



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Fareportal Inc. (Organization)
Decision number (file number)	P2018-ND-052 (File #008487)
Date notice received by OIPC	April 26, 2018
Date Organization last provided information	April 26, 2018
Date of decision	May 7, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the affected individual in Alberta 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 following information was involved in this incident, in various combinations:</p> <ul style="list-style-type: none">• name,• billing address,• billing telephone number,• email address, and• credit card number. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected via the Organization’s website.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	

<p>Description of incident</p>	<ul style="list-style-type: none"> On or about March 17, 2018, through security monitoring systems, the Organization discovered that between approximately January 1, 2018 and March 20, 2018, a now-former employee located in India was involved in diverting airline booking commissions from cheapoair.com, a branded website of the Organization. The ex-employee uploaded booking data (including personal data) from the Organization’s system into the accounts of certain web portals, such as a job board, which were potentially accessible by actors outside the company. The booking data was accessed and, in some instances, used to impersonate CheapOair agents and divert booking commissions to another travel agency.
<p>Affected individuals</p>	<p>The Organization estimated the incident affected approximately 5 individuals, including one (1) resident of Alberta.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> The relevant employee is no longer employed by the Organization. Notified law enforcement. Implemented additional security measures. Providing enhanced training to all contact center employees to prevent any recurrence of such incidents.
<p>Steps taken to notify individuals of the incident</p>	<p>The affected individual in Alberta was notified by letter sent April 25, 2018.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<p>Harm Some damage or detriment or injury that could be caused to the 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 reported the information could potentially be used to cause the harms of “Financial loss, fraud, identity theft, and negative effects on a credit record”.</p> <p>I agree with the Organization’s assessment. The contact and financial information could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on a credit record. Email addresses could be used to cause the significant harm of phishing.</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 credit card information could have been used by actors outside the company to impersonate CheapOair agents in order to divert the booking and related commission to a different travel agency, or other purposes”.</p> <p>In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (rogue employee, deliberate disclosure of personal information).</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 individuals as a result of this incident. The contact and financial information could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on a credit record. Email addresses could be used to cause the significant harm of phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (rogue employee, deliberate disclosure of personal information).

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the affected individual in Alberta was notified by letter sent April 25, 2018. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner