SNC·LAVALIN

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Submitted via email

September 18, 2019

Dear Sir/Madam:

We write to you to inform you of a cybersecurity incident at SNC-Lavalin Inc ("SNC-Lavalin," "we" or "our").

While this incident has primarily impacted data of employees, former employees and job applicants in Canada, it has been identified in the course of the investigation that the personal data of certain individuals in the United States is impacted, or may be impacted, by this incident.

While our investigation is ongoing, at this time, the evidence suggests that this incident involves the personal data of approximately five (5) New Hampshire residents.

When, how and why did the incident occur?

Between August 19th and September 3rd, 2019, an unauthorized actor tried to compromise Office 365 accounts of SNC-Lavalin employees. The unknown actor successfully accessed the account of one employee who was on leave.

As part of the SNC-Lavalin investigation and triage process, the mailbox is currently being reviewed by a dedicated team of investigators supported by our Data Protection Officer and Legal Team. This deep review includes an assessment of the extent of personal data and the affected individuals contained therein.

At this time, we have no evidence to suggest this account was specifically targeted.

When was the incident discovered?

The incident was discovered by our Global Security staff on September 3, 2019. At that time, we promptly initiated an investigation.

Where did the incident occur?

The affected employee's mailbox was hosted on Office365 servers in Quebec, Canada.

What safeguards did SNC-Lavalin have in place at the time of the incident?

At the time of the incident, SNC-Lavalin had several technical and organizational security controls, policies, and processes in place to protect its IT equipment, systems and data. The SNC-Lavalin user accounts were protected through various measures including:

- the Microsoft Password Protection Service, which prevents pre-determined passwords being used, including those that are easy to guess; and,

- SNC-Lavalin utilizes Multi-Factor Authentication (MFA) for cloud-hosted applications.

Unfortunately, due to the affected SNC-Lavalin employee being on extended leave, MFA had not been rolled out to the compromised Office 365 account at the time of the incident. Since the incident, the account has now been enrolled in SNC-Lavalin's MFA solution.

What personal information is affected?

The employee whose account was affected works in HR and handles personal data related to employees, former employees, and job applicants. At this time, we have evidence the data in the mailbox included: Name, Home Address, Personal Contact Details, Emergency Contacts, Substance Misuse Assessment Applications, Bank Account Details, and Government ID documentation (including copies of passports, driver's license, and SSN numbers). While this information is stored securely within our HR systems, we have identified that it is also contained within attachments to e-mail stored in the affected mailbox.

Has SNC-Lavalin notified the affected individuals?

SNC-Lavalin is providing notice to affected individuals on September 18, 2019. SNC-Lavalin is providing two years of credit monitoring for affected individuals via Experian.

Strengthening our security position

To help prevent a similar incident from occurring in the future, SNC-Lavalin is enhancing the security and monitoring of its environment and is working to implement further measures to prevent future unauthorized access to its Office 365 environment, as well as further enhance its IT security generally.

Affected individuals

As set out above, we do not have evidence that the personal data of any individual has been exfiltrated. However, out of an abundance of caution, we wish to inform the individuals of what happened and provide them with the ability to implement protective measures directly. Those protective measures include: (1) understanding what data has been exposed; (2) ID theft insurance; (3) credit monitoring; and, (4) a contact number so that we can continue to support them with advice and information as needed.

Who is your point of contact for this investigation?

Mr. Andrew Cox
Head of Data Privacy and Data Protection Officer
+44 1454 663466
Data_Privacy@snclavalin.com

Please allow me to take this opportunity once again to reassure you that a well-resourced investigation is underway and the affected individuals are our primary concern. We will at all times cooperate with you openly in order to assist you and all individuals affected by this unfortunate incident. Please do not hesitate to contact me if I can assist further.

Sincerely,

Andrew Cox
Head of Data Privacy and Data Protection Officer SNC-Lavalin

USA

On company letterhead

[Insert name and contact information]

Re: *Notice of potential breach of employee personal information*

DATE

Dear [insert name],

We are contacting you to inform you that your personal information may have been compromised as a result of a cyber security incident at SNC-Lavalin.

What happened?

On September 3, 2019, we discovered that an unknown and unauthorized third party had tried accessing user accounts on August 19, August 27 and September 3, and had gained access to the mailbox of one of our employees, which contained personal information.

As soon as we discovered the unauthorized access, we acted immediately to stop the intrusion and restore security to the impacted account.

We promptly engaged a significant amount of internal and external resources to conduct a comprehensive and wide-ranging forensic review to determine the scope of the intrusion, including the data that may have been compromised as a result of the incident. At all times, the priority of the investigation was to assess the risk to individuals in order to notify those impacted as soon as possible and continue to protect the data that we hold.

Our investigation has determined that the compromised mailbox contained documents and/or references related to former and current employees. The information we identified relevant to you may include personal and sensitive information such as name, employee number, job role information, birth date, social security number, addresses, salary, personal financial information, ID cards, driver's licences or passports.

Protecting your personal data

Although we have evidence that the mailbox was accessed, we do not have evidence that your personal data was removed or, indeed, that any personal data was removed.

However, we wish to notify you of the position so that you can take action to reduce the risk of potential harm associated with this incident. In addition to any steps that you wish to take, which should include increased vigilance around where your data is or has been used, we are providing you with two (2) years of free credit monitoring and identify theft restoration services.

Your subscription to Equifax ID Patrol includes:

- **3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, TransUnion® and Experian® credit reports**
- **Access to your Equifax credit report**
- **One Equifax 3-Bureau credit report**

- **Wireless alerts (available online only). Data charges may apply.**
- **Automatic Fraud Alerts[2]. With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).**
- **Credit Report Lock[3] Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.**
- **Internet Scanning[4] Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.**
- **Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID**
- **Up to $1 MM in identity theft insurance[5]**
- **Live agent Customer Service 24x7**
- **Identity Restoration - If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity. To be eligible for Identity Restoration, you must complete the enrollment process for the subscription offer by the enrollment deadline above. Call the phone number listed in your online member center for assistance.**

We urge you to sign up for the service as soon as possible. Your unique enrollment code (provided below) will expire on December 31, 2019.

To enroll, please visit myservices.equifax.com/patrol

Enrollment Code: <activation code from file>

Additional Information

We regret that you may have been affected by this incident and we understand that you may have questions or concerns. We have established a toll-free number specifically dedicated to employees affected by the incident. You may call 1-833-451-8809, from 9:00 am to 5:00 pm EST, Monday to Friday, if you wish to speak to someone.

We also recommend that you remain vigilant about suspicious activity involving your personal information in the upcoming months. As a matter of best practice, you should frequently review your credit report and credit card, bank and other financial statements for evidence of any unauthorized activity.

If you have reason to believe your information has been used for fraudulent purposes, we strongly recommend you contact your local police department and your national anti-fraud centre.

You should also remain vigilant about any calls, emails or letters you receive from an unfamiliar person or organization who is providing you with your own personal information in order to earn your trust. Credible organizations should never contact you directly and ask you to provide personal information. If you are contacted by an unidentified third party, do not provide any additional personal information and do not use any telephone number or email address they may provide. You should report any such suspicious activity to your local police department.

We want you to know that SNC-Lavalin values your privacy and takes this incident very seriously. In addition to the security enhancements already implemented, we will continue to look for opportunities to further strengthen and enhance our security infrastructure. Additionally, as part of our commitment to integrity and our obligations under the law, we have also notified appropriate privacy regulators.

Please don’t hesitate to call the toll-free number if you have any questions or concerns.

Sincerely,

Ian L. Edwards
Interim President and CEO

[1]Credit monitoring from Experian® and Transunion® will take several days to begin.

[2]The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3]Locking your Equifax credit file with Credit Report Control will prevent access to your Equifax credit file by certain third parties, such as credit grantors or other companies and agencies. Credit Report Control will not prevent access to your credit file at any other credit reporting agency, and will not prevent access to your Equifax credit file by companies like Equifax Global Consumer Solutions which provide you with access to your credit report or credit score or monitor your credit file; Federal, state and local government agencies; companies reviewing your application for employment; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; for fraud detection and prevention purposes; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4]Internet scanning will scan for your Social Security number (if you choose to), up to 5 bank accounts, up to 6 credit/debit card numbers that you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet Scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guaranteed that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[5] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

Experian® and TransUnion® are registered trademarks of their respective owners. Equifax® and ID Patrol® are registered trademarks. ©2017 Equifax Inc., Atlanta, Georgia. All rights reserved.