

NOVA SCOTIA ENERGY BOARD

IN THE MATTER OF: THE PUBLIC UTILITIES ACT

- and -

IN THE MATTER OF: AN INQUIRY about the impact of the cyber incident on **NOVA SCOTIA POWER INCORPORATED's** collection and retention of customer information, customer service and communications, billing processes and regulatory matters

INFORMATION REQUESTS

To: **Blake Williams**
Senior Director, Regulatory
Nova Scotia Power Incorporated
P.O. Box 910
1223 Lower Water Street
Halifax, NS B3J 3S8
By email: blake.williams@nspower.ca

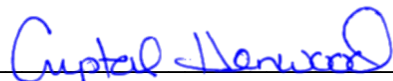
From: **Nova Scotia Energy Board**
Board Counsel Consultants
ING Law Consulting

Responses Due: **Wednesday, May 6, 2026**

Copies: 1electronic copy (PDF searchable)

Contact Person: Tricia Ralph
Board Counsel Consultant
ING Law Consulting
tralph@ing.law

Issued at Halifax, Nova Scotia, this 17th day of April, 2026.



Crystal Henwood, Clerk of the Board

Request IR-1:

With respect to privacy policies and procedures, please provide the following documentation. If any of the documents are not available, please provide the reasons for each request.

- a) Privacy training policy and procedures.
- b) Percentage of staff that completed privacy training in 2024 and 2025.
- c) Privacy complaint and inquiries policy and procedures.
- d) Privacy breach response plan and procedures.

Request IR-2:

With respect to governance and risk management processes addressing privacy risks, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

- a) Privacy governance framework.
- b) Publicly available privacy policy at the time of the cybersecurity incident.
- c) Internal privacy policy (if different from any publicly available privacy policy).
- d) Information as to whether Nova Scotia Power had a designated privacy officer prior to the cybersecurity incident and whether contact information for the officer was made publicly available.
- e) Data collection minimization policy and procedures.
- f) Consent management policy and procedures.
- g) Privacy audit plan and dates of any audits of access to personal data of customers implemented by Nova Scotia Power in the 2 years leading up to the cybersecurity incident.

Request IR-3:

With respect to reporting to regulators, notification to affected individuals, management and communication, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

- a) Date that Nova Scotia Power became aware of the cybersecurity incident.
- b) Date that the Office of the Privacy Commissioner of Canada was notified of the cybersecurity incident.
- c) Date(s) that any other privacy regulators were notified of the cybersecurity incident.
- d) Date(s) that affected individuals were notified of the cybersecurity incident.
- e) Template(s) of notification letter(s) to affected individuals.

Request IR-4:

With respect to collection and retention of customer information, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

- a) Collection, retention and destruction of customer information policy and procedures.
- b) Records of customer data destruction activities in the 2 years leading up to the cybersecurity incident.
- c) List of types of personal data types collected about customers and for what purposes.

Request IR-5:

With respect to measures implemented to mitigate risk to customers from fraud and identity theft following the cybersecurity incident, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

- a) Please provide a list of measures taken by Nova Scotia Power to mitigate risks to affected individuals from fraud and identify theft following the cybersecurity incident
- b) Please detail whether any complaints were received by affected individuals related to mitigation measures. If yes, how many, how were they responded to, and average response time.

Request IR-6:

With respect to whether any third-party service providers were involved in the breach and if yes, whether there were data sharing agreements in place with them. Please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

- a) Third-party service providers privacy risk assessment policy and procedures
- b) Whether there were any third-party service providers whose services were involved in the cybersecurity incident. If yes, please provide a copy of their contracts related to data sharing.
- c) If any third-party service providers whose services were involved with the cybersecurity incident, dates that they became aware of any breach of personal data and dates that they notified Nova Scotia Power of same.

- 1 d) Please confirm whether any third-party service providers whose services were involved
2 with the cybersecurity incident were audited by Nova Scotia Power in the 2 years leading
3 up to the cybersecurity incident.
4

5 **Request IR-7:**

6 With respect to communications with customers relating to cybersecurity related issues, please
7 provide the following documentation or information, as applicable. If any of the documents or
8 information is not available, please provide the reasons for each request.

- 9 a) Access to information requests policy and procedures.
10 b) Amount of access to information requests made by customers related to the cybersecurity
11 incident.
12 c) Information about whether access to information requests made by customers related to
13 the cybersecurity incident were responded to within 30 days.
14 d) Number of accesses to information requests that were not responded to within 30 days (if
15 any).
16 e) Number of privacy complaints and inquiries received from customers related to the
17 cybersecurity incident.
18 f) Information about whether all customers' privacy complaints and inquiries were responded
19 to related to the cybersecurity incident.
20 g) Average amount of time taken to respond to customers' privacy complaints and inquiries
21 related to the cybersecurity incident.