



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Columbian Mutual Life Insurance Company (Organization)
Decision number (file number)	P2016-ND-05 (File #000771)
Date notice received by OIPC	April 30, 2015
Date Organization last provided information	May 5, 2015
Date of decision	February 9, 2016
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 incident involved the following information:</p> <ul style="list-style-type: none">• name,• address,• bank account information, and• Social Insurance Number (SIN). <p>This information is about an identifiable individual and qualifies as “personal information” as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	

Description of incident	An unencrypted flash drive containing personal information of the Organization’s policy holders and their beneficiaries was lost during surface mail transmission.
Affected individuals	One individual in Alberta was affected.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • An investigation into the incident was conducted. • One year free identity protection, restoration and monitoring services were offered to the affected individual. • The Organization ceased transmitting personal information using flash drives. • The Organization has taken steps to review its procedures about the security and confidentiality of personal information.
Steps taken to notify individuals of the incident	The individual was notified by mail on April 17, 2015.
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 recognized that the affected individual may be at risk of identity theft and fraud.</p> <p>I agree with the Organization. The personal information involved includes sensitive identity and financial information, including Social Insurance Number. This information could be used to cause identity theft and fraud. These are significant harms.</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 the flash drive containing the personal information at issue was not encrypted, but was in a format that would make it difficult to access. Further, the Organization reported that it did not appear that the flash drive was stolen, but rather the package was damaged in transit the flash drive was lost.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the missing flash drive containing personal information was not encrypted and has not been recovered. Although the Organization believes it is possible the flash drive was lost, it cannot confirm there was no malicious intent involved.</p>

DECISION UNDER SECTION 37.1(1) OF PIPA

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 individual. The personal information involved includes sensitive identity and financial information, which could be used to cause the significant harms of identity theft and fraud. The missing flash drive was not encrypted and has not been recovered. The Organization cannot confirm there was no malicious intent involved.

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

I understand the Organization notified the affected individual in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner