Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Fareportal, Inc. (Organization)
Decision number (file number)	P2017-ND-128 (File #006290)
Date notice received by OIPC	August 21, 2017
Date Organization last provided information	September 7, 2017
Date of decision	September 7, 2017
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 individual in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (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"	The incident involved the following information: • credit card number, • expiry date, and • security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about July 21, 2017, a now-former employee of the Organization emailed customers' personal information from the Organization to his personal email address. • Some of the information was used to generate 15 single use cards (all of which were cancelled by the Organization).

	• The incident was discovered on July 25, 2017, when the ex-employee was found to have visited the call center after hours and used the computers, all without permission. As a result, the ex-employee's network and other activity was reviewed and the breach discovered.
Affected individuals	The incident affected three individuals, including one resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Restricted keycard and office access for non-essential personnel. • Revoked access to Transaction Management System (TMS) from all non-permanent employees. • Policy to revoke access to TMS, e-mail and office for any employee who does not follow attendance protocols. • Restrict access by agents during and after office hours. • The relevant employee is no longer employed by the Organization.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and mail on August 16, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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.	The Organization reported the following harms that might result from this incident: "Financial loss, fraud, identity theft, and negative effects on a credit record." I agree with the Organization. The financial information at issue could be used to cause the harms of identity theft, fraud, financial loss and negative effects on a credit record. These are significant harms.
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.	The Organization reported that "The credit card information could have been used again by the ex-employee, or forwarded to other unknown individuals. There is evidence of malicious intent because the ex-employee used the personal information to generate 15 single use cards which were cancelled. The credit card information has not been recovered because the ex-employee has left the state and his whereabouts are currently unknown." In my view, the likelihood of significant harm in this case is increased because the incident was the result of malicious intent (deliberate action and use of information for fraudulent purposes). The information has not been recovered.

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. The financial information at issue could be used to cause the harms of identity theft, fraud, financial loss and negative effects on a credit record. These are significant harms. The likelihood of significant harm in this case is increased because the incident was the result of malicious intent (deliberate action and use of information for fraudulent purposes). The information has not been recovered. 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 affected individuals were notified by email and mail on August 16, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner