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	Sabina Gold & Silver Corp. (Organization)
Decision number (file number)	P2020-ND-178 (File #016325)
Date notice received by OIPC	July 1, 2020
Date Organization last provided information	July 1, 2020
Date of decision	December 8, 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 incident involved all or some of the following information: • first and last name, • social insurance number, • mailing address, • bank account information, and • 2019 annual gross income paid by the Organization. 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 or about March 28/29, 2020, an unknown individual accessed an employee's email inbox.

	• The attacker set up an auto-forwarding rule which caused certain emails containing personal information of a group of employees and contractors to be forwarded to an external Gmail account. • The Organization determined the attacker had somehow obtained the employee's credentials (password) and accessed the account through a legacy protocol. • The Organization's investigation did not conclusively find evidence regarding how the credentials were obtained by the attacker (such as phishing, malicious website, or guess/use of a previous password) and confirmed the access by the attacker was limited to one email inbox. • The Organization reported there was no evidence to determine that the attacker had accessed any other personal information in the inbox; however, the Organization could not conclusively determine that other information in the inbox had not been accessed. Therefore, the Organization reviewed the subject inbox to determine whether additional employees might have been exposed. • The breach was discovered on April 1, 2020 when the Organization's IT Manager received an email alert concerning a potential security issue.
Affected individuals	The incident affected 83 individuals, including five (5) individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an IT incident review. • Removed auto-forward rule from the email account and put mailbox securely on hold to allow for further investigation. • Ran message trace report to determine what emails were forwarded. • Changed password for the employee's account. • Ran antivirus on the employee's workstation and laptop, and other employees (no exceptions found). • Reviewed emails forwarded (43 in total) to determine what sensitive information was exposed. • Ran a report to determine the existence of other malicious email forwarding accounts for all other accounts/employees (no exceptions found). • Ran a report to identify any other unauthorized or abnormal access to the Organization's network via external VPN connections (no exceptions found). • Applied Group Policy Object to disable external forwarding. • Disabled access to email accounts through legacy protocols. • Enabled multi-factor authentication on user accounts with additional of other security features. • Conducted further mailbox analysis and investigation.

	• Offered Equifax and TransUnion credit monitoring package to affected individuals. • Provided education and training provided to employees regarding cyber hygiene and awareness, including requirement to ensure no payroll information is sent by email unencrypted; • Implemented advanced threat protection add-on to provide enhanced security scanning of emails. • Enabled data loss prevention.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on April 2, 2020 (initial notice), April 8 and April 13, 2020 (follow up notices with credit monitoring offer), and June 20, 2020 (second notice).
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, *Name, address, gross pay and SIN (Initial Notice: 3 Alberta employees; Second Notice: 2 Alberta employees) could result in identity theft and fraud;* In my view, a reasonable person would consider that the contact, identity and financial information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. 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, *There is a likelihood that harm will result for the three Alberta employees whose names, addresses, SINs, and gross pay information were forwarded to the attacker. There is a real risk of harm but it is possibly less for the two Alberta employees whose personal information was potentially accessible to the attacker because the attacker may not have accessed this information. This assessment is based on the following factors:* *- The nature of the personal information (in particular, the SINs) is very sensitive personal information;* *- [The Organization] has been unable to identify the third party who obtained access to the personal information;* *- The personal information was not encrypted;* *- There is evidence of malicious intent as the forwarding rule was purposely placed, however, it is not clear that the attacker was looking for employee information;* *– The personal information could be used for criminal purposes, such as identity theft or fraud;* *– The information has not been recovered from the unidentified third party bad actor;*

	– A significant number of employees (105) were affected, with 63 of those employees having their SINs accessed as part of the breach. I agree with the Organization's assessment. A reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party, and the information has not been recovered. Additionally, the Organization can only speculate as to the motives of the attacker.

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 financial information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. These are all significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party, and the information has not been recovered. Additionally, the Organization can only speculate as to the motives of the attacker.

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 the affected individuals by email on April 2, 2020, April 8, 2020, April 13, 2020 and June 20, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner