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	Cowboys Casino (Organization)
Decision number (file number)	P2016-ND-60 (File #003046)
Date notice received by OIPC	June 9, 2016
Date Organization last provided information	July 5, 2016
Date of decision	September 2, 2016
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	I have jurisdiction because 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: <u>Employee information</u> • name, • address, • email address, • date of birth, • hours worked • hourly pay rate, • Social Insurance Number (SIN), • direct deposit banking information.

	Customer information • name, • address, • email address • date of birth, • occupation, • telephone number. 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	• The Organization's computer systems were compromised by hackers on May 25, 2016 and 6.5 gigabytes of data containing personal information were downloaded. • The incident was discovered on May 30, 2016 through an email sent by the hackers. The hackers threatened to release the information on the internet if a ransom payment was not made by the Organization.
Affected individuals	A total of 14,294 individuals were affected by the incident.
Steps taken to reduce risk of harm to individuals	• Steps were taken to contain the incident including password change, malware scans and network traffic monitoring. • Appropriate communication was sent to staff regarding secure use of computer systems. • The Organization initiated an investigation into the incident and hired third party firms including cyber security and cyber-criminal law experts to assist in the investigation. • The vulnerability used by the hackers to access the Organization's network was identified and addressed. • The Organization has implemented improved internal monitoring controls and procedures. • Steps have been taken by the Organization to develop and rollout secure computer use practices to its employees. • The incident was reported to the local law enforcement body.
Steps taken to notify individuals of the incident	The Organization began notifying affected individuals on June 2, 2016. The Organization confirmed on June 20, 2016 that all affected individuals have been notified.

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 "Any breach of personal identification could result in significant damage to any affected individual, including possible identity theft and all of the terrible things that can be associated that (Primarily financial)." I agree with the Organization. The information at issue includes sensitive identity, financial, and employment information that could be used to cause the harms of identity theft, fraud and financial loss, hurt and humiliation. Email addresses could be used to launch targeted social engineering attacks against the individuals in an attempt to steal additional personal information (phishing). 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 breach, but reported the steps it is taking with the intent of "limiting possible individual harm to possibly affected individuals." In my view, the likelihood of harm resulting from this incident is increased because the information was downloaded and has not been recovered. In addition, there is malicious intent associated with the incident – the computer system of the Organization was hacked and a ransom demand was made.

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 information at issue includes sensitive identity, financial, and employment information that could be used to cause the harms of identity theft, fraud and financial loss, hurt and humiliation. Email addresses could be used to launch targeted social engineering attacks against the individuals in an attempt to steal additional personal information (phishing). These are all significant harms. The likelihood of harm resulting from this incident is increased because the information was downloaded and has not been recovered. In addition, there is malicious intent associated with the incident – the computer system of the Organization was hacked and a ransom demand was made.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that the Organization notified all affected individuals by June 20, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner