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	Feld Entertainment, Inc. (Organization)
Decision number (file number)	P2018-ND-120 (File #009426)
Date notice received by OIPC	August 13, 2018
Date Organization last provided information	August 13, 2018
Date of decision	September 4, 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 individual whose information was collected 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: • name, • address, • wage/payroll/tax information, • bank account/routing information, and • for some individuals, passport numbers. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Beginning on or about May 28, 2018, the Organization identified suspicious email activity related to a phishing email sent to certain of the Organization's employees.

	• The Organization investigated, and, on June 21, 2018, determined that there had been unauthorized access to certain of the Organization's employee email accounts. • The Organization later confirmed that unauthorized access occurred between April 5, 2018 and June 29, 2018. • To date, the Organization has no evidence of any actual or attempted misuse of the personal information within the affected email accounts.
Affected individuals	The incidents affected one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Working to enhance security measures through implementation of multi-factor authentication. • Provided affected individuals with information about the event and about the steps they can take to better protect against misuse of their personal information. • Offered affected individuals complimentary access to 24 months of credit monitoring and identity theft restoration services. • Reported the incident to other state regulators, where required by law.
Steps taken to notify individuals of the incident	Beginning on August 6, 2018, the Organization provided written notice to all affected individuals, including one (1) Alberta resident.
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 did not specifically identify any harm(s) that might result from this incident. However, the Organization's notice to affected individuals said "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity." In my view, the comprehensive employment, financial and, in some cases, identity information at issue, could be used to cause the significant harms of identity theft and fraud.
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 did not specifically assess the likelihood of harm resulting from this incident but reported that to date it has "no evidence of any actual or attempted misuse of the personal information within the affected email accounts". In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious activity (phishing email) and the information was exposed over almost three months. The lack of reported misuse to date does not mean such activities will not occur in the future.

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 comprehensive employment, financial and, in some cases, identity information at issue, could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious activity (phishing email) and the information was exposed over almost three months. The lack of reported misuse to date does not mean such activities will not occur in the future. I require the Organization to notify the affected individual whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that beginning on August 6, 2018, the Organization provided written notice to all affected individuals, including one (1) Alberta resident. The Organization is not required to notify the individual in Alberta again.

Jill Clayton
Information and Privacy Commissioner