Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

JOINT INVESTIGATION INTO LIFELABS DATA BREACH

Information and Privacy Commissioner of Ontario PHIPA Decision 122

Information and Privacy Commissioner for British Columbia Investigation Report 20-02

Brian Beamish
Information and Privacy Commissioner of Ontario

Michael McEvoy
Information and Privacy Commissioner for British Columbia

June 25, 2020

EXECUTIVE SUMMARY

1 BACKGROUND

1.1.1 LifeLabs

1.1.2 The Data Breach

1.1.3 Investigative Process

2 ISSUES AND DISCUSSION

2.1 Issue 1: Scope of Information Compromised in the Breach

2.2 Issue 2: Personal Health Information and Personal Information

2.2.1 Was the Information Compromised in the Breach Personal Health Information and Personal Information?

2.2.2 Sensitivity and Potential Harms

2.3 Issue 3: Health Information Custodian and Organization

2.4 Issue 4: Reasonable Steps to Protect Personal Health Information and Personal Information

2.4.1 Reasonable Technical Safeguards

2.4.2 Steps to Contain and Investigate Breach

2.4.3 Risk Evaluation

2.4.4 Steps to Remediate Systems and Processes

2.5 Issue 5: Policies and Information Practices

2.6 Issue 6: Collection of Unnecessary Personal Health Information and Personal Information

2.7 Issue 7: Notice to Affected Individuals

3 ORDERS AND RECOMMENDATIONS

EXECUTIVE SUMMARY

On November 1 and 5, 2019, respectively, LifeLabs notified the Office of the Information and Privacy Commissioner of Ontario (ON IPC) and the Office of the Information and Privacy Commissioner for British Columbia (BC OIPC) of a potential privacy breach under Ontario's *Personal Health Information Protection Act* (PHIPA) and British Columbia's *Personal Information Protection Act* (PIPA). LifeLabs advised that on October 28, 2019, through a security assessment conducted by a third party, it had detected a cyberattack on its computer systems. After locking down the affected systems, LifeLabs was contacted by the attackers. The attackers claimed to have stolen the personal information and personal health information of LifeLabs' customers and threatened to release the information publicly unless LifeLabs paid a ransom. The attackers also threatened to include a report detailing the exploits of their attack in the information released publicly, and provided LifeLabs with a sample of the personal information and personal health information they had stolen.

After additional correspondence to substantiate the attackers' claims, LifeLabs paid the ransom. The attackers provided LifeLabs with a copy of their report and a substantial amount of data, consisting of the personal information and personal health information of approximately 8.6 million LifeLabs customers, located primarily in Ontario and British Columbia.

The ON IPC and the BC OIPC have conducted a joint investigation of the breach. Having concluded their investigation, the ON IPC and BC OIPC make the following findings:

1. LifeLabs failed to take reasonable steps to protect personal information and personal health information in its custody and control from theft, loss, and unauthorized access, collection, use, disclosure, copying, modification or disposal.

2. LifeLabs failed to have in place and follow policies and information practices that comply with PIPA and PHIPA.

3. LifeLabs collected more personal information and personal health information than is reasonably necessary to meet the purpose for which it was collected.

The ON IPC makes the following additional findings in this investigation:

4. LifeLabs has not implemented a process to notify all individuals about the details of what of their personal health information was compromised without requiring those individuals to make a formal access request. Therefore, LifeLabs has not

complied with its obligation to notify affected individuals of the breach at the first reasonable opportunity.

5. LifeLabs' contractual arrangements to provide laboratory services to a hospital is inadequate in defining the parties' respective roles and responsibilities under PHIPA.

Given these findings, the ON IPC and BC OIPC issue the following orders to LifeLabs:

1. LifeLabs is ordered to:

    - subscribe the appropriate staff on its security team to Telerik's security notification list; and

    - ensure that the staff are aware of their responsibilities to effectively monitor the list for security alerts.

2. LifeLabs is ordered to put in place comprehensive written information practices and policies that are in force and that set out the safeguards that LifeLabs has implemented with respect to information technology security in order to comply with PHIPA and PIPA.

3. LifeLabs is ordered to cease collecting failed login and password pairs and to securely dispose of the records of that information that it has collected.

The ON IPC also issues the following orders to LifeLabs:

4. LifeLabs is ordered to implement a process to notify all individuals of what of their personal health information was compromised by the breach without the individual having to make an access request pursuant to Part V of PHIPA.

5. LifeLabs is ordered to clarify and formalize its status under PHIPA with respect to its contractual relationships with Trillium and any other health information custodian in Ontario with whom it has a similar relationship.

In addition, we also make one recommendation to LifeLabs:

1. It is recommended that LifeLabs consult with independent third-party experts with respect to whether a longer period of credit monitoring service would be more appropriate in the circumstances of this breach.

1 BACKGROUND

1.1.1 LifeLabs

LifeLabs is Canada's largest provider of general health diagnostic and specialty laboratory testing services. It has been in operation for over 50 years and currently has 5,700 employees. It provides a full range of outpatient laboratory services and other testing services, including genetics and naturopathic testing. LifeLabs performs over 100 million laboratory tests each year, with 20 million annual patient visits to its locations. Its website hosts Canada's largest online patient portal, on which more than 2.5 million individuals access their laboratory results each year.

1.1.2 The Data Breach

This investigation concerns a large-scale data breach of LifeLabs' systems affecting the personal information and personal health information of its customers. Although the breach was initially discovered in October 2019, unauthorized access attributed to the attackers had been going on periodically since at least November 24, 2018. The breach involved, in total, an unknown number of LifeLabs' systems. However, the customer information determined to be compromised in the breach relates to four of LifeLabs' systems:

1. System A, a database of patient visit information from 1992 to 2015, used for historical enquiries.

2. System B, a billing tool used to submit invoices and receive payments.

3. System C, an enterprise data warehouse used to integrate and provide standardized access to frequently used data from different sources.

4. System D, an online appointment booking system.

LifeLabs first became aware of suspicious activity on October 28, 2019, when, in the context of a security assessment being conducted by an IT security company (CrowdStrike), LifeLabs was sent a notice alerting it to a likely compromise of System D. A user account was detected writing and executing malicious files as well as extracting sensitive information from two database servers. On notification, LifeLabs isolated the affected servers and disabled the compromised account. It then applied additional security controls to all compatible servers and systems to protect them against further compromise.

On October 31, 2019, LifeLabs received a ransom email from the attackers. In the email, the attackers claimed to have stolen patient records from LifeLabs and stated that their intent was to receive payment in exchange for the deletion of their copy of the data. They also offered to send LifeLabs a report detailing the exploits of their attack. To substantiate their claims, the attackers included a sample of patient records. The attackers threatened to release the data and their report onto the internet if they did not receive payment by November 15, 2019.

In response, LifeLabs initiated a full incident response investigation, with assistance from CrowdStrike, and began assessing and responding to the attackers' claims.

LifeLabs communicated with the attackers with the assistance of another third-party IT security company (Cytelligence). First, LifeLabs requested additional evidence to further substantiate the attackers' claims. In return, the attackers provided a high-level summary of the attack and additional patient records. Following this, LifeLabs made two payments to the attackers. A first, partial payment was made in return for the attackers' report. A second payment was then made to complete the exchange. In return for payment, the attackers provided LifeLabs with four datasets, which they indicated was all the LifeLabs data in their possession. These datasets were subsequently analyzed by LifeLabs and confirmed to contain data related to Systems A, B, C and D, described above.

The attackers' method of intrusion worked in stages. They first gained access to LifeLabs' network by exploiting vulnerabilities on two internet-accessible webservers hosting content for System D. Through these vulnerabilities, the attackers were able to upload their own malicious web pages to the webservers, granting themselves remote access to run commands. After escalating their privileges, the attackers were then able to extract information from two database servers storing data for System D. The attackers were also able to access a file share server on which a number of service account and administrator passwords were stored in an encrypted file.

The attackers claimed to have had the ability to move progressively (or "laterally" as it is known in information security parlance) through LifeLabs' network with a domain administrator token. However, LifeLabs' investigation was unable to verify actual lateral movement due to a lack of evidence and available forensic information. LifeLabs took into consideration the fact that the attackers were able to access data related to systems beyond System D. However, it concluded that this aspect of the breach should not be considered as proof of lateral movement.

After analyzing the datasets returned by the attackers, LifeLabs discovered discrepancies in some of them, raising questions as to their origin. LifeLabs' data analysis concluded that

the attackers did not extract the datasets related to Systems A, B and C from the live production servers those systems ran on. In contrast to the dataset returned by the attackers related to System D, which was confirmed by LifeLabs to have come from that system's live database servers, the datasets related to Systems A, B and C were found by LifeLabs to contain data that was out of date, incomplete and/or related to decommissioned systems. According to LifeLabs' analysis, it appeared that the attackers located old file reports or extract files of data from Systems A, B and C generated by a LifeLabs employee, and stole those, rather than accessing the current production systems themselves. However, LifeLabs was unable to locate any of the three purported file reports or extract files on its network.

LifeLabs' investigation found that the earliest known date of unauthorized access to its systems was November 24, 2018. However, the attackers claimed that the breach began sometime between July and October 2018. The last known date of unauthorized activity was November 1, 2019.

In total, records relating to approximately 8.6 million unique individuals were identified among the four datasets supplied by the attackers. The vast majority were from Ontario and British Columbia. However, individuals from all provinces were represented in the data. The datasets contained various types of personal information, including demographic information, email, phone number, address, health card number, laboratory results, healthcare provider information, security question and answers, and failed login and passwords. The number of individuals affected for each type varied across the datasets.[1]

LifeLabs notified the ON IPC of the data breach on November 1, 2019, and the BC OIPC on November 5, 2019.

On December 17, 2019, LifeLabs issued a public notice about the data breach to its customers and began working to directly notify approximately 85,000 individuals in Ontario whose laboratory test results were found in the datasets returned by the attackers. LifeLabs updated its public notice on January 9, 2020 to update the scope of the information affected by the breach.

To date, LifeLabs states that it has found no indication of unauthorized use or disclosure of patient data beyond the attackers.

[1] For a more detailed breakdown and analysis of the number of individuals and types of personal information at issue, see section 2.1.

1.1.3 Investigative Process

The ON IPC and the BC OIPC have conducted a joint investigation of this breach. The BC OIPC conducted the investigation under the authority of section 36(1)(a) of PIPA. The ON IPC conducted a review under section 58(1) of PHIPA. During this investigation, LifeLabs has been provided with numerous opportunities to provide documents, information, evidence, and representations to the ON IPC and BC OIPC with respect to the issues being investigated. This matter has a lengthy history with respect to requests and orders for production of documents and information, some of which is detailed in PHIPA Decision 114. LifeLabs provided some of the documents that it was ordered to produce in PHIPA Decision 114 and in a production order issued by the BC OIPC. However, it continued to claim that those documents were privileged, that privilege is not waived, and that they contained confidential information; and objected to the release of that information by the ON IPC and the BC OIPC. These claims have been addressed in an Interim Decision provided to LifeLabs.

In addition to requesting and ordering the production of relevant documents and information from LifeLabs, the ON IPC and BC OIPC also issued summonses to representatives of LifeLabs to attend at the office of the ON IPC in Toronto to give evidence under oath, which they did in February 2020. LifeLabs was given opportunities to make representations to the Commissioners regarding the matters at issue in this investigation, which they did.

In the course of conducting a review under PHIPA, the ON IPC follows the processes set out in its *Code of Procedure for Matters Under PHIPA* (the Code). Because of the joint investigation with the BC OIPC, some variations from the processes set out in the Code were necessary. The Code itself provides for this, stating that the ON IPC may waive or vary any of the processes set out in the Code if it is of the opinion that it would be advisable to do so in order to secure the just and expeditious determination of an issue.[2]

The ON IPC and BC OIPC received a number of calls from members of the public that raised a variety of concerns regarding the LifeLabs breach, including the quality of the service received from the LifeLabs call centres and that the length of the credit monitoring service offered by LifeLabs was too short. The callers were informed that the Commissioners had already commenced an investigation and would issue a public report when the investigation was completed.

[2] See the Code (https://www.ipc.on.ca/wp-content/uploads/2017/02/2017-code-phipa-e.pdf), section 29

2 ISSUES AND DISCUSSION

2.1 Issue 1: Scope of Information Compromised in the Breach

LifeLabs was able to verify that the four datasets the attackers returned to them after being paid a ransom consisted of information stolen from LifeLabs' network. Thus, it is clear that the scope of information compromised in the breach includes at least these four datasets. However, it is possible that additional information about individuals was compromised in the breach.

The attackers indicated that the four datasets represented all of LifeLabs' data in their possession. Yet, LifeLabs was unable to verify this. Apart from the suspicious activity discovered on October 28, 2019, in relation to System D, LifeLabs was unable to find evidence of any additional data exfiltration. This was so despite the fact that the attackers were able to access and remove data in relation to three other systems.

Nor was LifeLabs able to disprove the attackers' claim about being able to move laterally across its systems. Although LifeLabs was able to verify that the attackers had accessed five servers on its network, mostly in relation to System D, the available evidence was limited in the following ways:

- Reconstructing the potential historical access of the attackers to specific systems was not feasible because the system environment changed significantly due to the measures taken in response to the breach.

- At the time the breach was discovered, LifeLabs was in the process of onboarding a Privileged Access Management (PAM) solution. LifeLabs was unable to verify whether the domain administrator account that was leveraged by the attacker had been onboarded with the PAM solution by the time the breach was discovered. Nonetheless, LifeLabs believes it was not.

- According to LifeLabs, if an attacker successfully impersonates an authentication token, then the organization cannot differentiate the attacker's use of that authentication token from the legitimate use of the authentication token by an authorized user of the account.

- Theoretically, the attackers could have had access to any computer in the domain connected to the compromised account, depending on varying factors including the attackers' skill level.

Thus, the only real evidence limiting the scope of information compromised in the breach to the four datasets returned by the attackers is the attackers' own claim to that effect, a claim made while negotiating a ransom settlement with their victim.

Ideally, the evidence for determining the scope of a breach should come from the organization responsible for the protection of the information, not the perpetrators. If an organization is unable to sufficiently verify the scope of a breach, then the scope should be broadened to include not only what *was* accessed but what *may have been* accessed.

In the absence of additional evidence, LifeLabs has determined that the scope of information compromised in the breach consists of the four datasets returned by the attackers.

In total, the four datasets consist of approximately 16 million records relating to individuals. However, some individuals' records were contained in multiple datasets. After taking this into account, an aggregate total of approximately 8.6 million unique individuals were identified across the four datasets. This included approximately 7.2 million individuals from Ontario and approximately 1.3 million individuals from British Columbia. The remaining individuals were from other provinces or unknown geographical location.

LifeLabs originally stated publicly that approximately 15 million individuals were potentially impacted by the breach. However, according to LifeLabs, this reflected a conservative approach of estimating unique individuals in the entire LifeLabs production environment, not the datasets themselves. After conducting further analysis of the datasets, LifeLabs updated its numbers to 8.6 million individuals.

The following table provides a general breakdown of the information contained in the datasets related to Systems A and B.

Dataset	**Count of Affected Individuals**	**Geographic Location of Affected Individuals**	**Time Period**	**Data Elements**
System A	2,914,035	Ontario	November 1992 to February 2015	• Name • Date of birth

				• Health number • Service date • Healthcare provider name, address and ID
System B	1,274,968	Primarily British Columbia	November 2014 to May 2015	• Name • Gender • Date of birth • Address • Health number • Transaction date • Healthcare provider name, address and ID

The composition of the datasets related to Systems C and D was more complex, with significant differences in patient counts for various types of information. The following tables provide a general breakdown of each of these datasets, including a summary description at the end.

