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	Enoch Casino Limited Partnership and River Cree Resort Limited Partnership, known as the River Cree Resort and Casino ("the Organizations")
Decision number (file number)	P2016-ND-27 (File #002588)
Date notice received by OIPC	March 17, 2016
Date Organizations last provided information	April 28, 2016
Date of decision	May 2, 2016
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organizations are 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"	The Organizations are limited partnerships and are "organizations" as defined in section 1(1)(i)(iv) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following: <u>Customer Information</u> • name, • date of birth, • telephone number, • email address, • contact address, • photographs, and • a trespassing notice and photograph of one patron, and • a surveillance report from 2016 (i.e. surveillance camera operator's observations documenting gaming play and security incidents – includes individual names when available).

	<u>Employee information</u> • name, • date of birth, • telephone number, • email address, • contact address, • Social Insurance Number (SIN), • Canada Revenue Agency T4 slips (2010), • employee investigations, and • completed health and wellness forms. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organizations' information technology network experienced a disruption on March 11, 2016. • On March 14, 2016, the Organizations received an email from hackers indicating the Organizations' computer systems had been compromised and personal information was stolen. The Organizations were not aware of the privacy breach until they received the email. • The Organizations reported that the personal information of current and former employees and customers "may have been stolen" and that the Organizations believed that "some or all of the alleged stolen data has, in fact, been stolen". • The hackers threatened to release the personal information to the internet unless a ransom was paid. • The Organizations reported that the compromise of their computer systems may have started in January 2016.
Affected individuals	The following individuals were affected by this incident: • 941 current and former employees, • 130,000 customer "Player's Club" members, • one customer against whom a trespassing notice was issued, and • an estimated 300 customers whose names were mentioned in the surveillance report.

Steps taken to reduce risk of harm to individuals	• The Organizations initiated an investigation into the incident and hired a third party cyber security firm to assist. • Steps were taken to contain the incident including changing systems passwords, scanning computer systems for malicious software, etc. • A telephone line was established on March 18, 2016 and staffed with agents to assist in answering questions or concerns from individuals. • The incident was reported to law enforcement. • The Organizations are monitoring the internet for potential unauthorized disclosure of the personal information by the hackers. • The Organizations reported that steps have been taken to ensure appropriate controls are implemented to prevent future attacks.
Steps taken to notify individuals of the incident	• On March 17, 2016 a news release was issued regarding the incident. • The Organizations advised their employees of the incident on March 18, 2016. • On April 28, 2016, the Organizations began notifying current and future employees by letter. • On April 28, 2016 the Organizations began notifying 124,000 affected customers by letter, where address information is available. The Organizations reported that the balance of affected customers will be notified by email or telephone, where contact information is available. • The Organizations established a telephone hotline to respond to customer concerns.
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 Organizations reported that affected individuals are at risk of identity theft and fraud. I agree with the Organizations. The personal information involved is highly sensitive and includes identity (e.g. SINs), financial, and medical information for former and current employees. Identity information of customers is also involved. This information could be used to cause the harms of identity theft, fraud and financial loss. Health and wellness information, and information related to investigations, could also be used to cause the harms of hurt, humiliation, or reputational damage.

	Email addresses and telephone numbers of former and current employees and customers were also compromised. This information could be used for social engineering attacks such as phishing and spam. Information contained in surveillance reports and the trespassing notice could be used to cause the harms of hurt, humiliation and reputational damage. In my view, 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 Organizations reported that the likelihood of identity theft and fraud resulting from the incident is low. The Organizations reported that the hackers gave no indication that personal information was their target or that such information will be used for identity theft or fraud. Also, the Organizations reported that there has been no indication that personal information from the incident has been disclosed to the internet. In my view, the likelihood of harm resulting from this incident is increased because personal information was stolen and the ransom demand indicates malicious intent. Potential unauthorized disclosure of the personal information to the internet by the hackers increases the likelihood of further unauthorized use.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organizations and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. The personal information includes identity, financial, and medical information for former and current employees. Identity information of customers was also involved. This information could be used to cause the significant harms of identity theft, fraud and financial loss. Email addresses and telephone numbers could be used to cause the significant harms of phishing and spam. Additional information involved in this incident could be used to cause the significant harms of hurt, humiliation and reputational damage.

The likelihood of harm resulting from this incident is increased because personal information was stolen and the ransom demand indicates malicious intent. Potential unauthorized disclosure of the personal information to the internet by the hackers increases the likelihood of further unauthorized use.

I require the Organizations to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) on or before May 11, 2016. I understand that notification is currently underway in accordance with the Regulation.

In issuing a decision under section 37.1(1) of PIPA I may require organizations to satisfy any terms or conditions I consider appropriate. I require the Organizations to confirm to me in writing that affected individuals have been notified on or before May 11, 2016.

Jill Clayton
Information and Privacy Commissioner