Exhibit H

Compliance Letter to the Office of the Privacy Commissioner of Canada ("OPC") by Nova Scotia Power

Source: Office of the Privacy Commissioner of Canada

URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2026/2026-ns-power-ca/

Retrieved: July 11, 2026

Signed at Halifax, Nova Scotia, March 18, 2026

Full Document Content

General Terms

1. The Privacy Commissioner of Canada ("the Commissioner") oversees compliance with the Personal Information Protection and Electronic Documents Act ("PIPEDA" or the "Act"), which governs the collection, use and disclosure of personal information by private-sector organizations in the course of commercial activities.

2. Nova Scotia Power has agreed to fulfil the commitments set out in this Compliance Letter (this "letter") at the request of the Commissioner. In this letter, Nova Scotia Power confirms the actions that it has already taken to further safeguard personal information since the privacy breach that occurred starting on or around March 19, 2025 ("the breach") and commits to provide additional information and to perform certain additional tasks in relation to the breach.

3. Upon the Commissioner being satisfied that Nova Scotia Power has fulfilled all of the commitments set out in this letter, the investigation relating to the breach (the "investigation") will be discontinued in accordance with paragraph 12.2(1)(c) of PIPEDA, on the basis that the organization will have provided a fair and reasonable response. The Commissioner retains the discretion to continue the investigation or to initiate a complaint under subsection 11(2) of PIPEDA should he deem that Nova Scotia Power has not fulfilled the commitments set out in this letter or if new privacy concerns are brought to the Commissioner's attention in relation to this matter.

4. The Commissioner may request information and documents from Nova Scotia Power for the purpose of verifying that the organization is fulfilling the commitments it has made in this letter.

5. The Commissioner may seek further commitments from Nova Scotia Power following review of any additional information that he receives on the matter.

6. This letter, or part thereof, may be disclosed or made public by the Commissioner under ss. 20(2) of PIPEDA.

7. For greater certainty, nothing in this letter shall prevent or otherwise limit the Commissioner from exercising or performing any of his powers and duties under the Act.

8. This letter is not intended as, or to be construed as, an admission of liability or wrongdoing by Nova Scotia Power.

Incident Overview

The facts of the breach, as they are known on the date of signature of this letter, and as confirmed by Nova Scotia Power, are as follows:

Breach Timeline

- On or around March 19, 2025, a Nova Scotia Power employee visited a website that had been compromised by the "SocGholish" (FakeUpdates) malware. The employee clicked on a link in a pop-up on that site, which resulted in malware being downloaded and installed on Nova Scotia Power's systems. The malware created a background process and downloaded additional malware. This allowed the threat actor to gain access to Nova Scotia Power's systems and network.

- On or around April 8, 2025, the threat actor began to move laterally across systems in the Nova Scotia Power network environment, using accounts with domain administrator privileges. Between April 8 and April 22, 2025, the threat actor deployed and leveraged additional malware to perform internal reconnaissance and credential harvesting activities.

- Between April 23 and April 25, 2025, the threat actor exfiltrated data from on-premises network files and cloud storage.

- On April 25, 2025, the threat actor used credentials acquired during its previous credential harvesting activities to destroy backups and deploy ransomware.

- The breach was discovered on April 25, 2025, when Nova Scotia Power's employees reported that certain applications were not functional, which was as a result of the ransomware attack.

- Nova Scotia Power received communications from the threat actor that included a hyperlink to an unlisted page accessible through the Tor network on the dark web. The threat actor provided proof that it had obtained sensitive customer information, but no evidence has yet emerged that this sensitive data has been made public or sold. After its assessment of applicable sanctions laws and alignment with law enforcement guidance, Nova Scotia Power did not pay a ransom to the threat actor.

Scope of the affected information

- Nova Scotia Power has determined that approximately 375,000 of its current customers and approximately 540,000 former customers were affected by the breach.

- The compromised personal information varied by affected individual but included names, phone numbers, email addresses, mailing addresses, dates of birth, customer account histories (including customer payment/billing/credit history/bank account numbers), driver's license numbers, and social insurance numbers (SINs).

Complaints received by the OPC

- The OPC received numerous complaints regarding the breach of security safeguards.

- One of these complaints also related to Nova Scotia Power's collection and retention of SINs. Nova Scotia Power explained that SINs were included in the data accessed and exfiltrated by the threat actor from a data repository related to the organization's program for the provision of energy usage insights to its customers.

- A number of the complaints also related to the amount of time that Nova Scotia Power took to notify affected individuals, and in particular that the notification letters were sent by regular mail, which delayed delivery of the notifications.

Breach Response

- Following the breach, Nova Scotia Power took measures to ensure that the impacted environment was secured. The organization, through counsel, engaged a third-party cybersecurity and incident response team who assisted Nova Scotia Power with containment, investigation, and remediation efforts. This included containing and isolating the affected servers, limiting network connectivity, identifying and resetting compromised account credentials, and hardening (i.e., applying security enhancements) the environment.

- On April 28, 2025, three days after discovering the breach, Nova Scotia Power informed the public about the breach including through a news release posted on its website, which was reported on in the media.

- On May 1, 2025, Nova Scotia Power notified the OPC of the breach. The company also updated its website and conducted other communications outreach to inform the public that it had identified that certain customer personal information had been impacted, and that it was working to determine the nature and scope of the impacted data.

Direct Notification of Individuals

- On May 13, 2025, Nova Scotia Power started sending notification letters to approximately 277,000 current customers whose personal information Nova Scotia Power was able to determine had been impacted, and the next day, posted a public notice on its website providing details of the breach, including the types of information that had been affected.

- On October 31, 2025, Nova Scotia Power sent notification letters to approximately 97,000 additional affected customers. These customers were identified through the organization's continued investigation, with the assistance of third-party experts, including through the use of data discovery tools and extensive manual review, which the organization explained was a long and complex process.

Indirect Notification of Individuals

- Due to the nature of the business, Nova Scotia Power did not have up to date contact information for former customers who were affected by the breach. On June 25, 2025, the organization posted a notice on its website that the personal information of former customers had also been affected by the breach. The organization also disseminated notice information through multiple additional channels, including traditional media, social media, stakeholder communications, paid advertising and paid search optimization.

Credit Monitoring

- In its initial notification letters, Nova Scotia Power offered affected individuals 24 months of credit monitoring and identity protection services, which includes up to $1,000,000 of identity theft insurance. Starting on June 25, 2025, the organization increased the offer to five years of credit monitoring and identity protection services for affected individuals and expanded the offer to include all current and former customers, including customers who had not been identified as being affected.

Commitments

As part of this Compliance Letter, Nova Scotia Power voluntarily commits to the additional actions set out below with a view to ensuring the adequacy of its security safeguards, continuing to address risks associated with the breach, and preventing future breaches.

1. Confirmation of Deletion of Customer Social Insurance Numbers
By March 31, 2026, Nova Scotia Power will provide the Commissioner with confirmation that the organization has deleted all instances of customer social insurance numbers from its systems, subject to legal requirements to retain such information (e.g., pursuant to a legal hold, or tax reporting obligations) and implemented segregation of that data to ensure that it is not used for any other purpose.

2. External Security Assessment
By October 31, 2026, Nova Scotia Power will provide the Commissioner with a confidential security assessment and report conducted and prepared by a reputable and independent external security assessment firm to be approved by the OPC, which approval will not be unreasonably withheld. This report will assess enhanced safeguards in the organization's Information Technology environment as of the time of assessment, and will include at a minimum:
- a description of the safeguard enhancements implemented since the breach;
- an assessment of the effectiveness of Nova Scotia Power's information security safeguards

to protect personal information, and to prevent, detect, and respond to potential breaches;
- an assessment of the effectiveness of Nova Scotia Power's employee training and awareness program with respect to privacy and security;
- an assessment of the effectiveness of Nova Scotia Power's processes for notifying affected individuals as soon as feasible following a breach;
- the identification of any remaining gaps in assessed security safeguards and notification processes; and
- recommended solutions to address those gaps.

By October 31, 2026, Nova Scotia Power will inform the Commissioner in writing of the following:
- whether the firm has issued recommendations;
- whether it has accepted each of the recommendations;
- for each recommendation that the organization has not accepted, the reasons why, and what alternative measures it proposes to implement (along with timelines) to address the identified risk(s); and
- for each recommendation that has been accepted: whether the recommendation has been fully implemented; actions already taken by Nova Scotia Power to implement the recommendation; and for the measures that have not yet been fully implemented, an implementation plan, detailing the actions Nova Scotia Power will take to implement those measures and the dates by which they will be completed.

The recommendations (or lack thereof) and the implementation of measures to address them will be subject to review by the Commissioner for his determination of whether the measures implemented by Nova Scotia Power adequately address PIPEDA requirements and constitute a fair and reasonable response.

Signature

Upon signing this letter, Nova Scotia Power commits to the terms set out therein.

SIGNED at Halifax, in the Province of Nova Scotia, this 18th day of March, 2026.