



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	McNeill, Lalonde & Associates (Organization)
Decision number (file number)	P2019-ND-204 (File #012224)
Date notice received by OIPC	February 28, 2019
Date Organization last provided information	July 22, 2019
Date of decision	December 18, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The Organization reported “It is unclear at this stage precisely what information was involved in this incident. The individual had access to the following personal information of past and present employees: (i) names; (ii) dates of birth; (iii) social insurance numbers; (iv) home addresses; and (v) direct deposit information. The individual also had access to the names and dates of birth of spouses and dependants enrolled in the Company's employee group benefits plan”.</p> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On February 25, 2019, the Organization learned that an employee had been charged with fraud.• The Organization reported is “...concerned that the [employee] improperly collected, used and/or disclosed certain personal information that in the course of her employment”.

	<ul style="list-style-type: none"> The Organization reported it does not know if any personal information of three Alberta-based employees was compromised, but it has evidence that a Vancouver-based employee’s personal information was compromised.
Affected individuals	The incident affected 100 individuals, including 3 from Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Engaged external legal counsel and investigated to determine the scope of the individual’s wrong-doing. Advised local police service. Terminated the employee. Advised affected individuals to flag bank, credit, phone, utility and postal accounts. Advised individuals of the availability of credit insurance services paid for by the Organization. Notified data protection regulators. Strengthening background check processes. Providing training and instruction to employees about the dangers associated with identity theft and cybersecurity incidents. Reviewing systems to determine whether it can implement further safeguards to lessen the risk of such an incident in the future.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on February 27, 2019.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be “significant.” It must be important, meaningful, and with non-trivial consequences or effects.</p>	<p>The Organization reported that “The primary risks that could result from this incident are those related to fraud, financial loss and identity theft.”</p> <p>I agree with the Organization’s assessment. A reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of fraud, financial loss and identity theft.</p>
<p>Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.</p>	<p>The Organization reported that “It is currently of the view that there is a fair likelihood that harm will result from the individual’s actions in these circumstances given her criminal actions and history.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a rogue employee. The employee had access to the information for approximately four (4) months. The</p>

	Organization reported that personal information of a Vancouver-based employee was compromised.
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.</p> <p>A reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of fraud, financial loss and identity theft. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a rogue employee. The employee had access to the information for approximately four (4) months. The Organization reported that personal information of a Vancouver-based employee was compromised.</p> <p>I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified the affected individuals by email dated February 27, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner