ltd.*, (1989), 34 C.P.C. (2d) 190 (Alta. Q.B.) (the court held that a court order constitutes the compulsion of law to allow disclosure of customer data)).

An example of a disclosure required by law is section 628(1) of the Bank Act which requires banks to provide the Superintendent of Financial Institutions with information it requires (see Bank Act).

The compulsion of law exception may also include compulsion of a law outside of Canada (see *Park v. Bank of Montreal*, [1997] B.C.J. No. 787 (B.C.S.C.) (the court found that disclosure made by a Canadian branch of a Korean bank to the Korean criminal prosecutor's office constituted a compulsion of law because Korean law required the disclosure).

Duty to the Public to Disclose Customer Data

A duty to protect public interests can override the common law duty of bank secrecy in limited circumstances, such as where there is a danger to the state or the public (*Jubbal v. Royal Bank of Canada*, [1987] B.C.J. No. 1715) (B.C.S.C.). For example, courts have held that banks may disclose customer data under the public interest exception:

- For the purposes of preventing fraud whether it constitutes fraud or deceit in law (*Canadian Imperial Bank of Commerce v. Sayani* (1993), 11 B.L.R. (2d) 28 (B.C.C.A.)).
- For a liquidator of the Canadian Commercial Bank to disclose customer data under what is now known as the Winding-Up and Restructuring Act (see *Canada Deposit Insurance Corp. v. Canadian Commercial Bank* (1989), 71 C.B.R. 239) (Alta. Q.B.)).

Bank's Interests Require Disclosure

Banks may also disclose customer data where the interests of the bank require disclosure. However, banks must construe this exception narrowly (*Park v. Bank of Montreal*, [1997] B.C.J. No. 787 (B.C.S.C.)). Courts have found that banks can rely on this exception in specific circumstances to protect their interests including, for example:

- Where a bank has a security interest in a customer's property, it may protect that interest by advising others of the security interest (*Royal Bank of Canada v. Brattberg*, [1993] 8 W.W.R. 139 (Alta. Q.B.); *Royal Bank of Canada v. Vincenzi*, [1994] B.C.W.L.D. 1221 (B.C.S.C.)).
- Where the bank disclosed information about a dispute with its customer concerning a debt when the customer was attempting to incur other debt obligations (*Sayani*, 11 B.L.R. (2d) 28).

Customer Express or Implied Consent

Banks may also disclose customer data with the consent of the customer. Courts have held that certain relationships may provide the bank the customer's implied consent to disclose their data. For example, by giving a bank a security interest in property, courts have found that a customer consents to the bank disclosing that security interest to other interested parties (see, for example, *Vincenzi,* [1994] B.C.W.L.D. 1221).

However, banks should generally attempt to obtain express, written consent to disclose customer data rather than rely on implied consent for evidentiary purposes. Banks commonly obtain customer consent at the time the customer opens an account by requiring the customer to agree to the bank's standard terms and conditions and privacy policy. The standard terms and conditions and privacy policy should set out the bank's policies and practices concerning the collection, use, and disclosure of customer data under industry practice in Canada.

BANK ACT

The Bank Act governs all banks chartered in Canada. A bank charter defines the types of activities the bank may conduct and sets out the management obligations of the bank.

The Bank Act does not prohibit disclosure of customer data but consistent with the *Tournier* rules protects customer data from disclosure in various sections, including those that:

- Mandate bank directors, as part of their duty to supervise the management and business affairs of the bank, establish procedures for restricting the use of confidential information, which generally includes customer data (Section 157(2)(c), Bank Act).
- Require bank directors to designate a committee of the board of directors to monitor procedures for restricting the use of confidential information, which generally includes customer data (Section 157(2)(d), Bank Act).
- Obligate banks and their agents to take reasonable precautions to ensure that unauthorized persons do not have access to or use of their records, which generally includes customer data (Section 244(d), Bank Act).

Banks subject to the Bank Act must understand these provisions and ensure that they take steps to protect customer data. Banks violating the above provisions face fines of up to CAD500,000 on summary conviction, and CAD5 million on indictment (Section 985(1), Bank Act).

PIPEDA

PIPEDA governs the collection, use, and disclosure of personal information, in any form, by certain private-sector organizations, including banks. Personal information generally includes any information about an identifiable individual. Canadian courts and the OPC have found that information is about an identifiable individual when there is a serious possibility that an individual may be identified by using that information, alone or in combination with other information (see OPC: Interpretation Bulletin: Personal Information).

PIPEDA generally apply to any bank collecting personal information in Canada including foreign banks with offices, branches, and affiliates in Canada.

For more information on PIPEDA, see Practice Notes, Data Privacy Laws in Canada: PIPEDA (W-011-7386).

JURISDICTIONAL SCOPE

PIPEDA applies to personal information collected in Canada and generally does not apply to personal information collected outside of Canada. However, PIPEDA is silent on its territorial reach and Canadian courts have applied the common law "real and substantial connection" test to determine whether PIPEDA should apply and whether the OPC has jurisdiction to address a privacy complaint arising outside of Canada. The underlying question is whether there is a sufficient connection between Canada and the activity in question for Canada to apply its law.

In the recent decision of *A.T. v. Globe24h.com*, 2017 FC 114, the Federal Court determined that it had jurisdiction to make an extra-territorial order with worldwide effect against a foreign resident, requiring the foreign resident to remove documents from the internet where they contained personal information about Canadian citizens and violated PIPEDA.

PIPEDA generally does not apply to personal information collected outside of Canada.

PRINCIPLES

The ten fair information principles set out in PIPEDA form the basis of a bank's obligations when collecting, using, and disclosing personal information in Canada. These principles include:

- **Accountability**. Organizations are responsible for personal information in their possession or custody, including information that has been transferred to a third party for processing (Principle 1, Schedule 1, PIPEDA).
- **Identifying purposes**. Organizations must document and divulge to individuals the purpose for which their personal information is collected (Principle 2, Schedule 1, PIPEDA).
- **Consent**. Organizations may only collect, use, or disclose personal information with the knowledge and consent of the individual, subject to certain limited exceptions (Principle 3, Schedule 1, PIPEDA).
- **Limiting collection**. Organizations must limit the collection of personal information to what is necessary for the identified purposes and collect personal information by fair and lawful means (Principle 4, Schedule 1, PIPEDA).
- **Limiting use, disclosure, and retention**. Organizations must only use and disclose personal information for the purposes they collected it for, except with consent or as required by law. Organizations can retain personal information only as long as necessary to fulfill those purposes (Principle 5, Schedule 1, PIPEDA.).
- **Accuracy**. Personal information must be as accurate, complete, and up-to-date as is necessary to accomplish the purposes for which it is to be used (Principle 6, Schedule 1, PIPEDA).
- **Safeguards**. Organizations must protect personal information by safeguards appropriate to the sensitivity of the information (Principle 7, Schedule 1, PIPEDA).
- **Openness**. Organizations must make readily available to individuals specific information about its policies and practices relating to the management of personal information (Principle 8, Schedule 1, PIPEDA).
- **Individual access**. Individuals have the right to access and correct their personal information, subject to certain limited exceptions (Principle 9, Schedule 1, PIPEDA).
- **Challenging compliance**. Organizations must provide the means for an individual to challenge an organization's compliance with the above principles (Principle 10, Schedule 1, PIPEDA).

DATA TRANSFERS

In some situations, banks may want to transfer personal information cross-border including, for example, to the bank's overseas ground company or parent or to a third-party service provider. Under PIPEDA, banks remain responsible for all personal information

transferred to third parties inside and outside of Canada. Banks must use contractual measures or other means to ensure that third parties provide a level of protection that is comparable to the level of protection provided by the bank (see Outsourcing Considerations).

PIPEDA does not prohibit the cross-border transfer of personal information or distinguish between domestic and international transfers. However, the OPC has stated that an organization in Canada that transfers personal information to a foreign country should:

- Notify affected individuals about the transfer of their personal information to a foreign country.
- Inform affected individuals that their personal information may be available to the foreign country's government or law enforcement agencies under a lawful order made in that country.

Under Section 245 of the Bank Act, the Superintendent of Financial Institutions and Minister of Finance have the right in certain circumstances to:

- Prohibit the transfer or not process certain records, including those related to customer data, in certain countries.
- Maintain and process those records solely in Canada.

For more information, see the OPC's Guidelines for Processing Personal Data Across Borders and Practice Note, Cross-Border Personal Data Transfers (Canada) (W-009-4229).

CONSENT UNDER PIPEDA

PIPEDA generally requires the knowledge and consent of affected individuals to collect, use, and disclose their personal information. However, PIPEDA does provide certain exceptions where organizations do not need consent.

Circumstances Not Requiring Consent

Banks may collect and use personal information under PIPEDA without the knowledge or consent of the individual in certain circumstances, including where:

- The collection is clearly in the individual's interests and the organization cannot obtain consent in a timely way (Section 7(1)(a), PIPEDA).
- The collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province and collection with consent compromises the availability or the accuracy of the information (Section 7(1)(b), PIPEDA).
- The information is publicly available if the collection and use complies with the Regulations Specifying Publicly Available Information, SOR/2001-7 (13 December, 2000) (Regulations) (Section 7(1)(d), PIPEDA).
- It is required by law (Section 7(1)(e)(ii), PIPEDA).

PIPEDA also permits banks to use personal information without an individual's knowledge or consent where:

- The organization uses it to act in an emergency that threatens the life, health, or security of an individual (Section 7(2)(b), PIPEDA).
- It is contained in a witness statement and the use is necessary to assess, process, or settle an insurance claim (Section 7(2)(b.1), PIPEDA).

An organization may disclose personal information without the knowledge or consent of the individual in certain circumstances, including when the organization discloses the personal information to:

- Collect a debt owed by the individual (Section 7(3)(b), PIPEDA).
- Comply with a subpoena, warrant, or an order made by a court, person, or body with jurisdiction to compel the production of information or to comply with court rules relating to the production of records (Section 7(3)(c), PIPEDA).
- A government institution that has identified its lawful authority to obtain the information, and indicated that:
  - it suspects that the information relates to national security, the defense of Canada, or the conduct of international affairs;
  - it needs the information to gather intelligence, carry out an investigation, or enforce any law of Canada, a province, or a foreign jurisdiction;
  - it needs the information to administer any law of Canada or a province; or
  - it needs the information to communicate with the next of kin or authorized representative of an injured, ill, or deceased individual.

  (Section 7(3)(c.1), PIPEDA.)
- A government institution and the organization:
  - has reasonable grounds to believe that the information relates to a violation or potential violation of Canadian law or a foreign jurisdiction; or
  - suspects that the information relates to national security, the defense of Canada, or the conduct of international affairs.

  (Section 7(3)(d), PIPEDA.)
- Another organization and the disclosure is reasonable for the purposes of investigating a breach of an agreement or a violation of Canadian law and disclosure with consent compromises the investigation (Section 7(3)(d.1), PIPEDA).
- Another organization and the disclosure is reasonable for the purposes of preventing, detecting, or suppressing fraud and disclosure with consent compromises the ability to prevent, detect, or suppress the fraud (Section 7(3)(d.2), PIPEDA).
- A government institution or the individual's next of kin or authorized representative because it is necessary to identify an injured, ill, or deceased individual. If the individual is alive, the organization must inform the individual in writing without delay of the disclosure (Section 7(3)(d.4), PIPEDA).
- A person needing the information because of an emergency that threatens an individual's life, health, or security. If the individual is alive, the organization must inform the individual in writing without delay of the disclosure (Section 7(3)(e), PIPEDA).

Permitted disclosures also include when the personal information is:

- Contained in a witness statement and the disclosure is necessary to assess, process, or settle an insurance claim (Section 7(3)(e.1), PIPEDA).
- Publicly available and is specified by the Regulations (Section 7(3)(h.1)).

Decisions of the OPC and Canadian courts interpret the above exceptions narrowly and have further specified when organizations can rely on these exceptions. Banks should carefully consult PIPEDA and the applicable case law before collecting, using, or disclosing personal information without consent.

Obtaining Valid Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except in limited enumerated circumstances. The form of consent may vary depending on the circumstances and the type of information, considering the reasonable expectations of the customer. In determining the form of consent to use, organizations must consider the sensitivity of the information. Where the information is sensitive, express consent should generally be sought. (see OPC: Interpretation Bulletin: Form of Consent and OPC Guidelines for Obtaining Meaningful Consent).

PIPEDA does not specifically define sensitive information. However, financial information is generally considered sensitive. (see OPC Guidelines for Obtaining Meaningful Consent and OPC: Interpretation Bulletin: Form of Consent).

DISCLOSING ANONYMIZED PERSONAL DATA

The Office of the Privacy Commissioner of Canada (OPC) takes a strict view of anonymizing personal information under PIPEDA, particularly sensitive personal information, such as financial information. In a complaint against Canadian telecommunications company Bell Canada, the OPC found that Bell Canada violated PIPEDA despite steps it took to disclose only aggregated and anonymized information to advertisers. The OPC found that Bell Canada should have taken proactive steps, such as contractually prohibiting advertisers from using tracking cookies, device fingerprinting, account information or other tracking methods, to link ad profile information with the aggregated information to re-identify individuals. (see PIPEDA Report of Findings #2015-001, paras. 48-52). The OPC also questioned whether generating anonymous, aggregated data from particularly sensitive personal information, such as credit scores and using it for targeted advertising is appropriate in any circumstances (see PIPEDA Report of Findings #2015-001, paras. 53-58).

CUSTOMER DATA DISCLOSURES UNDER THE DATA PROTECTION LAWS AND COMMON LAW

Banks handling customer personal information face compliance obligations under the common law and PIPEDA.

ANALYZING COVERED DATA

Organizations must conduct separate analyses of their customer data handling and compliance obligations under their common law duties and PIPEDA because they protect different categories of data and apply in different circumstances. For example:

- PIPEDA broadly applies to the collection, use, and disclosure of personal information, while the common law duty protects the disclosure of a bank's customer data.
- Unlike the common law duty, PIPEDA does apply to information related to corporations.

POTENTIAL CONFLICTS

Banks may face a conflict between the common law and PIPEDA where one law allows for disclosure of information and the other does not. For example, a bank may face a situation where a *Tournier* exception permitting disclosure applies (other than consent) but an exception does not apply under PIPEDA permitting the disclosure. In this case, banks must obtain express consent for the disclosure under PIPEDA.

OUTSOURCING CONSIDERATIONS

COMMON LAW DUTY AND OTHER CONSIDERATIONS

Banks outsourcing their services to third-party service providers remain accountable for all outsourced activities, including the unauthorized disclosure of customer data. Banks must therefore conduct due diligence on third-party vendors before their engagement to ensure that, among other things, they can adequately protect customer data to the extent the third-party vendor can be given access to that data.

The Office of the Superintendent of Financial Institutions issued B-10 guidelines (Guidelines) setting out its expectations for federally regulated entities, including banks, that outsource or contemplate outsourcing one or more of their business activities to a service provider. The B-10 guidelines are not legally binding although Canadian banks generally treat them as though they are binding.

Under the Guidelines, banks are, among other things expected to:

- Evaluate the risks associated with all existing and proposed outsourcing arrangements.
- Develop a process for determining the materiality of arrangements.
- Implement a program for managing and monitoring risks, commensurate with the materiality of the arrangements.
- Ensure that the board of directors, chief agent, or principal officer receives information sufficient to enable them to discharge their duties under the Guidelines.
- Refrain from outsourcing certain business activities to the external auditor.
- Have contractual provisions setting out the bank's requirements for confidentiality and security which should meet a reasonable standard under the circumstances. The contract or outsourcing agreement should address:
  - which party has responsibility for protection mechanisms;
  - the scope of the information to be protected;
  - the powers of each party to change security procedures and requirements;
  - which party may be liable for any losses that may result from a security breach and notification requirements if there is a breach of security; and
  - the service provider's obligation to store the bank's customer data separately from the data provided by other clients.

PIPEDA

Under PIPEDA, organizations remain responsible for all personal information transferred to third parties, including outside of Canada (Principle 1, Section 4.1.3, Schedule 1, PIPEDA). Banks should perform pre-engagement due diligence on third-party service providers to ensure they can properly safeguard personal information. Effective due diligence requires banks to review and collaborate among privacy and data security staff, applicable business or operations groups, and the vendor to:

- Identify the types of personal information the bank needs to transfer, based on the proposed scope of work, to understand the sensitivity of that personal information.
- Explore options to lower risks by minimizing the vendor's proposed access to and use of personal information while still meeting business requirements.
- Examine the vendor's policies, procedures, internal controls, and training materials to assess its ability to:
  - recognize and manage changing data security risks;
  - conduct appropriate training and oversight of its employees and any applicable subcontractors;
  - meet the organization's privacy and information security policies; and
  - comply with applicable laws, regulations, and industry standards.
- Review the vendor's security measures to protect personal information including whether it uses encryption.
- Review the vendor's privacy and data security history, including any regulatory enforcement actions, litigation, or prior security incidents, such as data breaches.
- Understand the laws in the vendor's jurisdiction to identify additional risk factors that may impact the integrity, security, and confidentiality of personal information.

Banks should also put in place contractual protections to ensure a similar level of privacy protection to that promised to the bank's customers. Strong contractual terms include requiring the vendor to maintain reasonable security measures to protect customer data including obligations to:

- Protect customer data using anti-virus, firewall, protection, and decontamination tools that are consistent with industry best practices and to maintain and update security measures and back-up processes and procedures consistently with industry best practices.
- Collect, use, and disclose customer data under all applicable privacy laws and only for those purposes as are necessary to discharge, complete, or fulfill the third party's obligations under the contract.
- Perform its obligations under the contract in a manner that allows the bank to comply with its obligations under applicable privacy laws.
- Permit a bank to audit the privacy practices of the service provider to ensure compliance with the contract.
- Promptly provide notice to the bank if it receives a request for access to customer data, receives a complaint in relation to that data, or receives any notice that it has failed to comply with any applicable privacy laws.
- Provide reasonable assistance in:
  - responding to any access, amendment, correction, or similar request about that information;
  - investigating, mitigating, or responding to any complaint relating to the receipt, use, or disclosure of that information; and
  - responding to any requests or instructions issued by a governmental authority relating to that information.
- Destroy all copies of the information in its possession, power, or control promptly on:
  - the bank's request; or
  - the point at which the information is no longer required for the third party to perform its obligations under the contract.

ENFORCEMENT AND PENALTIES

COMMON LAW VIOLATIONS

Banks alleged to have violated a customer's privacy rights under *Tournier* may face private lawsuits for monetary damages or injunctive relief in court. Similar remedies may also be pursued using alternative dispute resolution mechanisms. Class actions are increasingly used in Canada to assert claims against banks and other large businesses concerning violations that are alleged to have affected multiple customers. Banks may also face lawsuits under other common law torts including breach of confidence and invasion of privacy (see, for example, *Jones v. Tsige*, 2012 ONCA 32 (Ontario Court of Appeal awarded CAD10,000 in damages to a man whose former wife, a bank employee, inappropriately accessed personal banking information about her ex-husband's new partner)).

DATA PROTECTION LAW

PIPEDA

Individuals or the OPC can initiate complaints under PIPEDA. After initiation of a complaint, the OPC may investigate and issue a report detailing the OPC's findings and recommendations. The report is non-binding on banks. However, if the bank does not implement the recommendation, the OPC may make an application in Federal Court asking the court to order the implementation of the recommendations. After the OPC issues a report or notifies the affected individual of the discontinuance of the investigation, the affected individuals can apply to the Federal Court for damages.

The Federal Court can order an organization to:

- Correct its practices.
- Publish a corrective notice.
- Pay damages to a complainant, including damages for humiliation.

Any person engaging in the following activities or obstructing the OPC in the investigation of a complaint or audit may also be guilty of an indictable offense and be fined up to CAD100,000 for:

- Violation of the provisions related to the retention of information subject to an access request.
- Retaliating against an employee for:
  - reporting a violation or reasonably suspected violation of PIPEDA to the OPC;
  - refusing to violate PIPEDA; or
  - complying in good faith with the legislative requirements.

02-19

About Stikeman Elliott

Stikeman Elliott is a global leader in Canadian business law and the first call for businesses working in and with Canada. Our offices are located in Montréal, Toronto, Ottawa, Calgary, Vancouver, New York, London and Sydney. We provide clients with the highest quality counsel, strategic advice, and workable solutions. The firm has an exceptional track record in major U.S. and international locations on multijurisdictional matters and ranks as a top firm in our primary practice areas including mergers and acquisitions, securities, business litigation, banking and finance, competition and foreign investment, tax, restructuring, energy, mining, real estate, project development, employment and labour, and pensions.

For more information about Stikeman Elliott, please visit our website at www.stikeman.com.

Contact us

Shawn Smith
sasmith@stikeman.com

Wesley Ng
wng@stikeman.com

Follow us

SE

Subscribe to updates on a variety of legal topics from Stikeman Elliott's Knowledge Hub at stikeman.com/kh

Stikeman Elliott LLP

Montréal Toronto Ottawa Calgary Vancouver New York London Sydney

Stikeman Elliott