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	LifeLabs Inc.
Decision number (file number)	**P2020-ND-036** (File #014221)
Date notice received by OIPC	December 16, 2019
Date Organization last provided information	March 2, 2020
Date of decision	March 17, 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 and is in the control of the Organization, 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: • name, • gender, • phone number, • address, • email address, • date of birth, • login and password, • Alberta Health Care number, • lab results. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta and is in the control of the Organization, PIPA applies.
DESCRIPTION OF INCIDENT	
☐ loss	☒ unauthorized access ☐ unauthorized disclosure
Description of incident	▪ A cyber attack involving unauthorised access to two web servers and two databases occurred. ▪ The incident was discovered on October 28, 2019.

	▪ The Organization engaged cyber security experts to isolate and secure the affected systems and determine the scope of the breach.
Affected individuals	The Organization reported that the incident affected approximately 21,700 Albertans.
Steps taken to reduce risk of harm to individuals	▪ Immediately engaged cybersecurity experts to isolate and secure the affected systems and determine the scope of the breach. ▪ Further strengthened their systems to deter future incidents. ▪ Engaged with law enforcement. ▪ Offered cybersecurity protection services to customers. ▪ Required returning customers to reset their passwords.
Steps taken to notify individuals of the incident	The Organization issued a public letter notifying affected Canadians of the incident. Where the Organization also had an email address of the affected individual, an email was sent.
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 potential harm could include identity theft or revealing sensitive health information (in the case of accessed lab test information). I accept the Organization's assessment. A reasonable person would consider the contact and identity information at issue could be used to cause the harms of identity theft, as well as fraud and financial harm. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Lab results information could be used to cause hurt and humiliation. 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 it "considers the risk to the affected customers to be low because: It is difficult to commit financial fraud with the data that was compromised … the criminal attackers disclosed that their intent was to receive payment for the safe return of the data and that they would not release the data if payment was received. … Our cyber security firms have not seen any public disclosure of customer data during their ongoing investigation … Since the attack, Lifelabs has implemented additional security safeguards such as encrypting our servers, resetting our passwords and actively monitoring new threats to help protect against secondary attacks; and We are offering our customers cyber security protection for one year …." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious intent.

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 and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Lab results could be used to cause hurt and humiliation. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious intent. The Organization did not say whether it had directly notified the affected individuals whose personal information was collected in Alberta and is in the control of the Organization. I have only *An Open Letter to LifeLabs Customers*, dated December 17, 2019 and updated January 9, 2020, which is not direct notification. **Therefore, in accordance with section 37.1(1)(a) of PIPA and section 19.1(1) of the *Personal Information Protection Act Regulation* (the Regulation), I require that the Organization directly notify the affected individuals whose personal information was collected in Alberta and is in the control of the Organization. In accordance with section 37.1(1)(b) and (2) of PIPA, I also require that the Organization confirm to me in writing, within 30 days of the date of this decision, (in light of the COVID-19 pandemic) that it has done so, and provide me with an anonymized copy of the notification.** **If the Organization is unable to directly notify any or all of the affected individuals, then it may ask me under section 19.1(2) of the Regulation to determine whether direct notification would be unreasonable in the circumstances and whether indirect notification may be given to any or all of the affected individuals: see, for example, Breach Notification Decisions P2018-ND-049, P2019-ND-152 and P2019-ND-156 (available at www.oipc.ab.ca).**

Rachel Hayward
Director, Compliance and Special Investigations