



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	PSFL Investments Canada Ltd. (Primerica) (the Organization)
Decision number (file number)	P2014-ND-14 (File #P2691)
Date notice received by OIPC	May 23, 2014
Date Organization last provided information	October 8, 2014
Date of decision	November 10, 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 Mississauga, Ontario. I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA, and the personal information was collected in Alberta.
Section 1(1)(k) of PIPA “personal information”	The incident involved all or some of the following information: <ul style="list-style-type: none">• name,• date of birth,• mailing address,• email address,• telephone number,• social insurance number,• policy numbers and details,• account numbers and details,• banking information,• client identification information,• disclosed medical information,

	<ul style="list-style-type: none"> • where applicable any information relating to the above provided to the Organization related to insured spouse or child rider, • where applicable any information relating to the above provided to the Organization, relating to another person such as in the case of an in trust for account, power of attorney or spousal contribution. <p>The information listed above is “personal information” as defined in section 1(1) (k) of PIPA.</p>
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"> • On or around April 12, 2014, one of the Organization’s agents experienced a break-in to his locked car. Some of the agent’s personal belongings and his laptop were stolen from the car. The information at issue was stored on the laptop. The laptop was password protected but not encrypted. • The agent discovered the loss of the laptop when he returned to his car. • Calgary Police Service was notified of the theft on April 13, 2014. • The laptop has not been recovered to date.
Affected individuals	195 clients of the Organization, who are residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Alerts placed on client accounts and account numbers of affected clients have been changed. • Fraud alerts placed on client accounts with Equifax and TransUnion Canada. • Enhanced monitoring of client accounts. • Fund companies have been notified of the breach. • Clients given the option to add a password to their accounts as an enhanced security measure.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on May 14, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the affected individuals as a	The Organization recognized that the types of harm that could result from the breach include identity theft, fraud and harm to reputation.

<p>result of the incident. The harm must also be “significant.” It must be important, meaningful, and with non-trivial consequences or effects.</p>	<p>In my view, the personal information involved in this case is highly sensitive. It includes include names, social insurance numbers, birthdates, addresses, and bank account information.</p> <p>This information could be used to cause harm such as 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 there is a real possibility the information may be used for fraud and identity theft.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the laptop was stolen and not encrypted. The laptop has not been recovered. To date, the Organization can not determine whether the personal information on the laptop has been accessed.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<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 involved includes name, date of birth, social insurance number, and financial information. The information was stored on a laptop that was stolen and not encrypted. The laptop has not been recovered. These factors contributed significantly to my decision.</p> <p>I require the Organization to notify the affected individuals 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 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner