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	Sabre Instrument Services Ltd. (Organization)
Decision number (file number)	P2021-ND-299 (File #020449)
Date notice received by OIPC	March 30, 2021
Date Organization last provided information	March 30, 2021
Date of decision	March 2, 2022
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 incident involved employee credentials (usernames and passwords) used to log into the Organization's system. The user names are employee email addresses, the majority of which include employee name. 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. The Organization reported that some of the email addresses at issue are business email addresses. As such, this information may qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation

	to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized disclosure of the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, this personal information is no excluded from PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On December 16, 2020, as part of a ransomware attack, an unknown threat actor installed malware in the Organization's system. • The Organization determined that the malware harvested and copied usernames and passwords used by its employees to log into the Organization's system. • The malware would have automatically copied usernames and passwords that were in the system on December 16-17, 2020. • The attacked was discovered on December 17, 2020. • The Organization's investigation determined that while the threat actor had access to these copied usernames and passwords, there was no evidence that the copied information was exported or misused.
Affected individuals	The incident affected 26 individuals whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an internal analysis and retained counsel who retained a third party cybersecurity firm to investigate. • Reset employee passwords. • Automatically generated the passwords used to log into the system. • Reset administrator passwords. • Re-built and upgraded the server. • Partitioned the backup server.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 29, 2021.

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, *Disclosure of passwords connected with individuals' names from their usernames gives rise to a risk that if the individual used the password for other purposes, that password would be compromised. The use of a password suggests some level of sensitivity in itself. If the passwords were used for certain accounts like banking, the risk would be higher.* *Because the usernames are email addresses, the unauthorized access gives rise to a risk of phishing or spam emails. However, there was no evidence at all that the copied information was exported or misused in any way.* In my view, a reasonable person would consider that the credential information at issue could be used to compromise other online accounts. Email addresses could be used for phishing, increasing vulnerability to identity theft, fraud and other online accounts. These are 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 real risk of the above harm occurring because the threat actor had access to the information. However, based on the information we have, the harm is unlikely to materialize because:* • *there is no evidence that the threat actor exported the information that was harvested and copied by the malware and no evidence that the information has been misused;* • *the threat actor's apparent intention was to demand a ransom, rather than collecting personal information for other uses; and* • *the passwords used to log into [the Organization's] system are automatically generated.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). The lack of evidence to date that the information has been misused does not mitigate the harm, as phishing, identity theft and fraud can happen months and even years after a data breach. Additionally, the Organization did not provide the evidence it relied on to conclude that personal information was not copied or

	misused. Although the Organization reported "the threat actor's apparent intention was to demand a ransom, rather than collecting personal information for other uses", I do not find this to be reassuring. The Organization can only speculate as to the perpetrator's motives.

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 credential information at issue could be used to compromise other online accounts. Email addresses could be used for phishing, increasing vulnerability to identity theft, fraud and other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). The lack of evidence to date that the information has been misused does not mitigate the harm, as phishing, identity theft and fraud can happen months and even years after a data breach. Additionally, the Organization did not provide the evidence it relied on to conclude that personal information was not copied or misused. Although the Organization reported "the threat actor's apparent intention was to demand a ransom, rather than collecting personal information for other uses", I do not find this to be reassuring. The Organization can only speculate as to the perpetrator's motives.

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 email on March 29, 2021. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner