Breach Notification Requirements in PIPEDA, PIPA Alberta, and the Quebec Privacy Act

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
Report to Commissioner	**ss. 10.1(1), (7), and (8)** **(1)** An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a **real risk of significant harm** to an individual. . . . **(7)** For the purpose of this section, **"significant harm"** includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. **(8)** The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include **(a)** the sensitivity of the personal information involved in the breach;	**ss. 34.1(1)-(2)** **(1)** An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a **real risk of significant harm** to an individual as a result of the loss or unauthorized access or disclosure. **(2)** A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.	**s. 3.5** Where a security presents a risk of serious injury to any individual(s), the organization must promptly notify: **(i)** the CAI; **(ii)** all individuals whose personal information is concerned by the incident (unless doing so would hamper a legal investigation into a crime or statutory offence);

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	(b) the probability that the personal information has been, is being or will be misused; and **(c)** any other prescribed factor.		
Time to give notification to Commissioner	**s. 10.1(2)** The report shall contain the prescribed information and shall be made in the prescribed form and manner **as soon as feasible after the organization determines that the breach has occurred.**	**s. 34.1(1)** An organization having personal information under its control must, **without unreasonable delay**, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information …	**s. 3.5** Where a security presents a risk of serious injury to any individual(s), the organization **must promptly notify**: (i) the CAI; . . . (iii) determine whether to notify anyone that could reduce the risk, and if such notification is made: (A) communicates only the personal information necessary for this purpose; and (B) the PIC records the communication of this information **(s.3.5)**
Report requirements	**s. 10.1(2) and ss. 2(1)-(3), PIPEDA Breach Regulation** **10.1(2)** The report shall contain the prescribed information and shall be made	**s. 19, PIPA AB Regulation** A notice provided by an organization to the Commissioner under section 34.1(1) of the Act	**s.3, Confidentiality Incidents Regulation** Notices to the Commission d'accès à l'information that a confidentiality

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred. **PIPEDA Breach Regulation** **2(1)** A report of a breach of security safeguards referred to in subsection 10.1(2) of the Act must be in writing and must contain **(a)** a description of the circumstances of the breach and, if known, the cause; **(b)** the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period; **(c)** a description of the personal information that is the subject of the breach to the extent that the information is known; **(d)** the number of individuals affected by the breach or, if unknown, the approximate number; **(e)** a description of the steps that the organization has taken to reduce the risk of	must be in writing and include the following information: **(a)** a description of the circumstances of the loss or unauthorized access or disclosure; **(b)** the date on which or time period during which the loss or unauthorized access or disclosure occurred; **(c)** a description of the personal information involved in the loss or unauthorized access or disclosure; **(d)** an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure; **(e)** an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure; **(f)** a description of any steps the organization has taken to reduce the risk of harm to individuals;	incident presents a risk of serious injury, given under the second paragraph of section 3.5 of the Act respecting the protection of personal information in the private sector (chapter P- 39.1), must be in writing and must contain: **(1)** the name of the body affected by the confidentiality incident and any Québec business number assigned to such body under the Act respecting the legal publicity of enterprises (chapter P-44.1); **(2)** the name and contact information of the person to be contacted in that body with regard to the incident; **(3)** a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description; **(4)** a brief description of the circumstances of the incident and what caused it, if known;

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	harm to affected individuals that could result from the breach or to mitigate that harm; **(f)** a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection 10.1(3) of the Act; and **(g)** the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach. **New information** **2(2)** An organization may submit to the Commissioner any new information referred to in subsection (1) that the organization becomes aware of after having made the report. **Means of communication** **2(3)** The report may be sent to the Commissioner by any secure means of communication.	**(g)** a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure; **(h)** the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.	**(5)** the date or time period when the incident occurred or, if that is not known, the approximate time period; **(6)** the date or time period when the body became aware of the incident; **(7)** the number of persons concerned by the incident and the number of those who reside in Québec or, if that is not known, the approximate numbers; **(8)** a description of the elements that led the body to conclude that there is a risk of serious injury to the persons concerned, such as the sensitivity of the personal information concerned, any possible ill-intentioned uses of such information, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes; **(9)** the measures the body has taken or intends to take to notify the persons whose personal information is concerned by the incident, pursuant to the second paragraph of section 3.5 of the Act respecting the protection of

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
			personal information in the private sector, and the date on which such persons were notified, or the expected time limit for the notification; **(10)** the measures the body has taken or intends to take after the incident occurred, including those aimed at reducing the risk of injury or mitigating any such injury and those aimed at preventing new incidents of the same nature, and the date or time period on which the measures were taken or the expected time limit for taking the measures; and **(11)** if applicable, an indication that a person or body outside Québec that exercises similar functions to those of the Commission d'accès à l'information with respect to overseeing the protection of personal information has been notified of the incident. The organization may use the Notification Form available on the CAI website.

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
Notification to individual	**s. 10.1(3)** Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.	**s. 37.1** **(1)** Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure **(a)** in a form and manner prescribed by the regulations, and **(b)** within a time period determined by the Commissioner. **(2)** If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).	**s. 3.5** Where a security presents a risk of serious injury to any individual(s), the organization must promptly notify: (i) the CAI; (ii) all individuals whose personal information is concerned by the incident (unless doing so would hamper a legal investigation into a crime or statutory offence);

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
		(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate. **(4)** The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization **(a)** to notify individuals under subsection (1), or **(b)** to satisfy terms and conditions under subsection (2). **(5)** An organization must comply with a requirement **(a)** to provide additional information under subsection (4),	

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
		(b) to notify individuals under subsection (1), or **(c)** to satisfy terms and conditions under subsection (2). **(6)** The Commissioner has exclusive jurisdiction to require an organization **(a)** to provide additional information under subsection (4), **(b)** to notify individuals under subsection (1), or **(c)** to satisfy terms or conditions under subsection (2). **(7)** Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.	
Time to give notification to individuals	**s. 10.1(6)**	**s. 37.1(1)**	**s. 3.5**

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	The notification shall be given **as soon as feasible** after the organization determines that the breach has occurred. (Note that the same standard is used in **s. 10.2(2)** regarding notification to organizations)	Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure (b) **within a time period determined by the Commissioner.**	Where a security presents a risk of serious injury to any individual(s), the organization **must promptly notify**: (i) the CAI; **(ii) all individuals whose personal information is concerned by the incident (unless doing so would hamper a legal investigation into a crime or statutory offence);**
Contents of notification to affected individual	**s. 10.1(4) and s. 3, PIPEDA Breach Regulation** **10.1(4)** The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information. **PIPEDA Breach Regulation**	**s. 19.1, PIPA AB Regulation** **(1)** Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must **(a)** be given directly to the individual, and **(b)** include	**s.5, Confidentiality Incidents Regulation** Notices to persons whose personal information is concerned by a confidentiality incident presenting a risk of serious injury, given under the second paragraph of section 3.5 of the Act respecting the protection of personal information in the private sector (chapter P-39.1), must contain **(1)** a description of the personal information covered by the incident or, if that information is not known,

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	3 A notification provided by an organization, in accordance with subsection 10.1(3) of the Act, to an affected individual with respect to a breach of security safeguards must contain **(a)** a description of the circumstances of the breach; **(b)** the day on which, or period during which, the breach occurred or, if neither is known, the approximate period; **(c)** a description of the personal information that is the subject of the breach to the extent that the information is known; **(d)** a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach; **(e)** a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and **(f)** contact information that the affected individual can use to obtain further information about the breach.	(i) a description of the circumstances of the loss or unauthorized access or disclosure, (ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred, (iii) a description of the personal information involved in the loss or unauthorized access or disclosure, (iv) a description of any steps the organization has taken to reduce the risk of harm, and (v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure. **(2)** Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the	the reasons why it is impossible to provide such a description; **(2)** a brief description of the circumstances of the incident; **(3)** the date or time period when the incident occurred or, if that is not known, the approximate time period; **(4)** a brief description of the measures the body has taken or intends to take after the incident occurred in order to reduce the risks of injury; **(5)** the measures that the body suggests the person concerned take in order to reduce the risk of injury or mitigate any such injury; and **(6)** the contact information where the person concerned may obtain more information about the incident.

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
		Commissioner determines that direct notification would be unreasonable in the circumstances.	
Form and Manner	**s. 10.1(5) and ss. 4, 5(1)-(2), PIPEDA Breach Regulation** **10.1(5)** The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner. **PIPEDA Breach Regulation** **Direct notification — form and manner** **4** For the purposes of subsection 10.1(5) of the Act, direct notification must be given to the affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances.	**s. 19.1, PIPA AB Regulation** **(1)** Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must **(a)** be given directly to the individual, and **(b)** include (i) a description of the circumstances of the loss or unauthorized access or disclosure, (ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred, (iii) a description of the personal	**s. 6, Confidentiality Incidents Regulation** The notices referred to in section 5 are sent to the persons concerned by the confidentiality incident. Despite the first paragraph, the notices referred to in section 5 are given by way of a public notice in any of the following circumstances: **(1)** when the fact of sending such notice is likely to cause increased injury to the person concerned; **(2)** when the fact of sending such notice is likely to cause undue hardship for the body; **(3)** when the body does not have the contact information for the person concerned. The notices referred to in section 5 may also be given by way of a public

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	Indirect notification — circumstances **5(1)** For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by an organization in any of the following circumstances: **(a)** direct notification would be likely to cause further harm to the affected individual; **(b)** direct notification would be likely to cause undue hardship for the organization; or **(c)** the organization does not have contact information for the affected individual. **Indirect notification — form and manner** **5(2)** For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.	information involved in the loss or unauthorized access or disclosure, (iv) a description of any steps the organization has taken to reduce the risk of harm, and (v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure. **(2)** Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.	notice if there is a need to act rapidly to reduce the risk of a serious injury or to mitigate any such injury. In such cases, the body must still send a notice to the person concerned with proper diligence, unless one of the circumstances listed in the second paragraph applies. Pursuant to this section, public notices may be made by any method that could be reasonably expected to reach the person concerned.
Notification to organizations	**s. 10.2(1)**	**N/A**	**N/A**

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	An organization that notifies an individual of a breach of security safeguards under subsection 10.1(3) shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.		
Time to give notification to organizations	**s. 10.2(2)** The notification shall be given as soon as feasible after the organization determines that the breach has occurred.	**N/A**	**N/A**
Disclosure of personal information without consent	**s. 10.2(3)-(4)** **(3)** In addition to the circumstances set out in subsection 7(3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if **(a)** the disclosure is made **to the other organization, the government institution**	**N/A**	**s. 18** A person carrying on an enterprise may, without the consent of the person concerned, communicate personal information he holds on that person **(1)** to his attorney; **(2)** to the Director of Criminal and Penal Prosecutions if the information

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	or the part of a government institution that was notified of the breach under subsection (1); and **(b)** the disclosure is made solely for the purposes of **reducing the risk of harm** to the individual that could result from the breach or mitigating the harm. **(4)** Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in the circumstance set out in subsection (3).		is required for the purposes of the prosecution of an offence under an Act applicable in Québec; **(3)** to a person or body responsible, by law, for the prevention, detection or repression of crime or statutory offences who requires it in the performance of his duties, if the information is needed for the prosecution of an offence under an Act applicable in Québec; **(4)** to a person to whom it is necessary to communicate the information under an Act applicable in Québec or under a collective agreement; **(5)** to a public body within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1) which, through a representative, collects such information in the exercise of its functions or the implementation of a program under its management;

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
			(6) to a person or body having the power to compel communication of the information if he or it requires it in the exercise of his or its duties or functions; **(7)** to a person to whom the information must be communicated by reason of the urgency of a situation that threatens the life, health or safety of the person concerned; **(7.1)** to a person or body in accordance with sections 18.1, 18.2, 18.3 and 18.4; **(8)** to a person who may use the information for study, research or statistical purposes in accordance with section 21 or a person authorized pursuant to section 21.1; **(9)** to a person who is authorized by law to recover debts on behalf of others and who requires it for that purpose in the performance of his duties;

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
			(9.1) to a person if the information is needed for the recovery of a claim of the enterprise; A person carrying on an enterprise must make an entry of every communication made under subparagraphs 6 to 9.1 of the first paragraph. The persons referred to in subparagraphs 1, 9 and 9.1 of the first paragraph who receive communication of information may communicate the information to the extent that such communication is necessary, in the performance of their duties, to achieve the purposes for which they received communication of the information. The holder of a security guard agency licence or investigation agency licence issued under the Private Security Act (chapter S-3.5) or a body having as its object the prevention, detection or repression of crime or statutory offences and a person carrying on an enterprise may, without the consent of the person

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
			concerned, communicate among themselves the information needed for conducting an inquiry for the purpose of preventing, detecting or repressing a crime or a statutory offence. The same applies in respect of information communicated among persons carrying on an enterprise, if the person who communicates or collects such information has reasonable grounds to believe that the person concerned has committed, or is about to commit, a crime or statutory offence against one or other of the persons carrying on an enterprise.
Record-keeping	**s. 10.3(1)-(2) and s. 6, PIPEDA Breach Regulation** **10.3(1)** An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control. **10.3(2)** An organization shall, on request, provide the Commissioner with access to, or a copy of, a record.	**N/A**	**s. 3.8 and ss. 7-8, Confidentiality Incidents Regulation** **3.8** A person carrying on an enterprise must keep a register of confidentiality incidents. A government regulation may determine the content of the register. A copy of the register must be sent to the Commission at its request.

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
	PIPEDA Breach Regulation **Record-keeping requirements** **6(1)** For the purposes of subsection 10.3(1) of the Act, an organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred. **Compliance** **6(2)** The record referred to in subsection 10.3(1) of the Act must contain any information that enables the Commissioner to verify compliance with subsections 10.1(1) and (3) of the Act.		**Confidentiality Incidents Regulation** **7** The registers provided for in section 3.8 of the Act respecting the protection of personal information in the private sector (chapter P-39.1) must contain **(1)** a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description; **(2)** a brief description of the circumstances of the incident; **(3)** the date or time period when the incident occurred or, if that is not known, the approximate time period; **(4)** the date or time period when the body became aware of the incident; **(5)** the number of persons concerned by the incident or, if that is not known, the approximate number;

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
			(6) a description of the elements that led the body to conclude whether or not there is a risk of serious injury to the persons concerned, such as the sensitivity of the personal information concerned, any possible ill-intentioned uses of such information, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes; **(7)** if the incident presents a risk of serious injury, the transmission dates of the notices to **the Commission d'accès à l'information** and the persons concerned, pursuant to the second paragraph of section 3.5 of the Act respecting the protection of personal information in the private sector, as well as an indication of whether the body issued public notices and, if applicable, its reasons for doing so; and **(8)** a brief description of the measures the body has taken after the incident occurred in order to reduce the risks of injury.

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
			8 The information in the registers must be kept up to date and kept for at least 5 years after the date or time period when the body became aware of the incident.
Penalties for non-compliance	**s. 28** Every organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or 27.1(1) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of **(a)** an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or **(b)** an indictable offence and liable to a fine not exceeding $100,000.	**s. 59(1)(e.1), (2)-(4)** **(1)** Subject to subsections (3) and (4), a person commits an offence if the person **(e.1)** fails to provide notice to the Commissioner under section 34.1; **(2)** A person who commits an offence under subsection (1) is liable, **(a)** in the case of an individual, to a fine of not more than $10 000, and **(b)**in the case of a person other than an individual, to a fine of not more than $100 000. **(3)** No person is liable to prosecution for an offence against this or any other Act by reason only of complying with a requirement of the Commissioner under this Act.	**ss. 90.1, 90.12 and 91 (1)-(2)** **90.1** A monetary administrative penalty may be imposed by a person designated by the Commission, but who is not a member of any of its divisions, on anyone who (1) does not inform the persons concerned in accordance with sections 7 and 8; (2) collects, uses, communicates, keeps or destroys personal information in contravention of the law; (3) does not report, where required to do so, a confidentiality incident to the Commission or to the persons concerned;

	PIPEDA	PIPA Alberta	Quebec Private Sector Privacy Act
		(4) Neither an organization nor an individual is guilty of an offence under this Act if it is established to the satisfaction of the court that the organization or individual, as the case may be, acted reasonably in the circumstances that gave rise to the offence.	**90.12** The maximum amount of the monetary administrative penalty is $50,000 in the case of a natural person and, in all other cases, $10,000,000 or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year. **91** Anyone who **(1)** collects, uses, communicates, keeps or destroys personal information in contravention of the law, **(2)** fails to report, where required to do so, a confidentiality incident to the Commission or to the persons concerned, commits an offence and is liable to a fine of $5,000 to $100,000 in the case of a natural person and, in all other cases, of $15,000 to $25,000,000 or, if greater, the amount corresponding

	PIPEDA	**PIPA Alberta**	**Quebec Private Sector Privacy Act**
			to 4% of worldwide turnover for the preceding fiscal year.