Dataset	**Count of Affected Individuals**	**Geographic Location of Affected Individuals**	**Time Period**	**Data Elements**
System C	7,019,179	Primarily Ontario	2010 to 2016	• Name • Gender • Date of birth

				• Address • Postal code • Health number and version code
	84,553	Ontario	January 2016	• Name • Gender • Date of birth • Address • Postal code • Health number and version code • Healthcare provider name, address, billing number, license number, status (active/inactive), type (ordering vs. copy-to) and specialty • Laboratory test number, date, location, type and results
	47,404	Ontario	January 2016	• Name • Gender • Date of birth • Address • Postal code

				• Health number and version code • Healthcare provider name, address, billing number, license number, status (active/inactive), type (ordering vs. copy-to) and specialty • Laboratory test number, date, location and type (no results)

In other words, the dataset related to System C contained the information of about 7,151,136 unique patients. For 7,019,179 of these, the dataset contained only patient demographic information; for 84,553, it contained patient demographic, healthcare provider and laboratory test information including results; and for 47,404, it contained patient demographic, healthcare provider and laboratory test information but without results.

Dataset	**Count of Affected Individuals / Number of Records**	**Geographic Location of Affected Individuals**	**Time Period**	**Data Elements**
System D	1,868,849	British Columbia and Ontario	November 2011 to October 2019	• Name • Phone number • Login (email address)
	614	British Columbia and Ontario	March 2012 to October 2019	• Name • Phone number

				• Login (email address) • Password (encrypted) • IP address
	2,914,065	British Columbia and Ontario	November 2011 to October 2019	• Name • Phone number • Login (email address) • Password (encrypted) • IP address • Challenge security questions and answers
	1,801,567	British Columbia and Ontario	July 2011 to November 2012	

In other words, the dataset related to System D contained the information of about 4,783,528 unique patients. For 1,868,849 of these, the dataset contained only name, phone number and login (email address); for 614, it contained the former plus password (encrypted) and IP address; and for 2,914,065, it contained all of the former information plus challenge security questions and answers. In addition, the dataset contained 1,801,567 records of failed login (email address) and password (plaintext) pairs.

2.2 Issue 2: Personal Health Information and Personal Information

2.2.1 Was the Information Compromised in the Breach Personal Health Information and Personal Information?

There is no dispute that the information compromised in the breach was "personal health information" as defined in section 4 of PHIPA and "personal information" as defined in section 1 of PIPA.

2.2.2 Sensitivity and Potential Harms

Although whether information is personal health information or personal information does not depend on its sensitivity or the potential harms that may result from its disclosure, these characteristics play an important role when considering other issues, such as whether reasonable safeguards were in place and whether an appropriate risk evaluation was conducted in the case of a breach. Regardless, once it is established that some information is personal health information or personal information, all of the obligations set out in PHIPA and PIPA apply to the responsible custodian or organization.

LifeLabs took the position that the vast majority of the information compromised in the breach was not highly sensitive and that the only "live" production environment for which unauthorized access was able to be verified (System D) had *no* sensitive information. Among other claims, LifeLabs submitted that only 1.5% of the compromised data consisted of laboratory test orders or results and that the other datasets did not contain "health" information *per se,* but, at most, limited contact/provider information and an individual's health card number.

We disagree with LifeLabs' assessment and find their approach to be very cavalier regarding the privacy of their clients' health information. For example, we completely reject the idea that health card numbers are not sensitive. All the compromised personal health information and personal information was sensitive. The datasets related to Systems A, B and C each contained patient demographic information including one's health number. In the right circumstances, this

information could be used by an identity thief to steal an individual's identity and impersonate them to obtain false credit or fraudulent benefits.

The datasets related to Systems A and B and some of the dataset related to System C also contained information about the affected individuals' healthcare providers. From this link or "metadata," it may be possible to infer general diagnoses or health outcomes by virtue of the healthcare provider's practice or speciality. For example, it would be reasonable to assume that a patient with links to an oncologist may have cancer or a history of cancer. More specific and revealing inferences would be possible for the group of patients in the dataset related to System C whose laboratory test *types* are revealed but not results. This information may lead to the embarrassment or stigmatization of individuals.

However, even more sensitive is the information about the group of patients in the dataset related to System C whose actual laboratory results were disclosed. The level of detail in

these records could lead to harms that, in addition to embarrassment and stigmatization could include the possibility of blackmail or extortion depending on the nature of the test and result.

The dataset related to System D may at first appear to contain the least sensitive information of the datasets. However, to assume this would be a mistake. Not only could the challenge security question and answers be used by an identify thief, but the failed login and password pairs may reveal the highly confidential login and password information one uses for authentication to other websites and applications. For who hasn't at some time accidentally attempted to login to a website or application using the login and password for another? If this information contained the authentication credentials to one's personal email address or online banking account, it is possible that an attacker could wreak much havoc to an individual's life. Our entire digital lives play out in some of these accounts. The harms that could result range from identity theft to financial loss and fraud to the misuse and appropriation of one's entire social network.

2.3 Issue 3: Health Information Custodian and Organization

There is no dispute that LifeLabs is a "health information custodian" as defined in section 3(1) of PHIPA.

There is no dispute that LifeLabs is an "organization" as defined in section 1 of PIPA.

2.4 Issue 4: Reasonable Steps to Protect Personal Health Information and Personal Information

Section 12(1) of PHIPA states:

> 12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custodyor control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

Section 13(1) of PHIPA states:

> 13 (1) A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.

Section 34 of PIPA states:

> 34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

From the way sections 12(1) and 13(1) of PHIPA and section 34 of PIPA are written, it is clear that they do not prescribe a "one-size-fits-all" approach to security. Neither they, nor the regulations in the case of PHIPA, set out a list of measures that every health information custodian or organization must put in place regardless of circumstance. Instead, they require custodians or organizations to have "reasonable" or "secure" measures in place. It follows that the same security measures may not be required of all custodians or organizations. Depending on the circumstances, the required measures may differ.

Determining what constitutes "reasonable" or "secure" in the circumstances requires a contextual consideration of the situation at hand. A number of factors come into play. These include the nature of the information, including its sensitivity and the number of records, as well as the nature of the custodian or organization, including its size.

Furthermore, simply because a breach occurred does not by itself mean that reasonable or secure measures were not in place. The standard set out in sections 12(1) and 13(1) of PHIPA and section 34 of PIPA is not perfection but reasonableness. It is therefore possible for personal health information or personal information to be accessed in an unauthorized manner and yet the measures in place still be reasonable or secure.

LifeLabs has cited a number of cases regarding how "reasonable in the circumstances" has been interpreted by the Supreme Court of Canada.[3]None of these cases is factually similar to the circumstances of the LifeLabs breach. However, the ON IPC and BC OIPC find that our discussion above of what is meant by reasonable security measures under PHIPA and PIPA is consistent with principles advanced in the cases cited by LifeLabs and with previous cases considered by the ON IPC and BC OIPC.

In this case, approximately 8.6 million individuals were affected by the breach, resulting in the compromise of sensitive, and in some cases highly sensitive, personal health information and personal information. LifeLabs is Canada's largest provider of general

[3] *Lessard v. Paquin et al.*, [1975] 1 SCR 665; *Stewart Elk Valley Coal Corp.*, 2017 SCC 30; *Gold v. Rosenberg* [1997] 3SCR 767; *Ingles v. Tutkaluk Construction Ltd.* 2000 SCC 12.

health diagnostic and specialty laboratory testing services, with 5,700 employees. These facts help to inform our analysis in the following sections.

2.4.1 Reasonable Technical Safeguards

Based on our review of the representations we received from LifeLabs, the information and documents that they provided, and the responses from LifeLabs' representatives when questioned under oath, the ON IPC and BC OIPC find that LifeLabs failed to implement reasonable information technology security measures to protect the personal health information and personal information in its custody or control.

In the discussion that follows, we at times refer to various security assessment reports performed by third parties on LifeLabs' systems, at the behest of LifeLabs. LifeLabs asserted that some of these reports do not necessarily represent an accurate, objective or fulsome depiction of LifeLabs' security posture. In particular, LifeLabs submitted that:

- some reports were in draft form and not yet formally completed;
- some reports contained material inaccuracies;
- some report findings omitted reasonable context which may be helpful in assessing the materiality of the identified issue; and
- the third-party consultants who produce such reports often draft them with a view towards generating further business and creating an urgency for additional spending.

We have taken these concerns of LifeLabs into account. In particular, we note that no finding or conclusion we make is based solely on claims identified in third-party security assessment reports of LifeLabs' systems. The role the reports play is secondary in nature, providing further support or evidence for claims already indicated or established.

Yet, despite their secondary role, it is important to note that our decision to refer to such third-party reports was guided by the following additional considerations:

- depending on the methodology used—for example, staff interviews, threat and risk evaluations and/or audits against predefined criteria—each type of security assessment has its own strengths and weaknesses;
- the risk of ulterior motives is present in any type of assessment, even internal or noncommercial ones;

- a key advantage of third-party assessments over internal ones is that they offer an *independent* perspective; and
- the selection of third parties, including an assessment of their credibility, was solely at the discretion of LifeLabs.

The nature of the data breach and the method of intrusion used by the attackers were such that the deficiencies identified in LifeLabs' security were not limited to a single measure or control, but rather encompassed multiple layers of defense mechanisms, across various parts of the organization. They are as follows.

1. *The webservers were susceptible to compromise due to known and publicized critical vulnerabilities.*

The attackers were able to initially breach and gain a foothold into LifeLabs' network by exploiting a set of vulnerabilities in the Telerik UI for ASP.NET AJAX web application framework that LifeLabs used in its online appointment booking system (System D). The set of Telerik vulnerabilities—CVE-2017-9248, CVE-2017-11317 and CVE-2017-11357—were publicly disclosed in 2017. Each was given a base score of 9.8 (out of 10.0) on the Common Vulnerability Scoring System (CVSS) in the National Vulnerability Database maintained by the U.S. National Institute of Standards and Technology (NIST).[4] A CVSS score of 9.8 indicates a critical vulnerability, with high impact and relative ease of exploitation.

In May and June of 2019, respectively, the Australian Cyber Security Centre and Canadian Centre for Cyber Security issued public alerts about the vulnerabilities, notifying IT professionals of their active exploitation by threat actors.[5] In particular, the Australian advisory provided that, "The tools to exploit this vulnerability have been publicly published and require only basic skills or knowledge to use successfully." Despite the publicity and criticality of the vulnerabilities, LifeLabs was unaware of the developing threat landscape affecting it as an organization.

LifeLabs submitted that it would be unreasonable to conduct vulnerability management by means of either a manual search of or a subscription to the tens of thousands of CVEs contained in the NIST National Vulnerability Database. We generally agree with this point; however, it bears little or no relation to the discussion above. Our reference to the NIST

[4] See https://nvd.nist.gov/vuln/detail/CVE-2017-9248; https://nvd.nist.gov/vuln/detail/CVE-2017-11317; and https://nvd.nist.gov/vuln/detail/CVE-2017-11357.
[5] See https://www.cyber.gov.au/threats/advisory-2019-126 and https://cyber.gc.ca/en/alerts/active-exploitation-telerik-ui-aspnet-ajax.

National Vulnerability Database was made to establish the criticality of the specific vulnerabilities exploited by the attackers. We do not suggest that LifeLabs should have conducted a manual search of or been notified of every vulnerability in it.

However, the matter is different when it comes to national cyber security centres. These centres play an important role in educating security professionals and managers about active exploitation trends and other serious threats to information assets and technological infrastructure. We would expect an organization such as LifeLabs to subscribe to these targeted alerts or at least be aware of current trends. Yet, in the present case, LifeLabs was not.

2. *Patch management for the compromised webservers was inadequate.*

LifeLabs received two email security alerts from Telerik regarding the vulnerabilities exploited by the attacker. The first was on June 29, 2017, and the second was on September 1, 2017. Both security alerts described the vulnerabilities as "critical" and described various mitigation paths to address them, including:

- downloading and applying a security patch;
- upgrading to a newer version of Telerik; and/or
- preventing access to certain Telerik components.

LifeLabs responded to the first security alert and installed the recommended security patch on the webservers for System D on August 13, 2017. However, LifeLabs did not respond to the second security alert, as it was not aware of the alert's existence despite having received it.

The second email security alert was filtered into the junk mail folder of the LifeLabs staff member who, at the time, was registered to receive communications from Telerik as LifeLabs' representative on its Telerik license. The staff member was a software developer who was not part of the security team and was not required to respond to security alerts as part of their job duties. Despite this, they forwarded the first security alert to LifeLabs' Senior Manager of Software Development and Chief Information Security Officer (CISO), but was unaware of the existence of the second alert prior to the discovery of the breach. No one else at LifeLabs was registered to receive security alerts from Telerik.

Although LifeLabs installed the patch related to the first security alert, the second alert provided additional requirements and contained an important update to the original patch.

Without having put in place these additional security measures, LifeLabs' webservers for its System D remained susceptible to the vulnerabilities exploited by the attackers.

LifeLabs submitted that it would be unreasonable to expect a software developer who was not part of the security team to search their junk mail folder for vendor security alerts as part of their job duties. We agree; however, this only serves to underscore the deficiencies in LifeLabs' patch management for the compromised webservers. The very fact that a non-security staff member was registered to receive security alerts demonstrates the problematic nature of LifeLabs' patch management capabilities.

Moreover, LifeLabs was given an opportunity to improve its security patching process, but either did not recognize it or failed to address it. After the software developer received the first security alert and forwarded it to LifeLabs' Senior Manager of Software Development and CISO, LifeLabs should have recognized that critical security information was being sent to non-security personnel. At this point, LifeLabs should have updated its processes to ensure that future Telerik security alerts would be sent to the appropriate staff for resolution. However, LifeLabs continued with the status quo, thereby doing nothing to prevent the second security alert from ending up in the junk mail folder of a software developer with no security responsibilities.

The same deficiencies that led to LifeLabs' failure to respond to the second email security alert from Telerik were also identified by a number of third parties who reviewed LifeLabs' security practices. A 2017 threat-risk assessment, 2018 vulnerability assessment and 2019 gap assessment each described shortcomings in LifeLabs' patch management program, including:

a) no dedicated personnel for patch management;

b) no formalized patching process; and

c) no proactive patching of servers.

Indeed, in LifeLabs' initial response to our questions about vulnerability identification and patching, it was unaware that it had received and responded to the first security alert from Telerik and even installed a patch on the webservers for its System D. It was only after we followed up and explicitly asked about vendor-supplied security alerts that LifeLabs discovered this important information.

3. *The compromised webservers did not operate under a least privileges model.*

The machine accounts running the webservers were granted what is known as "local administrator" privileges. What this means is that the accounts had the technical ability to install software, change configuration settings, and access protected areas of the computer. Yet, this functionality was not required by the webservers to perform their tasks. By default, the attackers were granted the same level of privileges as the machine accounts after compromising the webservers. Using these elevated privileges, the attackers were then able to install additional offensive security tools and further escalate their privileges by copying domain administrator access tokens from processes in the computer's memory.

LifeLabs acknowledged that the compromised webservers did not operate under a least privileges model; however, it submitted that at the time of the breach other key applications and systems did. We do not consider this latter point relevant. Operating according to a least privileges model is a key security safeguard and the fact that LifeLabs had implemented that model for some systems demonstrates that it was aware of this. However, we find that it is not reasonable that LifeLabs did not apply this model to the compromised webservers at issue in this breach.

4. *Logging and monitoring of privileged accounts were insufficient.*

Until CrowdStrike's proactive security assessment, which was implemented in October 2019, LifeLabs did not log and monitor actions taken by individuals with administrator privileges. A project to implement a privileged access management (PAM) solution began in May 2019 and was initially scheduled for completion by the end of summer. However, the project was delayed and the schedule for completion postponed to the end of 2019.

LifeLabs submitted that it had logging enabled in System D to record various actions taken by customers, as well as both logging and monitoring enabled in other systems to identify staff who

attempted to access or modify sensitive data without having the required enhanced permissions. We do not consider these latter points relevant. Given that the attackers were able to escalate their privileges, the issue before us is the logging and monitoring of *privileged accounts*, not those of customers or staff without enhanced permissions.

In other documents reviewed by our offices, LifeLabs claimed to have other forms of logging and monitoring in place. For example, in an April 30, 2019 description of its security controls for the purposes of a SOC II audit, LifeLabs stated that, "All logs from all servers and appliances are collected and sent to SIEM [security information and event management]" and that, "Intrusion detection systems are in place to provide continuous

monitoring of LifeLabs' network and prevention of potential security breaches." Similar statements were made in an October 28, 2019 review of LifeLabs by the British Columbia Provincial Health Services Authority's Information Management/Information Technology Services. In addition, LifeLabs stated that it worked together with its SIEM system provider to review and enhance the log aggregation at multiple intervals over the years prior to and leading up to the breach.

However, we conducted a review of the alert records generated from the LifeLabs' SIEM system. Our review determined that there were no alerts that correlate to the time of the breach or to the method of intrusion used by the attackers.

A similar lack of SIEM capabilities was also identified by a third party who reviewed LifeLabs' security practices. A 2019 gap assessment described LifeLabs' SIEM system as "partially executed but not sufficient" and "not appropriate for the size and complexity of LifeLabs." As such, due to inadequate logging and monitoring of privileged accounts, there was a lack of capabilities to detect unauthorized activity, not to mention a lack of evidence to assist in investigating the breach.

5. *Network segregation was inadequate.*

At the time of the breach, the LifeLabs network was flat, allowing computers located in multiple sites access into any location within the environment. Assessments performed by third parties for LifeLabs in 2018 and 2019 noted that LifeLabs' network architecture was predominantly flat with minimal separation. This granted the attackers a greater attack surface and opportunity to move laterally. In our view, LifeLabs did not provide adequate network segregation to inhibit lateral movement across its network.

6. *Vulnerability scans were insufficient and/or used inadequate scanning tools.*

LifeLabs did not begin performing regular vulnerability scans of its systems until March 2019, with the first audits completed in April 2019. Before that, only a single third-party vulnerability assessment was conducted in June 2018. Both the third-party vulnerability assessment and

LifeLabs' own vulnerabilities scans used the same scanning tool engine. In each case, the tool failed to detect the vulnerabilities in the webservers exploited by the attackers.

LifeLabs submitted that the scanning tool was equipped with plug-ins to identify the Telerik vulnerabilities. However, the plug-ins failed to recognize the registry key required for them to detect the need to patch LifeLabs' version of Telerik UI for ASP.NET AJAX. As such, according to LifeLabs, more frequent and/or regular vulnerability scanning would likely not have resulted in identifying any of the Telerik vulnerabilities.

While this conclusion is correct, we disagree with its overall applicability to the issue before us. If one follows LifeLabs' argument to its logical conclusion, then it would have been reasonable for LifeLabs' to conduct *no amount* of vulnerability scanning, since the tool it used would not have detected the Telerik vulnerabilities anyway. This is an absurd conclusion.

In our view, a broader perspective is required. It is not enough to simply point to the fact that some form of vulnerability scanning was conducted. The scanning must be directed at the applicable systems using an adequate tool for the right amount of time. It is clear that LifeLabs failed to meet at least one of the latter two criteria.

7. *Level of security staffing was inadequate.*

Before June 2017, LifeLabs did not have any staff responsible for information security as a distinct role. In June 2017, it hired its first CISO. In 2018, it added three additional positions: Security Manager, Security Engineer and Security Analyst. Four staff dedicated to information security out of 5700 employees represents a mere 0.07% of LifeLabs' total workforce.

Concerns with the level of security staffing were also expressed by a number of third parties who reviewed LifeLabs' security practices. A March 2018 information security maturity assessment rated the maturity of LifeLabs' security program. It gave LifeLabs an overall "people" score of 1.15 (out of 5.0). A score of 0–1.0 indicates an ad-hoc maturity level described as "occasional, not consistent, not planned, disorganized." A score of 1.0–2.0 represents a repeatable maturity level described as "intuitive, not documented, occurs only when necessary." A December 2019 assessment came to a similar conclusion. It gave LifeLabs' security program a score of 2 (out of 5) for "resource management and staffing," rating it with a risk level of "high." Here, a score of 2 indicates a managed maturity level defined by "individual initiative; growing business, small operations." The assessment concluded that "Information Security activities are being performed by skilled and engaged staff performing multiple roles. There are too few resources assigned to plan, build and run an enterprise-wide Cyber Security Program."

We believe it unacceptable for an organization of LifeLabs' complexity and size, dealing with large volumes of sensitive personal health information across multiple systems and applications, to have had the level of security staffing that it did.

8. *File integrity monitoring was insufficient*

Prior to CrowdStrike's proactive security assessment, which was implemented in October 2019, LifeLabs did not monitor the webservers of System D for unauthorized modification or creation of files, including the type of malicious web pages uploaded by the attackers (web shells). As such, the attackers' means of access into LifeLabs' network remained undetected until the discovery of the breach.

In conclusion, for all of the above reasons, the ON IPC finds that LifeLabs did not take steps that were reasonable in the circumstances to ensure that personal health information in its custody or control was protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing personal health information were protected against unauthorized copying, modification or disposal, contrary to section 12(1) of PHIPA. For the same reasons, the ON IPC finds that LifeLabs did not ensure that the records of personal health information in its custody or under its control were retained, transferred and disposed of in a secure manner, contrary to section 13(1) of PHIPA.

The BC OIPC finds that LifeLabs did not make reasonable security arrangements as per section 34 of PIPA to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks to personal information in its custody or under its control.

Since the breach, LifeLabs has taken steps to address the gaps in the security of its systems and processes that were exploited by the attackers or contributed to their exploitation. We have reviewed the detailed list of information technology security improvements LifeLabs has made and, with the exception of one area, we are satisfied it has addressed all the deficiencies we identify above. A discussion of the steps LifeLabs has taken to remediate its systems and processes is provided in section 2.4.4 below.

However, there is one aspect of LifeLabs' response to the breach that, in our view, has not been sufficiently addressed by its remediation efforts. LifeLabs has not stated whether Telerik security alerts are now being sent to the appropriate staff on its security team for resolution. **As such, we order LifeLabs to:**

- subscribe the appropriate staff on its security team to Telerik's security notification list; and
- ensure that the staff are aware of their responsibilities to effectively monitor the list for security alerts.

2.4.2 Steps to Contain and Investigate Breach

The ON IPC and BC OIPC are satisfied that, once having discovered the breach, LifeLabs took reasonable steps to contain and investigate it. LifeLabs indicated that it did the following:

- On October 28, 2019, after being notified that an unknown source had triggered its monitoring system, it immediately initiated a review of what was reported and quickly confirmed that the behavior noted in the systems was abnormal;
- It immediately isolated the affected servers from its systems to protect the data and prevent additional unauthorized access;
- It ensured that the affected servers remained offline until they could be further secured and hardened; and
- It independently confirmed the method of intrusion claimed by the attackers and addressed the vulnerabilities used to access its systems.

Following the discovery of the breach, LifeLabs stated that it took additional measures to protect customer information, including the following:

- It immediately engaged cyber security experts to isolate and secure the systems and determine the scope of the breach;
- It took steps to further strengthen its systems to deter future attacks;
- It worked in collaboration with experts experienced in cyberattacks and in negotiations with cyber criminals to retrieve the data;
- It engaged law enforcement, which is currently investigating the matter; and
- It is offering cyber security protection services to its customers, such as identity and fraud protection insurance.

2.4.3 Risk Evaluation

The ON IPC and BC OIPC find that LifeLabs failed to appropriately evaluate the risk of harm to individuals whose personal health information and personal information were involved in the breach.

In its public notice, *An Open Letter to LifeLabs Customers,* posted on December 17, 2019 and updated on January 9, 2020, LifeLabs cited that their "cyber security firms have advised that the risk to our customers in connection with this cyberattack is low and that they had not seen any public disclosure of customer data as part of their investigations."

However, as noted in section 2.2.2 of this report, the information disclosed ranged from patient demographics, to actual laboratory results, to failed login and password pairs individuals may use for authentication to other websites and applications. Taken together, the harms that could result from malicious use of this information include identity theft, financial loss, fraud, blackmail or extortion, embarrassment or stigmatization of individuals, and misuse or appropriation of an individual's other online accounts.

Considering the nature of the personal health information and personal information involved in this breach, the known criminal intent of the attackers, and LifeLabs' inability to confirm the attackers' deletion of the information, it is our view that the risk of harm to individuals impacted by this breach is medium-to-high depending on the types of personal information or personal health information at issue.

While we are satisfied with the steps LifeLabs took to contain the breach, evaluating and reporting the breach as a low risk of harm to individuals does not adequately inform or prepare individuals of the actions they can take on their own to further mitigate the risk of harm (for example, changing passwords on other online accounts that may be associated with the failed login and password pairs).

While LifeLabs has made some effort to protect customers' personal information by offering credit monitoring and conducting their own monitoring of information sharing, there is no guarantee that the stolen information will not be misused in some future period.

2.4.4 Steps to Remediate Systems and Processes

In response to the breach, LifeLabs indicated that it implemented a number of measures to remediate its systems and processes, including that it:

- appointed a CISO and hired additional IT security staff to implement information security improvements;
- hired a new Chief Privacy Officer and Chief Information Officer;
- invested additional funds into its Information Security Management program;
- engaged an independent third-party firm to evaluate its response to the data breach and the effectiveness of its security programs and capabilities as well as to make recommendations for further process enhancements;
- continues to deploy cyber security firms to monitor the dark web and other online locations for information related to the data breach;
- established an Information Security Council with internal and external members who will regularly report to the CEO and the Board of Directors on information security practices and protocols;
- implemented strengthened data breach detection technology across the organization; and
- ensured that departments throughout the organization will participate in annual security and privacy awareness and training programs.

LifeLabs provided a more detailed list of its information technology security enhancements, which we do not set out here due to LifeLabs' security concerns. As discussed in section 2.4.1 above, we have reviewed the list and are satisfied that (with one exception) LifeLabs has taken reasonable steps to address the shortcomings in its technical security measures.

2.5 Issue 5: Policies and Information Practices

Sections 10(1) and 10(2) of PHIPA state:

> 10 (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations.
>
> 10 (2) A health information custodian shall comply with its information practices.

Section 2 of PHIPA states:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
>
> (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information

Section 5(a) of PIPA states:

> 5 An organization must
>
> (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act

At the beginning of their investigation, the ON IPC and BC OIPC asked LifeLabs to provide all policies and procedures in effect at the time of the breach relating to information security, identification of security vulnerabilities, security patch management and installation, intrusion detection, auditing and logging, anti-virus mechanisms, software development and procurement, identification management, and security incident response and escalation.

LifeLabs provided a series of policies that addressed these matters and stated that they were in effect at the time of the breach. However, when the ON IPC and BC OIPC questioned the CISO of LifeLabs under oath, he indicated that the policies were in draft form and were not in effect at the time of the breach and were not in effect at the time that the CISO was questioned.

LifeLabs stated that these polices were not in effect but "reflect LifeLabs' practices to a large extent" and then proceeded to explain the process by which the draft policies were developed. LifeLabs stated that they were first drafted in 2018 to reflect the processes followed within LifeLabs' information technology security group at that time. LifeLabs' current CISO then revised

the policies to incorporate additional then-current practices. Finally, LifeLabs stated that it is currently conducting a final review of these policies to ensure that they align with the ISO 27001 information security management framework that LifeLabs is working towards implementing.

A custodian or organization of LifeLabs' size, whose daily operations involve handling a large volume of personal health information, should have in place written information technology security policies that are in force. In this context, draft policies that have not been approved or implemented by the custodian or organization cannot be said to be a policy of the custodian or organization.

One reason the legislation requires custodians and organizations to implement information practices and policies is to ensure that compliance with PHIPA and PIPA is consistent, repeatable, and not *ad hoc*. Effective information technology security practices, in particular, can be complex, detailed, and multi-layered. It is not possible to execute such practices consistently and repeatably without having written policies in place that are in force.

LifeLabs also provided additional information about its current and historical privacy program, including information about its policies and information practices in relation to access and correction requests, complaints and inquiries, privacy impact assessments, privacy training, confidentiality pledges, and its overarching privacy policy and privacy risk management framework. LifeLabs is certainly correct in asserting that policies and procedures addressing these matters are necessary to comply with sections 10(1) and 10(2) of PHIPA and section 5(a) of PIPA. However, the fact that LifeLabs had such policies and procedures in place does not negate the fact that they did not have in-force information technology security policies in place. Such policies are equally required for compliance with those sections of the legislation.

Custodians and organizations must not only have and implement information practices and polices that comply with PHIPA and PIPA, but they must also be able to *demonstrate* to the ON IPC and BC OIPC that they comply. In the absence of information technology security policies that were in effect at the time of the breach, LifeLabs has not demonstrated, to the satisfaction of the ON IPC and BC OIPC, that it had implemented information practices and policies that complied with PHIPA and PIPA.

The ON IPC finds that LifeLabs did not have in place information practices that comply with the requirements of PHIPA, contrary to sections 10(1) and 10(2) of PHIPA.

The BC OIPC finds that LifeLabs did not have formal policies or practices in place to comply with their obligations under PIPA, contrary to section 5(a) of PIPA.

As such, LifeLabs is ordered to put in place comprehensive written information practices and policies that are in force and that set out safeguards that LifeLabs has implemented with respect to information technology security in order to comply with PHIPA and PIPA.

2.6 Issue 6: Collection of Unnecessary Personal Health Information and Personal Information

Section 30 of PHIPA states:

> (2) A health information custodian shall not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be.

Sections 11, 14 and 17 of PIPA state:

> Subject to this Act, an organization may [(s.11) collect, (s.14) use, or (s.17) disclose] personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> fulfill the purposes that the organization discloses under section 10 (1),
>
> or
>
> are otherwise permitted under this Act.

System D collected failed login and password pairs. The login and passwords were stored in plaintext. In response to the question of why LifeLabs stored failed password and log-in pairs and for what purpose, LifeLabs stated that it purchased System D from a third party and that this was the way the system was designed. LifeLabs states that it was not aware that this system collected this information and that it did not use this information for any purpose.

As there was no purpose for the collection of the failed login and password pairs, LifeLabs should not have collected them.

A similar deficiency was noted by a third party who reviewed LifeLabs' security practices. An April 2017 threat-risk assessment stated that, "LifeLabs does not perform due diligence prior to acquiring new companies and integrating their data, applications, systems etc. into its environment."

It is no excuse for a custodian or organization to say that it adopted a particular practice simply because it acquired software that performed that function as a default. A custodian or organization must conduct the necessary due diligence to ensure that any third-party software or systems that it acquires enable it to comply with its statutory obligations.

The ON IPC finds that LifeLabs collected more personal health information than was reasonably necessary to meet the purpose for which it was collected, contrary to section 30(2) of PHIPA.

The BC OIPC finds that LifeLabs collected more personal information than was appropriate for the purposes for which it was collected, contrary to section 11 of PIPA.

As such, LifeLabs is ordered to cease collecting failed login and password pairs and to securely dispose of the records of that information that it has collected.

2.7 Issue 7: Notice to Affected Individuals

Section 12(2) of PHIPA states:

> Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
>
> > (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
> >
> > (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

Unlike PHIPA, PIPA does not explicitly require organizations like LifeLabs to notify affected individuals where there has been a privacy breach through, for example, the theft or loss of their personal information. The BC OIPC considers that it is not necessary to decide here whether an organization's "reasonable security arrangements" duty under PIPA

includes a legal duty to notify affected individuals of a privacy breach in appropriate circumstances.[6]

In reaching this conclusion, the BC OIPC has considered the ON IPC's finding, and order, below about LifeLabs' compliance with the express notification duty under PHIPA. The BC OIPC also takes notice of the fact that the Office of the Information and Privacy Commissioner of Alberta has, under Alberta's *Personal Information Protection Act*—which contains express breach notification provisions—ordered LifeLabs to notify affected individuals in that province.[7]

The BC OIPC also notes, in passing, that its guidance on responding to privacy breaches recommends that organizations should notify affected individuals where there is a risk of harm tothem, to help them avoid or mitigate the risk.[8] The guidance gives examples of the kinds of harm that can warrant notification, such as identity theft, risk to individual safety, or hurt, humiliation or damage to reputation. The guidance notes that hurt, humiliation or damage to reputation can be associated with a breach of medical information.

1. Public and Direct Notification of LifeLabs Customers

On December 17, 2019, LifeLabs issued a public notice on its website, *An Open Letter to LifeLabs Customers,* regarding the breach. The open letter was updated on January 9, 2020. LifeLabs has stated that the delay between discovery of the breach and the commencement of LifeLabs' notification of affected individuals was due to the fact that LifeLabs required this time to secure its systems against future attacks.

LifeLabs took out paid advertising in more than 100 local newspapers in British Columbia and Ontario, with notices regarding the breach. LifeLabs responded to more than 40 media inquiries, and the President and Chief Executive Officer conducted 8 media interviews. In addition, LifeLabs created a dedicated microsite and call centre to disseminate information about the breach and to answer questions from the public.

[6] An express notification duty is long overdue in British Columbia. The BC OIPC has for this reason recently submitted to a special committee of the British Columbia Legislature that PIPA should be updated to address this: Briefing for the Special Committee of the Legislature to Review the *Personal Information Protection Act* (June 2, 2020). https://www.oipc.bc.ca/special-reports/2426.
[7] *LifeLabs Inc.*, P2020-ND-036. https://www.oipc.ab.ca/media/1079221/P2020-ND-036014221.pdf. The notification duty under Alberta's Personal Information Protection Act arises where there is a "real risk of significant harm" to affected individuals.
[8] Privacy Breaches: Tools and Resources. https://www.oipc.bc.ca/guidance-documents/1428.

LifeLabs faxed notices regarding the breach to more than 56,500 healthcare providers and other clients with whom it had contractual relationships.

At its Patient Service Centres in British Columbia, Ontario and Saskatchewan, LifeLabs posted notices, displayed information on television screens, and distributed 76,000 information cards regarding the breach.

LifeLabs is offering one year of a credit monitoring service that includes dark web monitoring and identity theft insurance to any customer who requests it through a 1-888 call centre.

LifeLabs sent direct notifications regarding the breach by email to customers registered for its "Online Appointment Booking" website. LifeLabs also sent direct notifications by email to customers registered for the "my ehealth" (British Columbia only) or "my results" (Ontario only) websites.

In these email notifications, LifeLabs identified that the affected information could include name, address, email, logins, passwords, date of birth, health card numbers, gender, telephone numbers, password security questions, and laboratory test results.

However, these emails did not identify specifically which of these data elements were impacted for each individual. These notifications did state that "this message does not mean that you are one of the approximately 85,000 laboratory test customers impacted" and that LifeLabs would notify these customers separately.

LifeLabs required all customers with accounts on the Online Appointment Booking system to reset their passwords.

In the emails to "my ehealth" and "my results" account holders, LifeLabs indicated that the "my ehealth" and "my results" websites were not compromised in the breach. However, LifeLabs also required customers who had used the same email address in the "my ehealth" or "my results" systems as in the Online Appointment Booking system to re-set their passwords.

In total, LifeLabs sent direct notices to approximately 3 million customers for whom it had email addresses.

LifeLabs identified 131,957 individuals whose test orders (that is, the type of test that was ordered for the individual) were compromised in the breach. Of these, LifeLabs identified 84,533 individuals whose actual test results were compromised (ie. "the approximately 85,000 laboratory test customers" that LifeLabs referred to in its public and direct notices).

LifeLabs sent direct notifications by email to approximately 41,000 patients whose laboratory test results or orders were compromised. These are all of the individuals within these compromised data sets for whom LifeLabs has an email address. These individuals may have received both an email notifying them of the breach as well as the email notifying them that their test results or orders were compromised.

LifeLabs has stated that it has and will continue to directly notify by mail approximately 46,000 additional patients whose test results or orders were compromised after taking steps to validate the mailing addresses that LifeLabs has for these patients.

LifeLabs has also stated that it has and will continue to notify the other individuals whose laboratory results or orders were compromised through their referring health care providers. LifeLabs has indicated that its work to complete these notifications has been slowed by the fact that both LifeLabs and the referring health care providers have needed to focus on matters related to the COVID-19 response.

If an individual contacts LifeLabs' call centre, after validating the individuals' identity, the call centre is able to confirm whether the individual is one of the individuals whose laboratory test results or orders were compromised.

If individuals whose test results or orders were not compromised contact the call centre, LifeLabs does not inform the individual of what specific data elements of their personal health information were compromised. Instead, LifeLabs has stated that an individual must make an access request through the LifeLabs' privacy office to obtain this information.

2. Notification to individuals who have never attended at a LifeLabs Service Centre

In January 2020, Trillium Health Partners (Trillium) contacted the ON IPC to discuss its obligations with respect to notifying patients about the LifeLabs breach. LifeLabs has a Services Agreement with Trillium to provide "referred-out esoteric testing" services to Trillium. The ON IPC understands this to mean that instead of performing certain tests in-house, Trillium "refers" them out to LifeLabs and LifeLabs then sends the results back to Trillium. The ON IPC understands that this typically applies to rare or low-volume tests that require specialized technologies or skills. Trillium expressed concern that some of its

patients might not be aware that their personal health information was held by LifeLabs and may have been affected by the breach. The ON IPC requested and received a copy of the Services Agreement from both Trillium and LifeLabs.

One clause of the Services Agreement defines LifeLabs as an agent of Trillium pursuant to section 2 of PHIPA. The Services Agreement also states that LifeLabs agrees to receive personal health information from Trillium as part of LifeLabs' provision of services to Trillium and not on LifeLabs' behalf or for LifeLabs' own purposes. However, LifeLabs takes the position that there are conflicting clauses in the Services Agreement. It points to provisions of the Services Agreement that preclude either party from acting as an agent to the other. LifeLabs also points to clauses in the Services Agreement that dictate that LifeLabs controls the personnel, equipment and tools, quality control, testing processes, and subcontractors used to provide the services.

Section 2 of PHIPA states:

> "agent", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.

Section 17(4)(b) of PHIPA states:

> (4) An agent of a health information custodian shall,
>
> [...]
>
> (b) notify the custodian at the first reasonable opportunity if personal health information that the agent collected, used, disclosed, retained or disposed of on behalf of the custodian is stolen or lost or if it is used or disclosed without authority.

Section 17(4)(b) of PHIPA requires an agent to notify a health information custodian if personal health information that the agent collected, used, disclosed, retained or disposed of on behalf of the custodian is stolen or lost or if it is used or disclosed without authority. It is then the obligation of the health information custodian to determine whether it has an obligation to notify the individual of the breach.

LifeLabs takes the position that it is not an agent to Trillium. It states that it "independently collects, uses, and discloses personal health information [...] in its custody and control". LifeLabs further states that "when LifeLabs collects [personal health information] from a patient within Trillium, it is not the intention that Trillium[...] be the decision maker and direct how LifeLabs processes, stores or discloses it."

Notwithstanding LifeLabs' assertions, given the conflicting provisions of the Services Agreement, and the concerns expressed by Trillium, the ON IPC is not satisfied that LifeLabs is not an agent of Trillium, as that term is defined in PHIPA.

However, LifeLabs has established to the ON IPC's satisfaction that personal health information that it holds pursuant to its agreement with Trillium was not among the data sets that were compromised in the breach.

The ON IPC asked LifeLabs whether any personal health information that it held as an agent of any other health information custodian in Ontario was compromised in the breach. LifeLabs responded that it is not an agent to any other custodian in Ontario, for the same reasons that it set out with respect to Trillium.

The ON IPC asked LifeLabs to provide representations regarding how patients of LifeLabs customers, who may never have attended at a LifeLabs Patient Service Centre, would be notified of the fact that their personal health information could have been compromised in the breach.

LifeLabs acknowledged that some individuals may not have been aware that LifeLabs was the organization conducting their test. LifeLabs stated that it endeavoured in its public notifications to indicate that individuals may have been affected by the breach even if they had not attended at a LifeLabs Patient Service Centre. LifeLabs pointed to the micro-site that it published regarding the breach and noted that under the tab "Am I Impacted?" it states:

> The majority of individuals potentially affected are located in BC and Ontario and visited LifeLabs for medical testing or other locations like hospitals, medical clinics, private and public lab providers across BC and Ontario that send testing to LifeLabs.

LifeLabs also provided a copy of a notice that it ran in newspapers that contained similar language.

In addition, LifeLabs provided the ON IPC with a copy of the letter that it sent to health information custodians in Ontario with whom it had contractual agreements for laboratory testing services that stated:

> Note some patients may not be aware that LifeLabs provided them with service and we are requesting your assistance by posting the notice enclosed with this message.
>
> [...]
>
> LifeLabs has prepared the attached poster to inform customers of what happened and cyber security protection services that are available to them.
>
> **Please post this information as appropriate to inform your patient population that they may be affected.** [emphasis in original]

The enclosed notice that the health information custodians were asked to post indicates that LifeLabs completes diagnostic testing for patients of the health information custodian and sets out other information about the breach and how to contact LifeLabs.

3. Analysis

Section 12(2) of PHIPA does not require a particular type of notification. The ON IPC Guidance Document *"Responding to a Health Privacy Breach: Guidelines for the Health Sector"* (Breach Guideline) states that there are many factors to consider when deciding on the best form of notification and acknowledges that notification may be done in a variety of ways—for example, by telephone, in writing, or in person. The Breach Guideline also acknowledges that there may be exceptional circumstances where direct notification is not possible.[9]

In this case, LifeLabs does not have contact information for all individuals who have been affected by the breach. In many cases, laboratory results are sent to the individual's physician who ordered the tests and not directly to the individual. Therefore, it is understandable that LifeLabs would not have contact information for every patient who has received a test from it.

[9] *Responding to a Health Privacy Breach: Guidelines for the Health Sector*, Information and Privacy Commissioner of Ontario, page 2.

Indeed, LifeLabs stated in its representations that, in accordance with data minimization principles, it did not collect contact information for individuals if it was not necessary to provide services to the individual.

LifeLabs does have contact information in the form of an email address for individuals who registered on the Online Appointment Booking, my ehealth, or my results website because an email address is necessary to use these services.

In addition, this breach affected millions of individuals, making direct notification of each individual very difficult.

The ON IPC is satisfied that LifeLabs has or will be directly notifying those individuals for whom it has validated contact information. Given the magnitude of the breach combined with the fact that

LifeLabs does not have contact information for every affected individual, the ON IPC is satisfied that it was not possible to notify every individual directly.

LifeLabs has undertaken an extensive public notification campaign. While this does not guarantee that every affected individual will be notified in the same way as a direct notification, LifeLabs also established a dedicated call centre that individuals can call to receive more information about the breach. As such, based on the particular factual circumstances in this case, the ON IPC is satisfied with respect to LifeLabs' decision to notify individuals through a combination of public and direct notification and is satisfied that its decision to conduct a broad public notification campaign and to offer the credit monitoring services to *any* customer who requests it was a reasonable one in the circumstances.

As noted above, some of the complaints made to the ON IPC were about the service received from the LifeLabs call centre. Assuming these complaints to be accurate, they were limited in number and the ON IPC does not see them as establishing a systemic failure in LifeLabs' notification efforts. Some individuals who contacted the ON IPC stated that LifeLabs should have offered the credit monitoring service for longer than one year. The ON IPC recommends that LifeLabs consult with independent third-party experts with respect to whether a longer period of credit monitoring service would be more appropriate in the circumstances of this breach.

With respect to Trillium, LifeLabs has satisfactorily established that personal health information that it holds pursuant to its agreement with Trillium was not among the datasets

that were compromised in the breach. LifeLabs notified health information custodians with whom it had contractual agreements that some patients may not be aware that LifeLabs provided them with service and instructed the custodians to post a sign notifying their patients of this fact. In addition, in its notifications to the general public, LifeLabs stated that it serves customers on behalf of hospitals, medical clinics, private and public laboratory providers in addition to LifeLabs Service Centres. Therefore, in the specific circumstances of this case, the ON IPC is satisfied with the steps LifeLabs took to ensure that even individuals who had never attended at a LifeLabs Service Centre were notified of the breach. Given this, the ON IPC finds it unnecessary to make a finding about whether LifeLabs' is acting as an agent to Trillium or other health information custodians in Ontario with whom it has a similar contractual relationship.

Given all of the above, the ON IPC is satisfied with the *manner* in which LifeLabs notified affected individuals of the breach.

However, with respect to the *content* of the notification, the Breach Guideline also states that when notifying individuals affected by a privacy breach, a health information custodian should provide a description of the personal health information that was subject to the breach.[10] With the exception of the individuals whose test results or orders were compromised, other affected individuals were notified of *all* of the categories of personal health information that were compromised in the breach, but <u>not</u> specifically which categories of *their* personal health information were compromised.

In addition to transparency and accountability, one reason for the requirement to notify individuals if their personal health information is breached is so that individuals can take appropriate steps to protect themselves from any harms that may result. In order to do this, the individual generally needs to know specifically what information was breached. It is LifeLabs' obligation to provide this information to affected individuals.

Since LifeLabs relied in part on public notifications, which cannot, by their nature, inform each individual specifically what of their personal health information was compromised, it follows that some individuals would have to contact LifeLabs to obtain more specific information. However, to require an individual to make a formal written access request under Part V of PHIPA is unduly onerous. It requires an individual to go to significant effort to obtain information that they are already entitled to receive.

[10] *Ibid*.

In summary, LifeLabs has not implemented a process to notify all individuals what of their personal health information was stolen, lost, or used or disclosed without authority without the individual having to make a formal access request pursuant to Part V of PHIPA. Therefore, LifeLabs has not complied with its obligation to notify affected individuals of the breach at the first reasonable opportunity, contrary to section 12(2) of PHIPA.

As such, LifeLabs is ordered to implement a process to notify all individuals what of their personal health information was compromised by the breach without the individual having to make an access request pursuant to Part V of PHIPA.

Finally, the ON IPC has issued numerous decisions under PHIPA emphasizing how important it is that the role and status of health information custodians, their agents, and other regulated parties under PHIPA be clearly defined in formalized agreements.[11] This is important because the respective obligations of the parties flow from their status under PHIPA. This impacts all the parties' obligations with respect to safeguarding the personal health information, making decisions about its collection, use and disclosure, responding to access and correction requests, and, as illustrated in this case, notifying individuals if their personal health information has been breached. In this case, we find that LifeLabs' contractual arrangement with Trillium is inadequate in defining the parties' respective roles and responsibilities under PHIPA.

As such, LifeLabs is ordered to clarify and formalize its status under PHIPA with respect to its contractual relationships with Trillium and any other health information custodian in Ontario with whom it has a similar relationship.

3 ORDERS AND RECOMMENDATIONS

For the reasons given above, the Information and Privacy Commissioner of Ontario makes the following orders under section 61(1) of PHIPA and the Information and Privacy Commissioner of British Columbia makes the following orders under section 52(3) of PIPA.

ORDER 1

[11] See, e.g. PHIPA Decision 102, PHIPA Decision 62, PHIPA Decision 50.

LifeLabs is ordered to:

- subscribe the appropriate staff on its security team to Telerik's security notification list; and
- ensure that the staff are aware of their responsibilities to effectively monitor the list for security alerts.

ORDER 2

LifeLabs is ordered to put in place comprehensive written information practices and policies that are in force and that set out the safeguards that LifeLabs has implemented with respect to information technology security in order to comply with PHIPA and PIPA.

ORDER 3

LifeLabs is ordered to cease collecting failed login and password pairs and to dispose of the records of that information that it has collected.

For the reasons given above the Information and Privacy Commissioner of Ontario also makes the following orders under section 61(1) of PHIPA.

ORDER 4

LifeLabs is ordered to implement a process to notify all individuals of what of their personal health information was compromised by the breach without the individual having to make an access request pursuant to Part V of PHIPA.

ORDER 5

LifeLabs is ordered to clarify and formalize its status under PHIPA with respect to its contractual relationships with Trillium and any

other health information custodian in Ontario with whom it has a similar relationship.

LifeLabs must comply with the above orders 1 through 4 by August 7, 2020 and with order 5 by February 7, 2021. These timelines may be extended if LifeLabs is unable to comply in light of the current COVID-19 situation.

In addition to the orders, we also make one recommendation.

RECOMMENDATION 1
It is recommended that LifeLabs consult with independent third-party experts with respect to whether a longer period of credit monitoring service would be more appropriate in the circumstances of this breach.

June 25, 2020

Original Signed by:

Brian Beamish
Information and Privacy Commissioner of Ontario

Original Signed by:

Michael McEvoy
Information and Privacy Commissioner for British Columbia