

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

From: INQ Law/Consulting
c/o William Mahody, KC
Board Counsel and Consultant
Washington & Mahody
03-5475 Spring Garden Road
Halifax, NS B3J 3T2

To: The Consumer Advocate

Responses Due: July 29, 2026

Copies: 1 electronic copy (PDF searchable)

Contact Person: David J. Roberts
Consumer Advocate
Pink Larkin
1463 South Park Street
Halifax, NS B3J 3S9
Tel: (902) 423-7777
Email: droberts@pinklarkin.com

Request IR-1:

With regard to paragraph 13, page 6 of the Report of INQ Law/Consulting:

- A. What are the industry standards for organizations such as Nova Scotia Power regarding the content of a Personal Information Inventory?

Response: It is common industry practice for organizations to adopt a recognized privacy framework, such as the NIST Privacy Framework, or ISO 27701, to structure their data protection practices. The NIST Privacy Framework has an Inventory and Mapping category (ID.IM-P). Complying with this NIST Category enables an understanding of data processing by systems, products or services well enough to inform privacy risk management.

The relevant components of ID.IM-P are:

<i>Subcategory</i>	<i>Function</i>
<i>ID.IM-P1:</i> Systems/products/services that process data are inventoried.	<i>Gives the closed set of systems to check against the incident's affected asset list.</i>
<i>ID.IM-P2:</i> Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	<i>Directs who needs to be pulled in and who holds contractual breach obligations for a given affected system.</i>
<i>ID.IM-P3:</i> Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	<i>Converts what system was compromised into which categories of individuals were affected.</i>
<i>ID.IM-P4:</i> Data actions of the systems/products/services are inventoried.	<i>Indicates what was actually done with the data on that system (collection, storage, transmission), which is key to scoping what was exposed.</i>
<i>ID.IM-P5:</i> The purposes for the data actions are inventoried.	<i>Allows determination of whether the exposed data falls inside or outside stated collection purposes. This is important for notification framing and any secondary-use exposure.</i>
<i>ID.IM-P6:</i> Data elements within the data actions are inventoried.	<i>Enables identification of the field-level data points (eg. SIN, financial account, etc.) that live in the compromised system.</i>
<i>ID.IM-P7:</i> The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	<i>Enables determination of which jurisdictions' laws apply and whether a third-party processor's environment was the point of compromise.</i>

ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	Shows the data flow tying system to data elements, to owner, to third-party interaction. This allows the organization to determine what data points were affected.
--	---

- B. How would a “well-structured PI inventory” have enabled Nova Scotia Power to determine what data points were affected by the cyber incident?

Response: A well-built inventory maps personal information (PI) at the field level to the systems and repositories where it resides, not just at the system level. A well-structured PI Inventory would not just indicate what systems were compromised but also what specific data points were exposed. Had NSPI sufficiently mapped and inventoried both system level and more granularly, field level, this should have allowed NSPI to determine which exact data points were exposed, as opposed to types of PI that may have been compromised.

- C. What does INQ Law/Consulting conclude about the Personal Information Inventory maintained by Nova Scotia Power as a result of its admission that “it does not know and will never know what data points for each individual impacted customer were exposed through the incident”.

Response: This leads me to believe that either the PI Inventory was deficient or not operationalized. If ID.IM-P6 (data elements) and ID.IM-P8 (data processing mapping) had existed at a more granular level, NSPI should have been able to determine which exact data points were affected.

Request IR-2:

With reference to Paragraph 31, page 9 of the Report, what is the understanding of INQ Law/Consulting of the reason why periodic audits of internal access to personal information is a commonly expected practice in privacy management governance?

Response: The Protect-P (PR-P) function of the NIST Privacy Framework contains subcategory PR.AC-P4: “Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.” Access controls are the primary tool for detecting insider misuse. Typically, at the outset of granting internal access to PI, employees are granted access to the least amount of PI necessary to perform their job functions. However, over time, it is not uncommon for this alignment to stray as a result of things like role changes and project completion (ie access may have been granted for a specific project after which that access is no longer required). An audit is a mechanism that catches any such accumulated drift. Of note, as internal access was not a factor in the breach (rather it was an external cyber security attack), the lack of audit

1 *in the two years leading up to the Incident was not likely a factor in the breach.*
2 *Nevertheless, such audits are commonly expected in privacy management program*
3 *governance.*

6 **Request IR-3:**

7 With regard to paragraph 89, page 21 of the Report, which states:

9 “.....In my opinion, the initial offer of two years of credit monitoring was insufficient to address
10 the risks arising from the unauthorized access to SINs. Given that a SIN is a largely static identifier
11 that cannot be readily changed, the risk of misuse by threat actors is not confined to a defined
12 period but persists indefinitely. A two-year monitoring period did not, in my opinion, adequately
13 reflect that ongoing exposure. However, in my opinion, the extension of credit monitoring to five
14 years brought the remedial offering to a level that was reasonable given the nature of the
15 information compromised.”

- 16
17 A. What factors, including but not limited to best practices, examples from other similar
18 events, legal or regulatory standards, did INQ Law/Consulting consider to support the
19 conclusion that five years of credit monitoring is a reasonable mitigation of customer
20 risk from fraud and identity theft?

21
22 *Response: There are no legal or regulatory standards that set out a reasonable time period*
23 *for the amount of time that credit monitoring should be offered for. In reports from*
24 *Information and Privacy Commissioners across Canada, the amount of time has historically*
25 *been two years. However, as indicated below, some Commissioners are starting to*
26 *recommend that two years is not sufficient but rather five-ten years is more appropriate.*

27
28 *The Information and Privacy Commissioner for Saskatchewan has issued numerous reports*
29 *with findings that two-year credit monitoring is not sufficient but rather a minimum of five*
30 *years is more appropriate. For example, in [Investigation Report 370-2021, Saskatchewan](#)*
31 *[Liquor and Gaming Authority \(Re\), 2022 CanLII 109458 \(SK IPC\)](#), the Saskatchewan*
32 *Commissioner recommended that credit monitoring be provided for a minimum of five years*
33 *in response to a cyberattack.*

34
35 *Later, in 2025, the Saskatchewan Commissioner recommended that credit monitoring be*
36 *provided for a minimum of ten years in response to a cyberattack ([Investigation Report 136-](#)*
37 *[2024, 169-2024, 183-2024, 187-2024, 191-2024, Innomar Strategies Inc. \(Re\), 2024 CanLII](#)*
38 *[116817 \(SK IPC\)](#)).*

39
40 *In 2025, the federal Privacy Commissioner accepted a Letter of Commitment to the Office*
41 *of the Privacy Commissioner of Canada from PowerSchool where PowerSchool offered two*
42 *years of credit monitoring in response to a cyberattack.*

43
44 *In [Investigation Report IR25-01, Nova Scotia Government \(Re\), 2025 NSOIPC 2 \(CanLII\)](#),*
45 *the Information and Privacy Commissioner found that a credit monitoring service offering*
46 *of five years was reasonable where SINs were compromised but noted that the Saskatchewan*

1 *Commissioner had recently recommended a monitoring period of ten years in the above*
2 *noted case.*

3
4 *In my opinion, given the sensitivity of SINs, two years of credit monitoring was not sufficient*
5 *but should rather have been at minimum five years.*

6
7
8 B. Please provide any and all references or examples that were relied on to test the
9 reasonableness of NSPI's five-year credit monitoring offer.

10
11 *Response: Please see response to question IR-3 A above.*
12
13

14 **Request IR-4:**

15 In paragraph 106, page 26 of the Report, INQ Law/Consulting concludes that 8 of the 18 actions
16 of Nova Scotia Power relating to personal information that were reviewed, "did not meet best
17 practices, and were unreasonable in terms of meeting the expectations of customers and limiting
18 the impacts of the cyber security attack on customers."
19

20 Which of the actions listed in paragraph 106 were the most significant:

21
22 A. When viewed in light of the reasonable expectations of customers, and;
23

24 *Response: In my view, the actions most significant in terms of customer expectations were:*
25

- 26 1. *That SINs were collected when doing so was not required for legislated purposes;*
27 *and*
28 2. *That NSPI was not able to provide fulsome answers as to what exact data points*
29 *were compromised.*
30

31 B. In failing to limit the impact of the cyber security attack on customers?
32

33 *Response: In my view, the most significant action in terms of limiting the impact of the*
34 *cyber security attack was that NSPI retained customer data for too long. Had NSPI*
35 *disposed of the information once it was no longer needed, that data would not have been*
36 *available for access by the threat actors. SINs in particular should not be retained beyond*
37 *the time needed for the purpose of their collection.*