



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Function Point Productivity Software (Organization)
Decision number (file number)	P2016-ND-12 (File #000174)
Date notice received by OIPC	January 12, 2015
Date Organization last provided information	January 28, 2016
Date of decision	March 15, 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)(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,• email address,• credit card number,• credit card expiration date, and• credit card verification 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	

<p>Description of incident</p>	<ul style="list-style-type: none"> • An employee’s email account was accessed by an unauthorized individual between November 4 and 12, 2014, inclusive. • The email account contained customers’ completed credit card authorization forms.
<p>Affected individuals</p>	<p>One individual from Alberta was affected.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • The email account was isolated and the employee’s password was changed. • An investigation into the incident was initiated. • The Organization reviewed and updated its practices, procedures and systems controls. • One year free credit monitoring was offered to the affected individual.
<p>Steps taken to notify individuals of the incident</p>	<p>The customer was initially notified of the incident via email on November 13, 2015. The Organization mailed a notification letter to the affected individual after the investigation into the incident was completed.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<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 did not specifically identify any significant harms that might result from this incident; however, in its notification to affected individuals, the Organization referenced identity theft and fraud.</p> <p>In my view, the personal information involved is sensitive financial information that could be used to cause the harms of 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 low likelihood that harm could result from this incident given the data involved.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessible to an unauthorized individual with 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 the affected individual. The personal information involved sensitive financial information that could be used to cause the significant harms of identity theft and fraud. The information was accessible to an unauthorized individual with malicious intent.

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 has 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