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)	P2020-ND-004 (File #013699)
Date notice received by OIPC	September 20, 2019
Date Organization last provided information	September 20, 2019
Date of decision	February 11, 2020
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 individuals whose personal 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • name, • date of birth, • passport number, • medical and health insurance information, • government issued number, • Social Security number, and • username and password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization learned of suspicious activity involving certain employee email accounts related to a phishing scam. • The Organization's investigation confirmed unauthorized access to certain employee accounts on separate occasions between November 14, 2018 and January 25, 2019. • The Organization has no evidence of any actual or attempted misuse of the personal information within the affected email accounts.
Affected individuals	The incident affected 17 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated, reset passwords, assessed security. • Working to implement additional safeguards and training to its employees, including multi-factor authentication.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on September 5, 2019.
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 the types of harm that might result from this incident, but reported that it was "…providing access to fraud consultation and identity restoration services … [and] guidance on how to better protect against identity theft and fraud". In my view, a reasonable person would consider that the identity and health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Credentials could be used to compromise other online accounts. These are all 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 did not specifically assess the likelihood of harm resulting from this incident, but noted that it "…is not aware of any attempted or actual misuse of personal information". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action) and occurred on separate occasions across 2 ½ months. The lack of reported misuse of the information to date does not mitigate the potential harm from identity theft or other forms of fraud, which can occur months or even years after a breach.
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.	

A reasonable person would consider that the identity and health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Credentials could be used to compromise other online accounts. These are all significant harms.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action) and occurred on separate occasions across 2 ½ months. The lack of reported misuse of the information to date does not mitigate the potential harm from identity theft or other forms of fraud, which can occur months or even years after a breach.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand individuals were notified in writing on September 5, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner