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	Guillevin International Co. (Organization)
Decision number (file number)	P2021-ND-216 (File #018333)
Date notice received by OIPC	October 1, 2020
Date Organization last provided information	August 2, 2021
Date of decision	November 3, 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 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 operates in Alberta and is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	The Organization’s notice to affected individuals said the following concerning the information at issue… *...social insurance numbers were extracted as part of the security incident, although the documents containing your social insurance numbers were protected by passwords. We believe other personal information of our employees such as salaries, address, hours worked, schedules and insurance benefits could also have been exfiltrated.* 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	• On September 8, 2020, the Organization was the subject of a ransomware attack. A user account, compromised by phishing, was used in the incident. • It is reported that the attackers may have had access to the Organization’s network as early as August 13, 2020. • The Organization’s investigation determined that personal information was exfiltrated, however, some of the records were protected with a password.
Affected individuals	The incident affected 1,500 individuals, including 125 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Obtained forensic expertise and investigated the incident. • Implemented additional network activity monitoring. • Implemented revised privacy and security awareness training, leveraging the lessons learned from this breach. • Deployed measures to monitor the dark net. • Provided employees with identity theft monitoring and related insurance services. • Contacted police authorities. • Collaborated with the RCMP cybersecurity division.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 14, 2020.
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: *The categories of personal information which were compromised by malicious actors include social security numbers and other insurance-related information for our employees. For this reason, we consider that the possible harms can include identity theft, credit fraud and financial fraud. The insurance information did not include any health personal information, and we do not believe a riks [sic] of discrimination can occur, the information being largely financial in nature.* I accept the Organization’s assessment. A reasonable person would consider that the contact, identity, and employment information at issue could be used to cause the significant harms of identity theft, negative effects on a credit record, 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 reported: *The sensitive information was password protected and contained within one record as part of a large amount of data. We deployed technical measures to monitor potential uses on the dark net and online of such information. We provided employees with identity theft monitoring, related insurance and services to reassure them. We contacted the authorities and suggested to our employees adequate measures promptly so that they can reduce their own risks, as set forth in the attached notification letter. Therefore, we believe the residual risks are currently moderate. We have no indication that malicious actors have accessed password protected nformation [sic]. or used it, but we remain cautious to fully understand any riisks [sic] to our employees. We continue to monitor the situation to see if the risks are increasing.* *To the best of our knowledge, we can declare that none of our employees have been impacted by the breach after 10 months.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, phishing, deployment of ransomware). While the personal information at issue is protected by a password, the Organization did not respond to inquiries requesting clarification on the strength and nature of the technical safeguard. For example, it is unclear whether the password protection safeguards against brute-force attacks to unlock the record. Additionally, a lack of reported of misuse does not mitigate against future harm(s) as identity theft and fraud can occur months or 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 contact, identity, and employment information at issue could be used to cause the significant harms of identity theft, negative effects on a credit record, and fraud.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, phishing, deployment of ransomware).

While the personal information at issue is protected by a password, the Organization did not respond to inquiries requesting clarification on the strength and nature of the technical safeguard. For example, it is unclear whether the password protection safeguards against brute-force attacks to unlock the record.

Additionally, a lack of reported of misuse does not mitigate against future harm(s) as identity theft and fraud can occur months or 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 the Organization notified affected individuals by letter on September 14, 2020; however, it is not clear the notice complied with the requirements of section 19.1(1)(b)(ii) of the Regulation. The Organization did not respond to inquiries to clarify.

I require the Organization to confirm to my office in writing, within 10 days of the date of this decision, that the affected individuals whose personal information was collected in Alberta have been notified in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

Jill Clayton
Information and Privacy Commissioner