1. **What happened?**

   Through the proactive surveillance of our IT systems, LifeLabs recently identified a cyber-attack involving unauthorized access to our computer systems. Our investigations to date indicate that the affected systems contained customer information that could include name, address, email, birth date, login, password, health card number and lab results.

   Safeguarding our data is critical to our customers and it is a priority for LifeLabs. Immediately upon discovering the incident we engaged world-class cyber security experts to isolate and secure the affected systems, and determine the scope of the breach.

   At this time, our cyber security firms have advised that the risk to our customers in connection with this cyber-attack is low and that they have not seen any public disclosure of customer data during their investigations, which include monitoring of the dark web and other online locations. We have engaged law enforcement, and their investigation is underway.

2. **How many customers have been impacted? Were lab tests impacted?**

   There is information relating to approximately 15 million customers on the systems that were potentially accessed in this breach. In the case of lab test results, our investigations to date of these systems indicate that there are 85,000 impacted customers from 2016 or earlier located in Ontario; we will be notifying these customers directly. Our investigation to date indicates any instance of health card information was from 2016 or earlier.

3. **How has LifeLabs responded to the breach?**

Following discovery of the breach, LifeLabs has taken several measures to protect customer information:

- We immediately engaged world-class cyber security experts to isolate and secure the systems, and determine the scope of the breach;
- We are taking steps to further strengthen our systems to deter future attacks;
- We retrieved the data by making a payment. We did this in collaboration with experts who are experienced in cyber-attacks and in negotiations with cyber criminals;
- We engaged law enforcement, which are currently investigating the matter; and
- We are offering cyber security protection services to our customers, such as identity and fraud protection insurance.

4. **When did you find out about the breach?**

   LifeLabs' proactive surveillance identified the attack at the end of October 2019. We immediately launched investigations using world-class cyber security experts. In mid-November these experts advised us of the potential extent of the breach.

5. **Why are you notifying customers now?**

   Before notifying our customers of the breach, it was essential to conduct a thorough investigation into what happened to secure our systems, and determine the scope of the breach to ensure that we could inform all affected individuals with the most accurate and up to date information on what happened.

   We set up a microsite with information about how customers can take appropriate steps to protect themselves by signing up for cyber security benefits. During this time, we have also been working with our government partners and notified the respective privacy commissioners. We have also engaged with law enforcement, who are currently investigating the matter. Over the coming weeks we will continue a mass notification through public channels to notify our customers.

6. **What kind of information was affected by the breach?**

   Investigations indicate that the affected systems contain personal health information (PHI) of our customers, including name, address, email, customer logins and passwords, health card numbers, gender, phone number, password security questions and lab tests.

7. **Are my test results and information safe?**

   So far, our cyber security firms have not seen any public disclosure of customer data in their investigation and surveillance of the dark web and other online sources. However, we want to provide peace of mind to our customers who may be concerned, so we are offering cyber security protection services.

8. **What services are you offering to protect my information/data?**

   We are offering our customers cyber security protection for one year from TransUnion, which includes credit monitoring and fraud insurance protection. These services will give customers:

   - Unlimited online access to the TransUnion Credit report, updated daily.
     - A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
   - Unlimited online access to the TransUnion CreditVision® Risk score, with score factors and analysis updated daily.
     - A credit score is a three-digit number calculated based on the information contained in a consumer's credit report at a particular point in time.
   - TransUnion credit monitoring alerts with email notifications to key changes on a consumer's credit file to protect against identity theft and enable quick action against potentially fraudulent activity.
   - Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.

- Identity theft insurance of up to $50,000 in coverage to protect against potential damages related to identity theft and fraud.

You can activate these services by calling one of the following numbers to receive a unique activation code to register for these services online.

- **1-888-918-0467**

Please note that accepting the offer of credit monitoring does not prevent a customer from participating in any class action, if certified.

9. **Is your system working properly right now?**

   Yes. Our patient service centres, online booking and all operations are currently open for service.

10. **Should I change my password to my appointment booking or test results portal?**

    While our investigations to date indicate that our online test result portals were not impacted by this breach, our appointment booking system was; we will be directly notifying affected customers. Although we have isolated the affected servers and eliminated the unauthorized access, as a best practice, customers who are registered users for LifeLabs' online services should continually update their passwords regularly so they are strong, complex and unique. To reset your password please click **here. < https://www.lifelabs.com/contact-us/password-reset/>**

11. **How do I know that my tests were done at LifeLabs? How do I know if my health information is in your database?**

    The vast majority of LifeLabs' customers are in B.C. and Ontario. There are relatively few customers in other locations. If you have visited a LifeLabs for a test or received a test/service from LifeLabs Genetics and Rocky Mountain Analytical, then it is likely your information is in our database.

12. **Have affected customers been notified?**

In the interest of transparency, and as required by privacy regulations, we are making this announcement and notifying customers through public channels.

13. **Is the issue contained? Are you sure that any other systems haven't been compromised?**

    Yes, the issue has been contained. However, the investigation is still under way, and with the help of multiple leading cyber security firms, we are implementing further safeguards to protect our customers' information and reduce the risk of future attacks. We are also monitoring the dark web and other online locations, and so far, we see no indications of unauthorized use or disclosure of customer data.

14. **How do I get in contact with a privacy commissioner to learn about my rights?**

    While you are entitled to file a complaint with the privacy commissioners, we have already notified them of this breach and they are investigating the matter. Customers who have questions about their rights can learn more by contacting the privacy commissioner in their respective province.

15. **How will you notify the 85,000 customers from January 2016 or earlier located in Ontario whose test results were impacted?**

    If you have visited a LifeLabs location, it is possible your information may have been accessed without authorization as per the public notice on customernotice.lifelabs.com. If you are among the 85,000 customers from January 2016 or earlier located in Ontario whose test results were impacted; we will notify you directly. This direct notification will occur in the coming weeks, we are working with our partners to make that happen.

16. **Is LifeLabs offering credit monitoring for minors?**

    Yes; please provide your contact information to **LifeLabs' Privacy Office** for follow up.

Up ↑

https://www.lifelabs.com/terms-of-use/> | Cookie Policy < https://customernotice.lifelabs.com/cookie-policy/>