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	Underwriters Laboratories of Canada Inc. (Organization)
Decision number (file number)	P2021-ND-178 (File #020570)
Date notice received by OIPC	April 2, 2021
Date Organization last provided information	May 19, 2021
Date of decision	September 2, 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 incident involved all or some of the following information: "Personal Information (limited)" • copy of signature, • tax ID number, • date of birth, and • personal contact information. "Business Contact Information" (majority of the data) • name, • work email address, • work telephone number, • job role, and • office address. 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. Some of the 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 access to 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, PIPA applies to the business contact information. The Organization reported that the documents were primarily of a commercial nature, such as company filings and financial records, and were composed of mainly unstructured data. As well, the Organization reported that no consumer data was identified.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On February 13, 2021, the Organization detected unusual activity on its systems. • The Organization found that the unusual activity related to an attempt to encrypt certain systems by an unauthorised third party. • The Organization's preliminary findings indicated that the threat actor's primary objective was to cause disruption to the Organization's operations in order to extract a ransom. • The Organization reported it has no reason to believe that any personal data relating to data subjects in Alberta has been made permanently unavailable or deleted and has no evidence to suggest that any personal data relating to Alberta residents has been misused. • The Organization reported that multiple searches of the dark web tailored to look for any of the data involved in this incident have not found any such data.
Affected individuals	The incident affected 226 individuals residing in Alberta.

Steps taken to reduce risk of harm to individuals	• Promptly took various mitigating steps. • Shut down systems as a precaution, including those that were not displaying any suspicious activity. • Engaged several third parties to assist internal response teams in assessing and mitigating the incident. • Will determine any additional steps that should be adopted to reduce the risk of a similar event occurring in the future.
Steps taken to notify individuals of the incident	Affected individuals were notified on May 24, 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 that it … *…has identified only a limited number of data subjects where certain personal data of limited sensitivity was accessible by the threat actor... These individuals are… employees or business contacts, and a majority of the data that has been identified was business contact information only. Other limited categories of data accessed or exfiltrated and the number of data subjects we have identified, in connection with each category, are set out in the table included in the Schedule to this letter. This data relates to … employees and business contacts. No consumer data was identified.* In my view, a reasonable person would consider the contact, identity and employment information could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft 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 that it has … *… concluded that there is no likelihood of there being a real risk of significant harm to the identified data subjects affected by this Incident for the following reasons:* • *The data which was accessed is generally commercial in nature and the majority of the documents are in unstructured form, meaning that this information is very unlikely to be used in ways which could be harmful to individual data subjects. This is a very different situation from those involving large amounts of consumer data that are typically exploited by perpetrators of computer crime seeking to profit from the misuse of such data. In other words, from a criminal perspective, there is little value in the data affected in this case, and it would*

	involve disproportionate effort to seek to extract any such value. • *The threat actor responsible for this Incident is thought to have had the primary objective of causing disruption to [the Organization's] business operations in order to extract a ransom. The nature of [the Organization's] business makes it an unattractive target for cyber-criminals seeking to steal and profit from the misuse of data relating to individuals. In our experience, when the objective of such criminals is to exploit for their financial gain the data relating to individuals that is handled by commercial organizations, they typically target consumer-oriented businesses likely to have very large amounts of consumer personal data that can be sold illegally to commit fraud, including impersonation using stolen credentials and theft. Conversely, when organizations like [this Organization] are targeted by cyber-criminals, the objective is typically to cause disruption to business operations and benefit from that, rather than the exploitation of the relatively limited data relating to individuals that may be compromised. This was certainly the case in this instance and, as such, there is no evidence to suggest that any data relating to individuals was stolen for profit or otherwise misused by the threat actor.* • *Multiple searches of the dark web tailored to look for any of the data involved in this Incident have not found any such data.* • *[The Organization] is not aware of receiving any complaints from any employees or business contacts in Alberta that would suggest that data relating to them has been misused by any third party in connection with this Incident. This is also supported by the lack of any evidence that the perpetrators have sought to benefit in any way from potential misuses of the data involved.* 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 an unknown third party (deliberate intrusion, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach. The Organization can only speculate as to the motives of a threat actor.

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, identity and employment information could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud. 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 reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach. The Organization can only speculate as to the motives of a threat actor. 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 on March 24, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner