Related content

Privacy and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act for customer-facing employees

PIPEDA and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act

March 2012

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires organizations subject to the Act to undertake certain compliance activities, such as client identification and record keeping, activities. As well, certain transactions are required to be reported to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

The Office of the Privacy Commissioner of Canada supports efforts to combat money laundering and terrorist financing.

We advocate that programs or initiatives should be implemented in a manner that is privacy sensitive and consistent with privacy laws. As such, the collection of personal information must be limited to what is required and identified by legislation and regulations, and in addition to that, what is required for an organization's specific business purposes.

Below are some questions and answers related to privacy that may be of interest:

Do organizations have to take privacy laws into account when complying with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*?

What should an organization's policies and procedures explain about their personal information management practices?

Does PIPEDA require an individual's knowledge or consent if a disclosure (report) is made to FINTRAC, as required by section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*?

Is it important to limit the collection of personal information?

Why is limiting the collection of personal information a good thing?

Should an identity document be photocopied when ascertaining an individual's identity?

Should a health card be used to ascertain a customer's identity?

Should a Social Insurance Number be used to ascertain a customer's identity?

What should an organization be aware of if an individual requests information about disclosures made to FINTRAC?

Do organizations have to take privacy laws into account when complying with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*?

Yes!

Organizations subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* that are required to collect, use and disclose personal information to fulfill the requirements under that Act must still comply with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) or substantially similar provincial legislation.

PIPEDA applies to organizations engaged in commercial activities that collect, use or disclose personal information and Schedule 1 of PIPEDA contains ten (10) fair information principles for organizations to follow.

As well, the provinces of British Columbia, Alberta and Quebec have laws that are recognized as substantially similar to PIPEDA.

Related Information:

For additional information, please refer to the Office of the Privacy Commissioner of Canada's fact sheets on Complying with the Personal Information Protection and Electronic Documents Act and Privacy Legislation in Canada.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

What should an organization's policies and procedures explain about their personal information management practices?

According to the *Identifying Purpose* Principle in PIPEDA, the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

As well, the *Openness* Principle states that an organization shall be open about their policies and procedures. Individuals should be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is understandable.

Therefore, an organization's policies and procedures must explain the purposes for which it collects, uses, and discloses personal information, as required for its specific business purpose or as required by law. If an entity is subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the purposes should reflective activities related to that Act.

In PIPEDA case summary 2003-256, the Commissioner recommended that with respect to a bank's *personal deposit application forms*, the organization should ensure that:

1. The collection of the name, address, date of birth and occupation of the account holder are required by law;
2. The presentation of documentary evidence to prove identity is required by law.

For additional information, please refer to the Privacy Commissioner of Canada's fact sheet for PIPEDA Case Summary #2003-256 and the Office of the Privacy Commissioner of Canada's guide for businesses and organizations.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

Does PIPEDA require an individual's knowledge and consent if a disclosure (report) is made to FINTRAC, as required by section 7 of *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*?

No.

While an individual's consent is required for the collection, use or disclosure of their personal information, there are exceptions to the Consent Principle that are relevant with respect to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Exceptions to Consent

Section 7 of PIPEDA sets out the limited circumstances where knowledge or consent is not required.

As stated in s. 7(3)(c.2) of PIPEDA, an organization may disclose personal information to FINTRAC as required by section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (reporting to FINTRAC on a transaction that may be related to the commission or attempted commission of money laundering or terrorist activity financing) without an individual's knowledge or consent.

For more information about consent and exceptions to consent, please see the Office of the Privacy Commissioner of Canada's PIPEDA Self Assessment Tool and guide for businesses and organizations.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

Is it important to limit the collection of personal information?

Yes.

The *Limiting Collection* Principle in PIPEDA states that the collection of personal information shall be limited to that which is necessary to identified purposes.

An organization must limit collection to what is required and identified by legislation and regulations and what is required for its specific business purpose.

An organization must not indiscriminately collect personal information.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires organizations subject to the Act to record information for certain transactions – this can include an individual's name, address, date of birth, phone number and occupation.

As well, organizations may be required to record specific identity document information in the course of ascertaining an individual's identity this includes the type of identity document, document reference number and place of issue. An individual may be required to provide an identity document, such as a birth certificate, a driver's license, or similar type of document.

It is important for an organization to review the information they need to collect to comply with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and limit collection to what is required and identified by legislation and regulations, and in addition to that, what is required for its specific business purpose.

Please refer to question # 5 for information about photocopying identity cards, question #7 for information about health cards and question #8 for information about the Social Insurance Number.

For more information about limiting collection, use or disclosure of personal information please see the Office of the Privacy Commissioner of Canada's PIPEDA Self Assessment Tool and guide for businesses and organizations.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

Why is limiting the collection of personal information a good thing?

Yes!

Not only "over-collecting" personal information, human and financial resources are not spent collecting, storing, and safeguarding nonessential personal information. An organization can reduce operational inefficiencies and minimize its risk by following the *Limiting Collection* Principle.

An organization shall put in place policies and procedures that focus on collecting, using, disclosing or retaining that personal information which is required to fulfill legal or regulatory obligations, and in addition to that, is necessary for its specific business purpose.

For more information about limiting collection, use or disclosure of personal information please see the Office of the Privacy Commissioner of Canada's PIPEDA Self Assessment Tool and guide for businesses and organizations.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

Should an identity document be photocopied when ascertaining an individual's identity?

Organizations may need to collect personal information about individuals to fulfill obligations required by law and for its specific business purpose.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires organizations subject to the Act to ascertain the identity of customers who conduct certain types of transactions. Individuals may be required to provide an identity document, such as a birth certificate, a driver's license, or similar type of document.

If according to law an organization is required to collect and keep a photocopy or copy of an identity document, then an organization must comply.

If an organization is not required by law to collect a photocopy of an identity document, then an organization must consider whether or not retaining a photocopy of an identity document (or a copy in any form) is necessary for its legitimate business purpose, consistent with privacy legislation (PIPEDA or substantially similar legislation) and with the *Limiting Collection* Principle.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* states that in some cases organizations may be required to collect a photocopy or copy of an identity document, invoice or account statement. Some examples include:

- If the person's identity is ascertained from an attestation signed by a commissioner of oaths in Canada or a guarantor in Canada, and such use of the document is not prohibited by the applicable provincial law, a record of the attestation (*Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* s.64(1))
- If a person's identity is ascertained by relying on a photocopy or electronic image of a document provided by the person, that photocopy or electronic image (*Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* s.4.9(3))
- For certain non-face-to-face identification methods where a photocopy of an identity document is needed (*Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* Schedule 7).

An organization must consider what personal information is required and necessary in order to fulfill legal or regulatory obligation(s), and in addition to that for its specific business purpose, and only collect that information.

For more information about limiting collection, use or disclosure of personal information please see the Office of the Privacy Commissioner of Canada's PIPEDA Self Assessment Tool and guide for businesses and organizations

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

Should a health card be used to ascertain a customer's identity?

A health card is a sensitive identity document. As such, the information on health cards should only be collected in limited circumstances - such as when necessary or required by law.

In a number of provinces there is a stand-alone health information law that prescribes limits on the collection of health service cards and numbers. In some cases, there is an outright prohibition against requiring the production of these cards for any purpose unrelated to the provision of health services. In other cases, health services cards can only be used for meeting the ascertaining identity obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* if the production of this document is genuinely voluntary on the part of the individual.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* indicates that an identity can be ascertained by referring to a health card – but only if provincial legislation does not prohibit it (*Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* s.64(1)).

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* does not require a health card be photocopied, except in those circumstances where an organization is required to collect a copy or photocopy or copy of an identity document (Please see Question #6 for information on photocopying identity documents).

Given that health cards contain sensitive personal information and their use for identity purposes may be prohibited or limited in certain jurisdictions other identity documents, if available, should be used first to ascertain a customer's identity.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

Should a Social Insurance Number (SIN) be used to verify a customer's identity?

The Office of the Privacy Commissioner of Canada recommends that the Social Insurance Number (SIN) should not be used as a general identifier and organizations should restrict their collection, use and disclosure of SINs to legislated purposes.

While some private-sector organizations are required by law to request customers' or employees' SINs, the Office of the Privacy Commissioner of Canada remains opposed to the principle of mandatorily requesting the SIN for general purposes of identification.

However, there is no law prohibiting an organization from asking for a customer's SIN, or a customer from supplying the SIN, for purposes other than income reporting. Although the practice is not recommended, an organization may ask for the SIN, and a customer may choose to supply it, for reasonable purposes of identification, provided that the principles of PIPEDA are duly observed.

Some examples of legislated uses of the SIN include:

- Employers are authorized to collect SINs from employees in order to provide them with records of employment and T-4 slips for income tax and Canada Pension Plan (CPP) purposes.
- Organizations such as banks, credit unions, brokers and trust companies are required under the *Income Tax Act* to ask for customers' SINs for tax reporting purposes (e.g., interest earning accounts, RRSPs, etc.).

No private-sector organization is required to request a SIN for purposes other than income reporting. Even for a financial institution, if a customer's account is not of a type that earns interest (e.g., if it is a credit account as opposed to a savings account), there is no legal requirement for the organization to collect the individual's SIN, and no obligation for the individual to supply it.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* does not require an organization to report an individual's Social Insurance Number to FINTRAC.

Furthermore, FINTRAC's Guideline 6 explains that a Social Insurance Number should never be provided to FINTRAC on any type of report.

For more information about the social insurance number, please see the Office of the Privacy Commissioner of Canada's *Best Practices For The Use of Social Insurance Numbers In The Private Sector*.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

What should an organization be aware of if an individual requests information about disclosures made to FINTRAC?

An individual may request to be informed of disclosures made by an organization to FINTRAC, but that does not necessarily mean that the request can be granted.

Although Principle 4.9 of PIPEDA states that upon request an individual shall be informed of the existence, use and disclosure of their personal information and be given access to that information, there are exceptions that apply.

PIPEDA sets out clear procedures when responding to access requests involving personal information that has been disclosed to FINTRAC or other government institutions.

Request About Information Disclosed

Step 1 – Inform FINTRAC

According to section 9(2.1)(a)(i) of PIPEDA, an organization must notify FINTRAC in writing of a request made by an individual to the extent that the request pertains to:

- Where the organization disclosed personal information to FINTRAC without the individual's knowledge or consent on the grounds that the transaction may be related to the commission or attempted commission of money laundering or terrorist activity financing (section 7(3)(c.2) of PIPEDA).

An organization shall not respond to the request until receiving notification from FINTRAC approving or objecting to the access, or 30 days pass since FINTRAC was notified.

Step 2 – Grounds For an Objection from FINTRAC

FINTRAC could object to the organization complying with the request but must indicate the grounds for its objection. FINTRAC may object to the disclosure if it is of the opinion that compliance with the request could reasonably be expected to be injurious to the detection, prevention or deterrence of money laundering or the financing of terrorist activities.

Step 3 – In Case of an Objection

In the case of an objection, section 9(2.4) of PIPEDA indicates that the organization shall:

- Refuse the request;
- ***Notify*** the Privacy Commissioner of Canada, **in writing**, and **without delay**, of the refusal;
- Not provide the requested information relating to the disclosure;
- Not mention that the organization notified FINTRAC or the Privacy Commissioner of Canada; and
- Not mention that FINTRAC objected to the request.

For additional information on access, please refer to the Office of the Privacy Commissioner of Canada's guide for businesses and organizations and section 9 of PIPEDA.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca

Additional Links and Information

Office of the Privacy Commissioner of Canada speeches and submissions regarding the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Privacy Commissioner of Canada's PIPEDA Findings:

PIPEDA Case Summary #2007-389
The importance of explaining the reasons for collecting personal information.

PIPEDA Case Summary #2006-347
Investment dealer needs personal information to comply with securities regulations.

PIPEDA Case Summary #2005-296
Language of consent and monitoring activity challenged.

PIPEDA Case Summary #2003-256
Customer finds bank's collection, use and disclosure of personal information excessive in order to open a personal deposit account, considers bank's purposes vague.

PIPEDA Case Summary #2002-61
Applicant objects to credit check as condition for opening bank account.

PIPEDA Case Summary #2002-48
Bank accused of inappropriately demanding birthdates from account applicants.

PIPEDA Case Summary #2002-93
Individual complains that bank used personal information for purpose other than that for which it was collected.

For reference material about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*'s client identification, record keeping and reporting requirements, please visit FINTRAC's website: http://www.fintrac-canafe.gc.ca