



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Equifax Canada Co. (Organization)
Decision number (file number)	P2014-ND-50 (File P2494)
Date notice received by OIPC	October 29, 2013
Date Organization last provided information	October 29, 2013
Date of decision	January 15, 2014
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The organization is required to notify that 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 incorporated in Nova Scotia and registered in Alberta as an extra-provincial corporation. 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”	Credit report information comprising: <ul style="list-style-type: none">• Name• Home address• Social Insurance Number• Account numbers• Creditor names and payment history for credit accounts in individual’s name
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p>Description of incident</p>	<p>In August, 2013 an unknown party accessed the Equifax website and purchased copies of credit reports using stolen credit card numbers. Equifax discovered this incident in September 2013 after it was informed that certain credit report inquiries had been purchased with stolen credit cards.</p> <p>Equifax requires that individuals wishing to obtain a credit report via the website provide some personal information to authenticate their identity. In this case, the unknown party provided the required information and then purchased credit reports for the affected individuals using stolen credit card numbers.</p> <p>The Organization concluded that the affected individuals were victims of identity theft.</p>
<p>Affected individuals</p>	<ul style="list-style-type: none"> • 119 affected individuals in Canada. • 1 affected individual in Alberta.
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • The Organization conducted a verification of its online systems and authentication process and confirmed that these systems and processes were not the cause of the breach. • The Organization contacted the affected individuals and informed them they had been victims of identity theft. • The Organization placed a fraud alert message on the affected individuals' credit files and informed them of steps they could take to protect their accounts and their identity. • The Organization informed law enforcement of the incident.
<p>Steps taken to notify individuals of the incident</p>	<p>Notification sent by mail to affected individuals on October 28, 2013.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<p>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>	<p>In my view, the personal information involved is highly sensitive. It contains identity information such as home address, social insurance numbers, account numbers, and credit histories.</p> <p>The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. In my view, 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 affected individuals had likely been victims of identity theft as the unauthorized party that gained access to the credit reports already had in hand detailed identity and financial and information that they used to gain access to the credit reports. Further, the credit reports were purchased using stolen credit cards, indicating fraudulent activity.</p> <p>In my view, the likelihood of harm resulting from this incident is high because the personal information was obtained through fraudulent means and the incident appears to be directly connected to identity theft.</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 involves sensitive identity information, such as social insurance numbers, account numbers and credit histories. The personal information was obtained through fraudulent means and directly connects to identity theft. These factors contributed significantly to my decision.</p> <p>I require the Organization to notify the affected individual 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 customers in a letter dated October 28, 2013, in accordance with the Regulation.</p>	

Jill Clayton
Information and Privacy Commissioner