



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Well.ca (Organization)
Decision number (file number)	P2015-ND-45 (Case File #P2588)
Date notice received by OIPC	February 25, 2014
Date Organization last provided information	March 22, 2014
Date of decision	May 19, 2015
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”	I have jurisdiction because the Organization is an “organization” as defined in section 1(1)(i)(i).
Section 1(1)(k) of PIPA “personal information”	The incident involved the following information: <ul style="list-style-type: none">• name,• billing address,• credit card number,• credit care expiry date,• card verification value (CVV) code. <p>This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected in Alberta.</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">• The Organization reported that “one of its third party service providers was illegally compromised between December 22, 2013 and January 7, 2014”.

	<ul style="list-style-type: none"> • The Organization investigated the incident and found that customer personal and financial information was accessed in an unauthorized manner.
Affected individuals	A total of 3,891 individuals were affected; 689 affected individual are residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • The incident was reported to law enforcement; • Relevant credit card providers and payment processors were notified; • An email contact address and toll-free line were established to address questions or concerns regarding the incident; • Customers were advised to obtain copies of their credit report from Equifax and TransUnion and review them; • Customers were advised to place a free fraud alert on their credit reports.
Steps taken to notify individuals of the incident	The Organization was unable to identify the specific customers affected by the incident. As a result, the Organization directly notified all customers with transactions during the relevant time period.
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 the affected individuals may be at risk for financial harm.</p> <p>I agree with the Organization. The personal information involved includes sensitive financial information that could be used to cause the harms of 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 there may be a risk of financial harm resulting to the affected individuals.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was “illegally compromised” indicating the incident was the result of malicious intent.</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 affected individuals. The personal information involved includes sensitive financial information that could be used to cause the significant harms of identity theft and fraud. The personal information was “illegally compromised” indicating the incident was the result of malicious intent. 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 individuals affected by the incident in accordance with section 19.1 of the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner