



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Emery Jamieson LLP
Decision number (file number)	P2014-ND-13 (File #P2859)
Date notice received by OIPC	August 29, 2014
Date Organization last provided information	November 12, 2014
Date of decision	November 28, 2014
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The organization is required to notify those individuals 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 incorporated in Alberta. I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	The incident involved all or some of the following information about the individuals: <ul style="list-style-type: none">• name;• address;• partial Social Insurance Number;• partial birthdate;• partial bank account number;• salary and deductions;• start date; and• status within organization. This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected in Alberta.

DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none"> • Some time between August 25-28, 2014, the employee payroll register containing detailed employee information was lost or misplaced. • The employee payroll register was left outside the locked cabinet where it is stored during the payroll processing period.
Affected individuals	<ul style="list-style-type: none"> • 68 employees
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Reported to the Edmonton Police Service. • Alerted payroll provider of loss in case any attempts were made to contact them.
Steps taken to notify individuals of the incident	<ul style="list-style-type: none"> • Affected employees were notified by email on September 2, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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>The Organization recognized the affected individuals may be at risk for identity theft and fraud.</p> <p>In my view, the personal information involved is sensitive. It contains partial Social Insurance Numbers, partial bank account numbers, partial dates of birth and salary information. The types of harm that could result from the loss of personal information in this instance are identity theft and fraud. In my view, these are significant harms.</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>The Organization reported that given the limited nature of key information on the payroll register, it considered there not to be a real risk of significant harm to the affected individuals.</p> <p>In my view, despite the fact that some of the lost information was only partial numbers, collectively, enough information was lost that there is a real risk that an individual who obtained this information could use it to the detriment of the affected individuals in terms of identity theft or fraudulent activity. The likelihood of harm resulting from this incident is increased because the personal information was lost and has not been recovered.</p>
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. The personal information involves sensitive identity information, such as partial Social Insurance</p>	

Numbers, partial bank account numbers, partial dates of birth and salary information for all affected individuals. Collectively, enough information was lost that an individual who obtained this information could use it to the detriment of the affected individual. The information has been lost and has not been recovered. These factors contributed significantly to my decision.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the plan members in an email dated, September 2, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Elizabeth Denham
Information and Privacy Commissioner for British Columbia