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	Grey Eagle Casino (Organization)
Decision number (file number)	P2021-ND-065 (File #005816)
Date notice received by OIPC	June 13, 2017
Date Organization last provided information	June 13, 2017
Date of decision	March 9, 2021
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"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • Social Insurance Number (SIN), • name, • address, • information about long term disability claim, • salary information, • number of hours worked, • exit interview information, • employee complaints. 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 January 10, 2017, an email was sent to the Organization's IT Manager claiming to be from the Organization's Human Resource Manager. • On January 12, 2017, the hackers sent a bogus email containing instructions about a "new password" to employees of the Organization. One employee acted on the instructions, which led to the compromise. • The incident was discovered on January 17, 2017 when the hackers sent screenshots of human resource documents and the Organization's payroll system to the Organization. • The perpetrators demanded a ransom.
Affected individuals	The Organization did not report the number of affected individuals.
Steps taken to reduce risk of harm to individuals	• Retained a third party cyber security firm to conduct forensics analysis and incident response on its IT systems. • Took steps to monitor the network, change systems passwords and scan computer systems for malicious software. • Reported the incident to law enforcement. • Notified the Organization's payroll provider and instructed it to take measures to secure the payroll system including account deactivation and password changes. • Notified other providers with instructions to disable users until appropriate passwords were changed. • Emailed staff regarding secure use of computer systems. • Monitoring the internet for unauthorized disclosure of the personal information.
Steps taken to notify individuals of the incident	• Current employees were notified in person and in writing. • Former employees were notified via registered mail. • One affected individual was deceased and could not be notified.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 level of sensitivity of the information (names, address, wages) is considered to be low." Further, "The likelihood of Identity Theft occuring [sic] to those employees whose names and addresses were breached is considered low." In my view, a reasonable person would consider the contact information at issue (name, address) alone could not be used to cause significant harm. However, in conjunction with identity and employment information, this information could be used to cause the harms of identity theft and fraud. Disability claims information

	could be used to cause the harms of hurt, humiliation and embarrassment. 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 reported: *The likelihood of Identity Theft occurring [sic] to those employees whose names and addresses were breached is considered low.* *The employee whose Social Insurance Number was breached passed away in 2013 and therefore it is deemed that there is no real significant harm in terms of identity theft. Although the group of hackers sent a screen shot of an employee's name, hours worked and net pay, it is not known whether the group of hackers actually infiltrated the ...Payroll System*. In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action, ransom demand).

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 the contact information at issue (name, address) alone could not be used to cause significant harm. However, in conjunction with identity and employment information, this information could be used to cause the harms of identity theft and fraud. Disability claims information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action, ransom demand).

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 the Organization notified the affected individuals, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner