

Nova Scotia Energy Board

IN THE MATTER OF *The Public Utilities Act*, R.S.N.S. 1989, c.380, as amended

M12273

Board Inquiry into Nova Scotia Power's Cybersecurity Incident

Nova Scotia Power
Incident Report

December 22, 2025

REDACTED

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

TABLE OF CONTENTS

1			
2			
3	1.0	INTRODUCTION	3
4	2.0	THE INCIDENT	7
5	3.0	AFFECTED SYSTEMS AND DATA	12
6	3.1	Compromised Systems	12
7	3.2	Data & Personal Information	14
8	4.0	RESPONSE AND RECOVERY ACTIONS	15
9	4.1	Mitigation and Restoration Actions	15
10	4.2	Communications to Customers	19
11	4.3	Other Stakeholders	28
12	4.4	Response Analysis	30
13	5.0	COLLECTION AND RETENTION OF PERSONAL INFORMATION	32
14	6.0	IMPACT ANALYSIS	33
15	6.1	Impact	33
16	6.2	Assessment of Potential Harm	35
17	7.0	M12457 DIRECTION	37
18	8.0	RECOMMENDATIONS	38
19	8.1	Enhancing Security Measures and Preventing Future Breaches	38
20	8.2	Additional Security Audits, Policy Updates, and Employee Training	40
21	8.3	New Strategies and Proactive Measures	40
22	8.4	Customer Communications	41
23	8.5	Collection and Retention of Personal Information	43
24	9.0	CONCLUSION	45

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1.0 INTRODUCTION

In its July 14, 2025 letter regarding the cybersecurity incident (Incident) experienced by Nova Scotia Power Inc. (NS Power, Company), the Nova Scotia Energy Board (NSEB, Board) advised that “the Board will require a report from NS Power about the incident”¹ and that “[t]he Board believes NS Power should be able to file this incident report by the end of this year, but if NS Power does not believe this date is achievable, it may propose another.”² The NSEB noted that the Incident report should include several categories of information,³ as follows:

- Incident Description
- Affected Systems and Data
- Indicators of Compromise
- Root Cause Analysis
- Impact Analysis
- Response and Recovery Actions
- Collection and Retention of Personal Information
- Recommendations

On November 7, 2025, the NSEB provided additional direction as follows:

1. Settle any outstanding dues of vendors or suppliers as soon as possible, and in the January monthly report, indicate what percentage of invoices remain pending, along with an aged analysis of the payables and the reasons for the accounts outstanding beyond 30 days. The Board will also refer this matter to MNP to further investigate causes of the NS Power's financial technology data compromise and assess its data handling practices.

¹ M12273, Board Inquiry into Nova Scotia Power's Cybersecurity Incident, NSEB Letter, July 14, 2025, page 1.

² M12273, NSEB Letter, July 14, 2025, pp. 2-3.

³ M12273, NSEB Letter, November 7, 2025, pp. 1-2.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

2. In the incident report to be filed by the end of this year, please provide a Gantt chart that includes a list of all the summary tasks/rolled-up tasks currently undertaken to achieve full recovery. The chart should specify the expected completion time, start date, finish date, and percentage completion. If no progress is made from one month to the next, this should also be clearly indicated along with the reasons.

3. A separate chart is to be provided in the Incident Report which includes the list of Board matters or potential proceedings which are impacted and a forecast date for the restoration of normal activities in each matter.⁴

In accordance with the Board's direction, this report provides the information requested. This report also provides a Gantt chart of systems restorations timelines and another chart with a list of impacted Board matters and proceedings. Please refer to Appendices A and B, respectively. With respect to the NSEB's direction regarding outstanding dues to vendors and suppliers, the Company is working to compile this information and anticipates being in a position to provide the requested information to the Board in early February 2026.

On December 3, 2025, the Premier of Nova Scotia issued an open letter to the NSEB regarding the Incident. The Premier called on the Board to launch a formal investigation into:

1. The fairness and legality of NSP's estimated billing methodology.
2. The adequacy of consumer protections and communication during this period.
3. The timeline and contingency planning for restoring accurate billing systems.
4. Whether NSP should provide financial relief, credits, or bill smoothing options to affected customers.
5. Whether NSP is subject to financial penalties; and if so, the maximum amount that can be levied.⁵

⁴ M12273, NSEB Letter, November 7, 2025, p. 2.

⁵ M12600, Minister of Energy – Accountability for Nova Scotia Power Inc., Minister of Energy Letter, December 3, 2025.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 The NSEB replied to the Premier by letter on December 10, 2025, providing, in part, the following:

2
3 Upon receipt of your letter, the Board opened a new matter (M12600). Given the
4 connection between these issues and the Board's ongoing inquiry into the
5 cybersecurity incident (M12273), the Board will consider whether the issues raised
6 in your letter would be most effectively and efficiently addressed in a separate
7 proceeding or in the ongoing cybersecurity inquiry.

8 //

9 The Board anticipates scoping the necessary additional processes for the
10 cybersecurity matter upon receipt of the utility's formal report later this month. The
11 content of the report and the responses to the Board's outstanding information
12 requests will inform whether the issues outlined in your letter would be most
13 appropriately addressed in the cybersecurity matter or separately in the new
14 matter.⁶

15
16 The Company notes that many of the issues raised by the Premier, specifically the estimated
17 billing, customer communications, timelines and contingency planning for restoration of normal
18 billing, and customer assistance programs, were addressed in the monthly Incident update report
19 for November provided by NS Power on December 1, 2025, with additional details provided
20 herein. Finally, the Board's second set of Information Requests (IR) received under this matter on
21 December 3, 2025, deal specifically with the customer billing issue. Responses to those IRs are
22 due to the NSEB on December 23, 2025. Accordingly, NS Power believes that M12273 is the
23 appropriate proceeding in which to address the issues raised by the Premier without the need for a
24 new matter.

25
26 On December 10, 2025, the NSEB provided additional direction by letter stemming from a
27 customer complaint (M12457). In its letter, the NSEB noted as follows:

28
29 At this stage, the Board requires that NS Power report back on the progress made
30 and outcomes of this broader review. As this review involves broader issues than
31 that of the complainant, it is appropriate that the update be provided in a separate
32 process from the initial complaint. The Board would, therefore, request that NS
33 Power include information on the progress made on this issue in the final report in

⁶ M12600, NS Power Letter, December 10, 2025, p.1.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 Matter M12273-Board Inquiry into Nova Scotia Power's Cybersecurity Incident.
2 This would be the most efficient way to address the matter.⁷

3

4 Accordingly, the Board's directive is addressed in this report.

5

⁷ M12457, NSPI Complaint – Systemic Regulatory Compliance Issues – Blarney Stone Restaurant, NSEB Letter, December 10, 2025.

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

2.0 THE INCIDENT

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the Incident:

- A detailed account of how NS Power discovered the breach.
- A description of the attack vector.
- A timeline of events from detection to resolution.⁸
- A description of evidence and artifacts indicating the presence of the breach, such as unusual network traffic or suspicious files.
- Whether NS Power was aware of activity prior to the breach that could have caused it to be alerted about a potential breach.⁹
- A description of how the breach occurred.
- An identification of vulnerabilities or security gaps that were exploited.¹⁰

NS Power addresses each in this section.

Discovery of the Breach and Background

The Incident involved a sophisticated and coordinated criminal cyberattack on certain of NS Power's information technology systems and data.

The Incident was discovered on April 25, 2025, when NS Power employees reported certain applications on the Company's systems were not functional. Upon immediate investigation, it became evident that a threat actor had gained unauthorized access into certain parts of NS Power's information technology network and servers which support portions of its business applications.

⁸ M12273, NSEB Letter, July 14, 2025, p. 1.

⁹ M12273, NSEB Letter, July 14, 2025, p. 1.

¹⁰ M12273, NSEB Letter, July 14, 2025, p. 2.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

Immediately following detection of the Incident, NS Power activated its established incident response and business continuity protocols, engaging Osler, and through Osler, Mandiant's cybersecurity and incident response team.

Under the direction of Osler, Mandiant assisted the Company and other cybersecurity experts with containment, investigation, and remediation efforts, and took immediate actions to contain and remediate the unauthorized activity, including containing and isolating affected servers, limiting network connectivity, identifying and resetting compromised account credentials, and hardening the environment. Teams within NS Power also began working diligently with cybersecurity experts to further isolate the operational technology and energy delivery systems.

The Company continues to have no evidence the threat actor accessed any operational technology or energy delivery systems.

Based on the investigation, the Company believes that an unauthorized third party gained access on or around March 19, 2025 and, beginning on or around April 25, 2025, exfiltrated certain data, including personal information of the Company's customers.

NS Power notified law enforcement of the Incident. More specifically, NS Power notified the Canadian Centre for Cybersecurity (CCCS), the Royal Canadian Mounted Police (RCMP), and the Canadian Security Intelligence Service (CSIS) on April 27, 2025 and provided them with information about the Incident. Given the nature of the cyber attack, the critical infrastructure nature of the company and the North American electric utility industry, and the high confidence our advisors had of the identity of the threat actor, the Company also notified the Federal Bureau of Investigation (FBI).

NS Power also reported the Incident to the Office of the Privacy Commissioner of Canada (OPC) on May 1, 2025, with an update on May 14, 2025. The OPC initiated an investigation into the

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

Incident, on May 28, 2025 and the Company is actively and fully cooperating with the OPC to support the OPC's investigative efforts.

Incident Timeline & Attack Vector

The forensic investigation of the Incident has been complex.

It was determined that the initial point of entry of the attack was as a result of an employee visiting a legitimate website on the internet and clicking on a link in a pop-up, that resulted in malicious software being installed on their system. The malicious software itself was sophisticated and was able to evade detection from NS Power's protection system, and its detection and response capabilities. This software created a malicious background process that then downloaded additional malware, and established persistence on the infected NS Power system.

The date of initial compromise of the Company's systems was determined to be March 19, 2025. The initial malicious javascript payload was identified as FAKEUPDATES (also publicly reported as "SocGholish").

Shortly after the system was compromised, [REDACTED]

Between March 19, 2025, and April 8, 2025, the threat actor leveraged these persistence mechanisms to access the system and perform network reconnaissance, as noted above. On April 25, 2025, the threat actor deployed the [REDACTED] ransomware.

On April 8, 2025, the threat actor began to move laterally to systems in the environment using accounts with elevated privileges. The threat actor then deployed additional malware in additional systems.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

Between April 8 and April 22, 2025, the threat actor leveraged this malware to access systems in the environment and to perform additional internal reconnaissance and credential harvesting activities.

Beginning on or around April 25, 2025, the threat actor exfiltrated data from on-premises network files shares and NS Power's data analytics cloud storage environment (REDACTED) resources to threat actor-controlled infrastructure.

On April 25, 2025, there was deployment of the ransomware and associated encryption activity, as well as destruction of backups using the previously acquired credentials.

The threat actor used a sophisticated combination of known attack paths and novel use of more recent attack methods to evade detection. REDACTED

On April 25, 2025, NS Power disabled external access to the NS Power environment, and began to isolate systems with suspicious or malicious activity.

Mandiant confirmed the Incident was contained on April 29, 2025 (i.e. within four calendar days after discovery), and the Company has not identified evidence of threat actor activity within the NS Power environment since April 29, 2025.

NS Power provided additional detail relating to the incident timeline in the materials provided to the Board's consultant MN&P in relation to this investigation.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 The Incident has not caused any disruption to physical operations at NS Power's generation,
2 transmission and distribution facilities, and the Incident has not impacted the Company's ability
3 to safely or reliably provide electricity to customers in Nova Scotia.
4

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

3.0 AFFECTED SYSTEMS AND DATA

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the affected systems and data:

- An identification of compromised systems and data.
- Specific details about the type and amount of personal information exposed.¹¹

NS Power addresses each in this section.

3.1 Compromised Systems

NS Power has previously described affected systems in its October 1, November 3, and December 1, 2025 monthly Incident update reports, under the Incident Impact and Response section. Those systems include, broadly:

- Enterprise Resource Planning (ERP) systems:
 - PeopleSoft
 - PowerPlan
 - Oracle E-Business Suite
- Customer Billing and Customer Systems:
 - MyAccount
 - Advanced Metering Infrastructure Head End System
 - Backup Advanced Distribution Management System
 - MV90
 - Packaged Contact Center Enterprise

¹¹ M12273, NSEB Letter, July 14, 2025, p. 1.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

- Additional systems:
 - Aligne Fuels/Plant Information (PI)
 - Geospatial Information System
 - Adept Restoration
 - Certain Laptop Computers
 - Self-Serve Business Intelligence & Analytics
 - [REDACTED]
- Cybersecurity systems and tools:
 - Active Directory
 - Privileged Access Management Tool
 - Security Information and Event Management Tool
 - Vulnerability Management Tool
 - Public Key Infrastructure System
 - Data Classification and Data Loss Prevention Tools
 - Mobile Device Management Tool
- Data Centre Technology:
 - Servers & Virtual Environment
 - Network & Firewall Infrastructure
 - Backup Systems
 - Network Attached Storage (NAS)
 - SharePoint File Storage

Please also refer to Appendix A which provides the above noted list of affected technology systems, and Gantt chart illustrating restoration progress to date and timelines.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

3.2 Data & Personal Information

[REDACTED]. The process to identify the customers who were directly impacted has been extremely complex, and has been completed. As set out in the notices sent to impacted customers, the impacted data would have varied by customer, and depended, in part, on the information a customer would have provided NS Power (i.e. not all personal information elements would have been impacted for all notified customers).

The Company stated in its notice to impacted customers that the unauthorized third party gained access to various types of personal information of customers that included the following: name, phone number, email address, mailing and service addresses, NS Power program participation information, date of birth, and customer account history (such as power consumption, service requests, customer payment, billing, and credit history, and customer correspondence), driver's license number, and social insurance number (SIN). For some customers, bank account numbers (for pre-authorized payment) may also have been impacted, if this information was provided by these customers. With respect to direct notifications, the Company issued two versions of notification letters to impacted customers. The letters were substantively identical, except that one version advised the customer that based on the investigation, their social insurance number may have been affected by the Incident.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

4.0 RESPONSE AND RECOVERY ACTIONS

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the response and recovery actions:

- Steps taken by NS Power to contain and mitigate the breach.
- Actions taken by NS Power to eradicate the threat and restore affected systems.
- NS Power's communication with stakeholders, including customers, employees, NERC, NPCC, E-ISAC, Canadian Centre for Cyber Security, and regulatory bodies.
- An analysis of what went well with NS Power's response to the incident and what NS Power can improve.¹²

NS Power addresses each in this section. Please also refer to Section 2 above.

4.1 Mitigation and Restoration Actions

Immediately following detection of unauthorized access, NS Power activated its incident response and business continuity protocols, engaged leading third-party cybersecurity experts, and took actions to contain and isolate the affected servers and prevent further intrusion.

Since the discovery of the event, NS Power has mobilized a team of internal and external specialists to support the recovery effort. The Company's immediate priorities focused on containment, eradication and remediation of the threat, and conducting a thorough analysis to understand the full scope and nature of the Incident.

¹² M12273, NSEB Letter, July 14, 2025, p. 2.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 Immediate remediation actions were taken:



11 Further intermediate remediation steps that have been taken include:



24 Ongoing remediation steps include:



**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

[REDACTED]

NS Power is also advancing efforts to restore and, where necessary, rebuild core business applications and infrastructure — including finance, human resource, procurement, certain customer billing systems, and integrations between those systems and other supporting systems — by leveraging secure backups and reestablishing security and monitoring protocols across systems. These recovery efforts are focused on ensuring continuity and stability for the Company's business operations and customers.

To coordinate work streams on business restoration and information security strengthening efforts, a business restoration process office (RPO) has been established within NS Power. Restoration efforts are continuing, and [REDACTED] has been retained as a strategic partner and systems integrator to assist in this process.

Key additional remediation and restoration efforts related to strengthening the Company's cyber security systems include:

[REDACTED]

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED



Existing Safeguards

At the time of the Incident, NS Power had implemented a common set of cybersecurity standards and policies that are informed, in part, by the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, and the Company regularly reviews and makes continuous improvements to its cybersecurity programs to ensure it is in line with the latest guidance. In connection with these efforts, NS Power has recently completed an extensive two-year update to its cybersecurity practices to comply with current policies and anticipated changes in standards communicated by NIST.

NS Power's cybersecurity framework (which applies to its information technology program more generally) includes specific policy and control standards aligned with NIST's Core Functions as noted below:

- Identify – Establishes organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Establishes the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Establishes the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Establishes the appropriate activities to take action regarding a detected cybersecurity event.
- Recover – Establishes the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

In relation to NS Power's operational program, NS Power's core energy operations are designed to comply with other industry-specific rules and standards relating to cybersecurity and IT including, but not limited to, those mandated by the North American Electric Reliability Corporation (NERC). NERC conducts extensive periodic audits (including security) of the Company's Energy Operations to ensure effective compliance.

NS Power maintains a cybersecurity training and awareness program and conducts mandatory quarterly cyber training and monthly phishing simulation testing exercises with all employees to educate employees about NS Power's information security policies and common risks, and to help them understand their information security responsibilities.

4.2 Communications to Customers

Customer Communications and Response

The Company adopted a best-practices approach to mitigating potential harm to customers whose personal information was impacted by the Incident. This approach was grounded in a commitment to transparency, timely communication, and a customer-centric focus. The Company's objective throughout has been to provide affected individuals with meaningful support, reduce the risk of harm, and maintain trust through accountability.

The Company's robust transparency effort is evidenced by the public communications that NS Power has engaged in throughout the Incident.

NS Power implemented a previously developed and tested consistent multi-channel approach throughout the response efforts for all public communications. For each update, the transparency effort involved postings on a dedicated cyber update landing page on the Company's website and social media channels, notice to all local media, and communications directly to key account/business customers, government and other stakeholders in addition to employees.

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

To ensure customers were kept informed, the Company also employed a multi-platform paid media strategy that includes online, as well as TV, print and radio to reach a wide variety of customer demographics. In addition, NS Power activated a paid search strategy throughout the Incident to ensure that the NS Power website and information appeared as the top search result when customers used search engines (i.e. Google) to find information about the Incident. This paid search strategy was also used to reduce the risk of fraudulent activity related to searches for the official Nova Scotia Power website. Social media accounts have been regularly updated and monitored, and where appropriate, the Company has provided answers to related customer questions online. Customers were also able to speak directly with NS Power customer care representatives on the phone throughout the Incident for any questions or concerns.

Customer Notification Timeline

As noted above, the Company became aware of the Incident on Friday, April 25, 2025. The next business day, on Monday, April 28, 2025, NS Power informed customers that it was actively responding to a cybersecurity incident, and encouraged customers to report any suspicious emails or phone calls.

On May 1, 2025, NS Power determined that customer information had been impacted in the Incident, and promptly updated customers using the multi-channel strategy noted above to inform them that they had identified that certain customer personal information had been impacted in the Incident, and again encouraged them to remain vigilant and cautious of unsolicited communications and potential scams. The Company informed customers that they were working urgently to determine the full nature and scope of the data that may have been affected. The Company also initiated the process of notifying affected individuals, including retaining third-party service providers to assist with this effort.

[REDACTED]

[REDACTED]

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]

5
6 On May 13, 2025, NS Power sent direct notices to approximately 277,000 current customers whose
7 personal information the Company was able to determine had been impacted in this incident.

8 The following morning (May 14, 2025), the Company also issued a press release, provided a
9 detailed update on its website, and updated its various social media accounts, which received
10 widespread coverage in the local and national media. Senior Company personnel, including the
11 President & CEO, participated in multiple media interviews to ensure that the public remained
12 informed about the Incident.

13
14 NS Power's notice to impacted customers also included guidance for steps they could take to
15 reduce any risk of harm resulting from the incident (including steps to protect themselves from
16 fraud or potential identity theft). This notice included an offer for two years of complimentary
17 credit monitoring and identity monitoring services for impacted individuals.

18
19 The credit monitoring service offered to customers is provided by TransUnion and has been
20 specifically designed to protect individuals in the case of a data breach, and offers them access to
21 the following protective features:

- 22
- 23 • Unlimited online access to their TransUnion Canada credit report, updated daily, which
24 offers individuals access to the individual's financial history and is one of the primary tools
25 leveraged for determining credit-related identity theft or fraud.
26
 - 27 • Unlimited online access to their credit score, updated daily.
28

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

- 1 • Credit monitoring, which provides individuals with email notifications to key changes on
2 an individual's TransUnion Canada credit report. These credit alerts help protect
3 individuals against identity theft, enable quick action against potentially fraudulent activity
4 and provide them with additional reassurance.
5
- 6 • Access to online educational resources concerning credit management, fraud victim
7 assistance and identity theft prevention.
8
- 9 • Access to Identity Restoration agents who are available to assist individuals with questions
10 about identity theft. In the unlikely event that an individual becomes a victim of fraud, a
11 personal restoration specialist will help to resolve any identity theft.
12
- 13 • Up to \$1,000,000 of expense reimbursement insurance related to identity theft.
14
- 15 • Dark Web Monitoring, which monitors surface, social, deep, and dark websites for
16 potentially exposed personal, identity and financial information and helps protect
17 individuals against identity theft.
18

19 Thereafter, NS Power continued to keep customers updated regarding the ongoing incident and
20 investigation through updates on its website landing page dedicated to cyber updates.
21

22 On May 22, 2025, NS Power became aware that the threat actor had published data on the dark
23 web, and promptly provided an update to customers through the same channels as previous
24 updates, including updating the company's website and social media channels, notifying local
25 media, and conducting media interviews.
26

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

Former Customers

As the Company continued its investigation of the impacted data, NS Power determined that personal information relating to former customers had also been impacted by the Incident.

On June 25, 2025, NS Power notified the public that information related to former customers had also been impacted in the Incident. In addition, out of an abundance of caution, and in the interest of assisting customers further to mitigate the potential harm to current and former customers arising from the Incident, NS Power proactively extended the credit monitoring offer to five years for all current and former customers. Customers who had already registered for credit monitoring had their monitoring timeframe automatically extended.

Given that NS Power does not have updated contact information for its former customers, the Company worked to share this indirect notification as broadly as possible. In addition to its website, NS Power actively shared this information with media, on social media, with stakeholders, through paid advertising, as well as national paid search optimization, to reach as many current and former customers as possible.

Additional Customer Notification

NS Power has continued its investigation into the scope and nature of the impacted data with the assistance of leading third-party data analysis experts to determine the precise number of impacted individuals. This was a highly complex and time-consuming exercise, which included using data discovery tools, and extensive manual review.

As a result of these efforts, Nova Scotia Power identified approximately 97,000 additional customers who were impacted in this incident. Nova Scotia Power sent direct notices to these individuals on October 31, 2025, and offered them an additional opportunity to sign up for credit monitoring, to the extent they have not already done so.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 In sum, at this time, Nova Scotia Power has sent direct notifications to approximately 375,000
2 customers who have been identified as being impacted in this incident.
3

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

Customer Support for Credit Monitoring and Dedicated Call Centres

Promptly upon becoming aware of the Incident, NS Power established a dedicated call centre where individuals could receive more information about the Incident, and support for credit monitoring sign-ups, whose number was included in the notice letters and made available to customers.

As is standard in incidents of this nature, to ensure that the call centre had sufficient capacity to handle the volume of calls and allow NS Power's customer service team to focus on a subset of escalated queries, this call centre was staffed by TransUnion employees who had been provided with prepared responses from NS Power, and instructed to escalate any queries that could not be addressed to the Company so that customers could receive a call-back from the NS Power customer service team. This also allowed customers to connect directly with TransUnion for assistance in signing up for credit monitoring (and a dedicated phone line for questions about the credit monitoring process was included with the instructions provided to customers in their letter).

Having TransUnion operate the call centre enabled flexible staffing to accommodate the initial high volume of calls, and reassignment of call centre staff as call volumes dropped.

Where a customer requested a call back or had questions that could not be answered by the prepared information provided to the call centre staff, a list of customer call back requests, with relevant information, was provided to NS Power on a daily basis, whose customer care team would reach out to these customers.

To assist current and former customers with the sign-up process, the Company deployed dozens of employees to communities across the province to provide hands-on support for customers who prefer assistance in person, recognizing that not all customers may be comfortable registering online, and to ensure that customer needs are being met and access to services was being provided. More than 30 of these community sessions were held, assisting over 700 customers in signing up

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 for the credit monitoring service. Our focus on community engagement sessions builds on NS
2 Power's approach over the past two years where we regularly engage with customers on reliability
3 and other customer topics of interest.

4
5 In addition, the NS Power website was updated with additional tips and tools to help customers
6 navigate support services and a fact sheet was created with information about the service and tips
7 for signing up. This guidance also included information on additional measures customers could
8 take to protect themselves against identity theft. Thousands of paper copies were distributed and
9 available to customers across the province through the customer support sessions at community
10 locations. In addition, the fact sheet was available at NS Power local depots and provided to MLAs
11 and local councilors' offices. NS Power has actively encouraged customers and its employees to
12 reach out to their family and neighbours to encourage them to sign up.

13
14 ***Customer Support for Bills***

15
16 NS Power acknowledges and understands customer concerns with the estimated billing process.

17
18 When billing resumed in June, NS Power created a dedicated webpage at nspower.ca/billing to
19 outline the billing process and options available for customers. Since that time, the
20 company has included three separate inserts with customer bills to communicate
21 information regarding the impacts of the Incident on billing, and the need to estimate bills
22 and adjust them once meters are read either physically or data is able to be retrieved
23 remotely. These bill inserts have also all included notice of and direction
24 to the website content. NS Power also informed customers of the improvements made to the
25 online customer portal (My Account) including new features and information on updated login
26 screens for better security and user experience.

27
28 NS Power will continue to revise bill insert content to reflect the current customer experience and
29 options, including further promotion of the ability for customers to submit a photo of their meter.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 With the challenges related to estimated billing causing concerns for customers, Nova Scotia
2 Power is also holding a series of in-person community sessions across the province to answer
3 questions and help customers understand the options related to their bills. These sessions are
4 promoted through local media (including radio and TV), shared with local government and other
5 stakeholders, and published on the homepage of the company's website. In December 2025,
6 sessions have been held in Yarmouth, Port Hawkesbury and Truro, helping dozens of customers
7 with their bills. Additional sessions, originally scheduled for December but postponed due to
8 inclement weather, are scheduled for January 2026 in Sydney and Middleton. A list of upcoming
9 dates can be found at nspower.ca/billing.

10

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

Ongoing Customer Communications Efforts

As discussed above, NS Power has been committed to transparency in its communications with customers and other stakeholders throughout the cyber response to date. This approach has focused on the importance of sharing known information in a timely and transparent matter, without speculating on information yet to be confirmed by the investigation into the cyber incident.

Nova Scotia Power's communications response and approach to the cyber incident, and the subsequent need to communicate with customers about estimated billing has and will continue to evolve based on availability of new information, customer feedback, and as systems continue to be restored. As the issue has progressed, Nova Scotia Power has been able to share more specific information with customers and stakeholders across more channels. In-person sessions in rural communities are a key example of this, as is the use of paid ads on both rural and urban radio stations to reach customers who may not use digital modes of communication. Building on the success of community information sessions related to reliability, the company has held sessions to assist customers with the sign-up process for credit monitoring and more recently to help customers understand their options related to estimated billing. Feedback from customers at these in-person sessions, as well as customer feedback received through digital channels and the Customer Care Centre continue to shape the information the Company is providing and the channels the Company is using to ensure customers have the information they need.

As discussed elsewhere in this report, part of the internal process related to this incident will include a review of lessons learned, including a review of communications with customers.

4.3 Other Stakeholders

NS Power employees have been a key stakeholder audience throughout the Incident, as they were impacted as employees and as customers. Employees have received ongoing communications in the form of emails, in-person updates from senior leadership and from direct supervisors

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

throughout the response and restoration to date. Ahead of each public update related to the cyber investigation, employees were made aware of the latest information and what to expect in terms of public information, increased media coverage, and senior officials appearing before various provincial government committees. Where appropriate, employees were provided with Frequently Asked Questions (FAQs) to help answer their questions and help employees answer questions they were receiving from friends and family who are also customers of NS Power. In addition to updates related to the cyber response itself, employees were regularly updated about payroll, as the Company worked to restore payroll systems impacted by the Incident.

Due to the high volume of employee communications being shared in the early stages of response and restoration, a weekly summary email of all employee communications provided that week was also developed and shared with employees during the early stages of the Incident. As the Company's internal communications portal was impacted by the Incident and no longer available as a repository for employee updates, the Company established a new SharePoint site, accessible to all employees. This site continues to function as a key information resource for employees looking to read the latest update and find answers to FAQs.

As part of NS Power's communications to customers and stakeholders, additional key interest groups were also kept informed of key updates and milestones during the cyber response and investigation effort. These stakeholders included Efficiency Nova Scotia/E1, The Clean Foundation, the Independent Energy System Operator – Nova Scotia, representatives of the Affordable Energy Coalition, and key contacts within Nova Scotia's Mi'kmaw communities. NS Power also notified NERC, the Electricity Information Sharing and Analysis Center (E-ISAC), and the Northeast Power Coordinating Council, and provided them with information about the Incident.

As noted above, NS Power notified law enforcement of the Incident. More specifically, NS Power notified the Canadian Centre for Cybersecurity (CCCS), the Royal Canadian Mounted Police (RCMP), and the Canadian Security Intelligence Service (CSIS) on April 27, 2025 and provided

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

1 them with information about the Incident. Given the nature of the cyber attack and the critical
2 infrastructure nature of the company and the North American electric utility industry, the Company
3 also notified the Federal Bureau of Investigation (FBI).

4
5 NS Power also reported the Incident to the Office of the Privacy Commissioner of Canada (OPC)
6 on May 1, 2025, with an update on May 14, 2025.

7
8 **4.4 Response Analysis**
9

10 The Company considers that its response to the incident—encompassing containment,
11 remediation, and investigation—was effective and executed in a very timely and highly
12 coordinated manner, having regard to the severity and complexity of the attack.

13
14 The Company attributes the effectiveness of its response primarily to preparatory measures that
15 were in place prior to the Incident, including:

- 16
17 • the advance engagement and retention of experienced third-party cybersecurity and
18 incident-response experts, which ensured their immediate availability once the incident
19 was identified;
20 • reliance on high-caliber external expert advice and technical expertise throughout the
21 response and investigation;
22 • regular review and updating of incident-response plans and playbooks in advance of the
23 Incident; and
24 • the conduct of repeated tabletop and simulation exercises, which helped ensure that
25 personnel were familiar with their respective roles and responsibilities and supported an
26 orderly and efficient execution of response activities.

27
28 During the Incident response, governance structures and workstreams were clearly established,
29 and appropriately experienced and skilled subject-matter experts and decision-makers were

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 engaged from the outset. This facilitated timely escalation, prioritization of actions, and
2 coordinated decision-making. Internal communication and coordination among executive
3 leadership, relevant business units, and the Incident-response team functioned very effectively
4 throughout the Incident response period.

5
6 At the same time, the Company recognizes—as a matter of sound governance and consistent with
7 industry practice—that even an effective incident response will identify areas for refinement. The
8 Incident has provided NSP with valuable, practical, real-world insights that could not have been
9 fully replicated through planning or exercises alone.

10
11 Accordingly, and irrespective of its assessment of the effectiveness of the response, the Company
12 is treating the Incident as a learning exercise to further strengthen its preparedness and resilience.

13
14 Areas of focus for continuous improvement include:

- 15
- 16 • updating incident-response plans and playbooks to reflect observed, real-world conditions;
 - 17 • incorporating incident-specific lessons and scenarios that are difficult to anticipate fully
 - 18 through tabletop exercises; and
 - 19 • enhancing documentation to improve repeatability, training, and the Company's
 - 20 institutional knowledge for future responses.

21
22 The Company considers this continuous improvement approach to be an essential component of
23 responsible cybersecurity governance.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

5.0 COLLECTION AND RETENTION OF PERSONAL INFORMATION

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the collection and retention of personal information:

- A review of NS Power's policies and practices for the collecting, use and retention of personal information to identify any policy or compliance gaps that affected the type and amount of personal information exposed.¹³

At the time of the Incident, NS Power had formally documented its approach to privacy compliance through an established and robust suite of written privacy policies, procedures, and related documentation. In the wake of the Incident, NS Power is working to enhance its overall privacy governance framework and build on its existing privacy program (policy, procedures and standards) by taking the following actions:

- Ensuring the Company's privacy officer who, along with the privacy committee, will be responsible for:
 - clarifying expectations for all NS Power employees relating to data and privacy protection and cybersecurity and enhancing privacy training
 - enhancing the operationalization of the privacy program; and
 - further promote a culture of privacy and risk-based decision-making, where employees are encouraged to escalate and report privacy issues and there are clear reporting processes in place.

¹³ M12273, NSEB Letter, July 14, 2025, p. 2.

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

6.0 IMPACT ANALYSIS

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the impact analysis:

- Assessment of the breach's impact on NS Power, including financial, operational (including operation of the grid and its communication with customers such as AMI meters, outage map, web-based customer service interfaces, and service connection requests), and reputational damage.
- Evaluation of the potential harm to NS Power's existing and former customers, and employees.¹⁴

NS Power addresses each in this section.

6.1 Impact

NS Power financial and internal operational impacts noted by the Board above have been reported in the Company's monthly Incident update reports and in the preceding sections, as well as our publicly available financial statements. Please also refer to **Appendices A** and **B** for a list of systems affected and affected regulatory matters, respectively. As noted above, with respect to the operation of the grid, the Company continues to have no evidence the threat actor accessed any operational technology or energy delivery systems. Core operations and the electric grid continued uninterrupted – no power was lost to Nova Scotians.

NS Power is aware of the concerns this incident has caused for customers and is committed to restoring trust with its customers. Peter Gregg addressed this in his opening statement to the Standing Committee on Natural Resources and Economic Development on November 25, 2025:

¹⁴ M12273, NSEB Letter, July 14, 2025, p. 2.

2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED

At Nova Scotia Power, our commitment to providing reliable power to Nova Scotians has been unwavering for over 100 years. We recognize that the recent cyber event has affected the trust we have built with our customers, and I want to acknowledge and apologize for the concern and disruption this has caused.

Over the past 215 days, our team has worked around the clock to restore and strengthen our systems and to support our customers. And we recognize that the cyber incident continues to impact our customers, including concerns about estimated bills. To you the committee, and to all Nova Scotians, my promise to you is if we have overestimated your bill, we will fix it. If you have overpaid, we will fix it. And if we make a mistake, we will fix it.

//

Most importantly we remain focused on the impact this has had on Nova Scotians. We understand the ongoing challenges related to billing, payments to our suppliers, and longer wait times to speak with our care team, and we are working diligently to resolve them. Restoring all systems will take time, but we are providing flexible options for our customers – such as equal billing, pay-what-you-can arrangements, and photo meter reads – until we're able to reconnect our systems and provide up-to-date bills.

Except for tax reporting purposes, we no longer collect social insurance numbers and are on track to complete their removal from our systems by March 31st. We are also on track to reconnect customer meters with our billing systems by the end of March. Our team has worked to address outstanding payments to suppliers, and we expect to be caught up on these payments before the end of the year.

//

In closing, I want to reiterate our commitment to supporting Nova Scotians, minimizing the impact of this incident, and rebuilding trust. We do not take this responsibility lightly. Again, my promise to you is if we have overestimated your bill, we will fix it. If you have overpaid, we will fix it. And if we make a mistake, we will fix it.¹⁵

Please also refer to section 4.2 above for full details on how NS Power is addressing impacted customers and their concerns.

¹⁵ Peter Gregg, President & CEO, Nova Scotia Power, Opening Statement to the Standing Committee on Natural Resources and Economic Development, November 25, 2025.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

6.2 Assessment of Potential Harm

As outlined above, NS Power determined through its investigation that certain customer information stored on the impacted servers was accessed and taken by an unauthorized third party. However, while NS Power recognizes the potential impact the Incident may have had on customers, Nova Scotia Power continues to have no evidence that this information has been further misused, or of any financial harm to customers resulting from this Incident.

The Company adopted a best-practices approach to mitigating potential harm to customers whose personal information was impacted by the Incident. This approach was grounded in a commitment to transparency, timely communication, and a customer-centric focus, as described in detail above in Section 4.2. The Company's objective throughout has been to provide affected individuals with meaningful support, reduce the risk of harm, and maintain trust.

As also noted above, the Incident has not caused any disruption to physical operations at NS Power's generation, transmission and distribution facilities, and the Incident has not impacted the Company's ability to safely or reliably serve customers in Nova Scotia.

The Incident caused a severe, adverse impact on the Company's billing systems, and NS Power recognizes that concerns have been raised about the Company's estimated billing process. The Company is treating these concerns very seriously. In the immediate response to the Incident, NS Power committed and confirmed that customers would not be charged late fees or have their service disrupted as a result of this Incident. NS Power is committed to addressing these impacts, and to alleviating the concern and disruption it has caused customers. NS Power has never intentionally overbilled its customers and has been steadfast and consistent in its commitment to customers that it is actively trying to address the issues and, where mistakes have been made, they will be fixed.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 NS Power continues to work with customers to offer payment options. The Company encourages
2 any customers who have concerns to call the Customer Care Centre. Restoring all systems will
3 take time, but the Company is providing flexible options for customers—such as Equal Billing,
4 pay-what-you-can arrangements, and photo meter reads—until NS Power is able to reconnect the
5 systems and provide up-to-date bills.

6

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

7.0 M12457 DIRECTION

As noted in the introduction, the NSEB directed NS Power to address the broader review outcomes arising from M12457. Each of the Board's questions are addressed in turn in Appendix C.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

8.0 RECOMMENDATIONS

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the recommendations:

- Recommendations for, among other things:
 - enhancing NS Power's security measures and preventing future breaches.
 - additional security audits, policy updates, and employee training.
 - implementing new strategies and proactive measures to strengthen NS Power's cybersecurity defenses.
 - improving communications and responsiveness to the concerns and needs of NS Power's impacted customers.
 - strengthening and addressing gaps in the collection and retention of personal information.¹⁶

Each is addressed in turn below.

8.1 Enhancing Security Measures and Preventing Future Breaches

NS Power has taken the following steps to enhance its cybersecurity environment to facilitate the prevention of future breaches:



¹⁶ M12273, NSEB Letter, July 14, 2025, p. 2.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29

[REDACTED]

Ongoing steps to enhance NS Power's cybersecurity environment include the following:

[REDACTED]

Key additional remediation and restoration efforts include:

[REDACTED]

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

8.2 Additional Security Audits, Policy Updates, and Employee Training

Section 4.1 addressed additional security audits, policy updates, and employee training as summarized below.

Regarding security audits, NERC conducts extensive periodic audits (including security) of the Company's Energy Operations to ensure effective compliance. In addition, as noted in the Company's Incident monthly updates, the Office of the Privacy Commissioner of Canada (OPC) has initiated an investigation into the Incident, which remains ongoing. The Company continues to fully cooperate with the OPC and remains committed to addressing the OPC's concerns and resolving the investigation in an efficient and expeditious manner.

Regarding policy updates, NS Power had implemented a common set of cybersecurity standards and policies that are informed, in part, by the NIST Cybersecurity Framework, and the Company regularly reviews and makes continuous improvements to its cybersecurity programs to ensure it is in line with the latest guidance. In connection with these efforts, NS Power has recently completed an extensive two-year update to its cybersecurity practices to comply with current policies and anticipated changes in standards communicated by NIST.

Regarding employee training, NS Power maintains a cybersecurity training and awareness program and conducts mandatory quarterly cyber training and monthly phishing simulation testing exercises with all employees to educate employees about NS Power's information security policies and common risks, and to help them understand their information security responsibilities.

8.3 New Strategies and Proactive Measures

With respect to new strategies and proactive measures, please refer to section 8.1 above.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

8.4 Customer Communications

With respect to improving communications and responsiveness to the concerns and needs of NS Power's impacted customers, as noted in section 4.2 above, the Company adopted a best-practices approach to mitigating potential harm to customers whose personal information was impacted by the Incident. This approach was grounded in a commitment to transparency, timely communication, and a customer-centric focus. The Company's objective throughout has been to provide affected individuals with meaningful support, reduce the risk of harm, and maintain trust.

NS Power took the following actions:

- Conducted a consistent multi-channel public communications approach throughout the response efforts.
- Conducted a multi-platform paid media/advertising strategy.
- Implemented a paid search strategy throughout the Incident to ensure that the NS Power website and information appeared as the top search result when customers used search engines (i.e. Google) to find information about the Incident.
- Updated and monitored social media accounts and, where appropriate, provided answers to related customer questions online.
- Provided customers the ability to speak directly with NS Power customer care representatives on the phone and via email throughout the Incident for any questions or concerns.
- Notified affected individuals, including retaining third-party service providers to assist with this effort.
- Provided guidance to customers for steps they could take to reduce any risk of harm resulting from the incident (including steps to protect themselves from fraud or potential identity theft). This notice included an offer for two years of complimentary credit

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 monitoring and identity monitoring services for impacted individuals. The Company
2 subsequently extended the offer of complimentary credit monitoring to five years on June
3 25, 2025. Customers who had already registered for credit monitoring had their offer
4 automatically extended.

- 5 • Established a dedicated call centre where individuals could receive more information about
6 the Incident, and support for credit monitoring sign-ups, whose number was included in
7 the notice letters and made available to customers.
- 8 • Staffed this call centre with TransUnion employees who had been provided with prepared
9 responses from NS Power and instructed to escalate any queries that could not be addressed
10 to the Company so that customers could receive a call-back from the NS Power customer
11 service team.
- 12 • Provided guidance on registering for credit monitoring posted online and made available
13 in locations throughout the province.
- 14 • Created a fact sheet with information about the service and tips for signing up.
- 15 • Distributed and made available thousands of fact sheet paper copies to customers across
16 the province through customer support sessions at community locations. In addition, the
17 fact sheet was available at NS Power local depots and provided to MLAs and local
18 councilors.
- 19 • Deployed dozens of employees to communities across the province to provide hands-on
20 support for customers.
- 21 • Updated the NS Power website and social media channels also with additional tips and
22 tools to help customers navigate support services.

23
24 NS Power continues to keep customers updated regarding the ongoing incident and investigation.
25 In summary, at this time, Nova Scotia Power has sent direct notifications to approximately 375,000
26 customers who have been identified as being impacted in this incident.
27

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

8.5 Collection and Retention of Personal Information

At the time of the Incident, NS Power had formally documented its approach to privacy compliance through an established and robust suite of written privacy policies, procedures, and related documentation, including which govern its collection, use and retention of personal information.

As described in Section 5, in the wake of the Incident, NS Power is working to enhance its overall privacy governance framework and build on its existing privacy program.

With respect to the collection and retention of customer social insurance numbers, as noted in Peter Gregg's opening statement to the Standing Committee on Natural Resources and Economic Development on November 25, 2025, appended to NS Power's December 1, 2025 Incident monthly update report, "Except for tax reporting purposes, we no longer collect social insurance numbers and are on track to complete their removal from our systems by March 31st."¹⁷

Prior to 2018, it was NS Power's practice to collect social insurance numbers (SINs) from customers as part of authentication and identification of a customer during the account opening process. In 2018, NS Power changed that practice and no longer collected SINs (except in limited circumstances detailed below).

Subsequently in 2019, Customer Service Representatives were instructed to remove SINs for the Customer Information System (CIS) whenever a SIN was encountered within CIS. In May of 2024, NS Power developed and commenced a process to purge customer SINs from the CIS environment.

In limited circumstances, NS Power continued to collect SINs from customers where there was a legal requirement to do so. SINs continued to be collected for tax reporting purposes where NS

¹⁷ Peter Gregg, President & CEO, Nova Scotia Power, Opening Statement to the Standing Committee on Natural Resources and Economic Development, November 25, 2025.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 Power was required to issue a T5 in connection with interest over \$50 earned in a year on a
2 customer deposit.

3
4 In 2021, Nova Scotia Power initiated a customer energy management program called MyEnergy
5 Insights to better inform customers of their energy usage patterns. The MyEnergy Insights program
6 required a daily export of customer information from NS Power's CIS into a staging area within
7 NS Power's Azure environment (cloud storage environment). Within this staging area, certain
8 daily exports from July 2021 were targeted by the threat actor for exfiltration. It is important to
9 note that all data within the Azure environment was (and is still) encrypted at rest with only
10 approved users having authorized access to that environment. Based on the investigation, the
11 Company believes that the data exported to the Azure staging area for the MyEnergy Insights
12 program in July 2021 included the SINs (and other personal information) of certain NS Power
13 customers and was among the data that was targeted for exfiltration by the threat actor. Upon
14 discovery by the Company, the Azure storage was immediately locked down.

15
16 On June 25, 2025, Nova Scotia Power publicly committed to permanently deleting instances of
17 SINs that remained in the Company's systems. The Company has initiated a process to identify
18 and remove instances of SINs contained within its records. This search has progressed significantly
19 and is being conducted with the assistance of external experts. Except where SINs are legally
20 required for tax reporting purposes, any such information identified will be securely deleted. NS
21 Power anticipates obtaining confirmation of its completion of this process by March 31, 2026.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

9.0 CONCLUSION

NS Power trusts that the foregoing addresses the NSEB's direction with respect to the information requested in its letters of July 14, 2025 and November 7, 2025.

NS Power experienced a sophisticated cyberattack discovered on April 25, 2025, with evidence of unauthorized access beginning around March 19, 2025. While customer and Company data was exfiltrated and internal business technology systems were affected, there is no evidence that operational technology or energy delivery systems were accessed or disrupted. NS Power activated incident response and business continuity protocols, engaged Mandiant under counsel, and notified CCCS, RCMP, CSIS, and the FBI; the Company also reported the incident to the Office of the Privacy Commissioner of Canada and continues to cooperate with their investigation.

To protect and inform customers, NS Power issued staged notifications while also advising former customers and expanding the complimentary offer of TransUnion credit and identity monitoring to five years (which includes protective measures such as access to identity restoration services, and up to \$1,000,000 of expense reimbursement insurance related to identity theft). The Company has also maintained a multi-channel communications program, established a dedicated call center staffed by TransUnion, and provided in-person community support, guidance, and dark-web monitoring updates as the investigation proceeded.

Recovery and resilience efforts continue, including [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Consistent with commitments made publicly, NS Power is eliminating SINS from systems (except for limited legal requirements) and is working to reconnect customer meters to billing systems; ongoing progress, system restoration timelines, and Board-related matters are tracked in the appended charts and monthly updates.

**2025 Nova Scotia Power's Cybersecurity Incident Report
REDACTED**

1 Finally, NS Power submits that many of the Premier's requests of the NSEB by letter on December
2 3, 2025 have been already addressed through the various materials provided as part of this
3 proceeding, or will be as part of future proceeding deliverables, including NS Power responses to
4 Board IRs issued on December 3, 2025. Given the relation of the billing concerns to the Incident,
5 it is appropriate to have them considered as part of this process.

REDACTED

Request IR-1:

Please provide a timeline of this cybersecurity incident, including:

- (a) the date of the breach;**
- (b) the date suspicious activity was discovered;**
- (c) the date the cyber breach was confirmed;**
- (d) the date law enforcement and cybersecurity agencies were notified;**
- (e) the date all public or media releases were issued by the utility (including copies of the releases or updates); and**
- (f) the date of all public media interviews provided by any member of the utility's senior management team, including particulars of each.**

Response IR-1:

(a-d) The investigation of this cybersecurity incident (Incident) remains ongoing. The information in this response reflects NS Power's current understanding of the Incident.

The Incident involved a sophisticated and coordinated cyberattack on certain of NS Power's information technology systems and data.

The Incident was discovered on April 25, 2025, when NS Power employees reported certain applications on the Company's systems were not functional. Upon immediate investigation, it became evident that a threat actor had gained unauthorized access into

REDACTED

1 certain parts of NS Power's information technology network and servers which support
2 portions of its business applications.

3
4 Immediately following detection of the Incident, NS Power activated its established
5 incident response and business continuity protocols, and engaged Osler, and through Osler,
6 Mandiant's cybersecurity and incident response team.

7
8 Under the direction of Osler, Mandiant assisted the Company and other cybersecurity
9 experts with containment, investigation, and remediation efforts, and took immediate
10 actions to contain and remediate the unauthorized activity, including containing and
11 isolating affected servers, limiting network connectivity, identifying and resetting
12 compromised account credentials, and hardening the environment. Teams within NS
13 Power also began working diligently with cyber security experts to isolate the operational
14 technology and energy delivery systems. The Company has no evidence the threat actor
15 accessed any operational technology and energy delivery systems.

16
17 Based on the investigation to date, the Company believes that an unauthorized third party
18 gained access on or around March 19, 2025 and, beginning on or around April 25, 2025,
19 exfiltrated certain data, including personal information of the Company's customers.

20
21 NS Power notified law enforcement of the Incident. More specifically, NS Power notified
22 the Canadian Centre for Cybersecurity (CCCS), the Royal Canadian Mounted Police
23 (RCMP), and the Canadian Security Intelligence Service (CSIS) on April 27, 2025 and
24 provided them with information about the Incident. Given the nature of the cyber attack
25 and the critical infrastructure nature of the company and the North American electric utility
26 industry, the Company also notified the Federal Bureau of Investigation (FBI).

27
28 NS Power also reported the Incident to the Office of the Privacy Commissioner of Canada
29 (OPC) on May 1, 2025, with an update on May 14, 2025.

REDACTED

1 The OPC initiated an investigation into the Incident on May 28, 2025, and the Company is
2 actively and fully cooperating with the OPC to support the OPC's investigative efforts.

3 The Company has also provided updates to the Nova Scotia Energy Board, as well as other
4 relevant government officials throughout the Incident and investigation.

5
6 The Incident has not caused any disruption to physical operations at NS Power's
7 generation, transmission and distribution facilities, and the Incident has not impacted the
8 Company's ability to safely or reliably serve customers in Nova Scotia.

9
10 **Transparency and Steps Taken to Reduce Risk of Harm**

11
12 The Company adopted a best-practices approach to mitigating potential harm to customers
13 whose personal information was impacted by the Incident. This approach was grounded in
14 a commitment to transparency, timely communication, and a customer-centric focus. The
15 Company's objective throughout has been to provide affected individuals with meaningful
16 support, reduce the risk of harm, and maintain trust.

17
18 The Company's robust transparency effort is evidenced by the public communications that
19 NS Power has engaged in throughout the Incident.

20
21 NS Power developed and implemented a consistent multi-channel approach throughout the
22 response efforts for all public communications. For each update, the transparency effort
23 involved postings on the Company website and social media channels, notice to all local
24 media, and communications directly to key account/business customers, government and
25 other stakeholders in addition to employees.

26
27 The Company also employed a multi-platform advertising strategy that includes online
28 media, as well as TV, print and radio to reach a wide variety of customer demographics. In
29 addition, NS Power activated a paid search strategy throughout the Incident to ensure that

REDACTED

1 the NS Power website and information appeared as the top search result when customers
2 used search engines (i.e. Google) to find information about the Incident. Social media
3 accounts have been regularly monitored, and where appropriate, the Company has provided
4 answers to related customer questions online. The Customer Care Centre remained fully
5 operational and available during the Incident and customers were also able to speak directly
6 with NS Power customer care representatives on the phone for any questions or concerns.

7
8 **Customer Notification Timeline**

9
10 As noted above, the Company became aware of the Incident on Friday, April 25. The next
11 business day, on Monday, April 28, 2025, NS Power informed customers that it was
12 actively responding to a cybersecurity incident, and encouraged customers to report any
13 suspicious emails or phone calls.

14
15 On May 1, 2025, NS Power determined that customer information had been impacted in
16 the Incident, and promptly updated customers to inform them that they had identified that
17 certain customer personal information had been impacted in the Incident, and again
18 encouraged them to remain vigilant and cautious of unsolicited communications and
19 potential scams. The Company informed customers that they were working urgently to
20 determine the full nature and scope of the data that may have been affected. The Company
21 also initiated the process of notifying affected individuals, including retaining third-party
22 service providers to assist with this effort.

23
24 On May 13, 2025, NS Power sent notices to approximately 277,000 current customers
25 whose personal information the Company was able to determine had been impacted in this
26 incident.

27
28 The following morning (May 14, 2025), the Company also issued a press release, and
29 provided a detailed update on its website and social media pages, all of which received

REDACTED

1 widespread coverage in the local and national media. Senior Company personnel
2 participated in multiple media interviews to ensure that the public remained informed about
3 the Incident.

4
5 The process to identify what data was impacted has been extremely complex and remains
6 ongoing. As set out in the notices sent to impacted customers, the impacted data would
7 have varied by customer, and depended, in part, on the information a customer would have
8 provided NS Power (i.e. not all personal information elements would have been impacted
9 for all notified customers).

10
11 The Company stated in its notice to impacted customers that the unauthorized third party
12 gained access to various types of personal information of our customers that included the
13 following: name, phone number, email address, mailing and service addresses, NS Power
14 program participation information, date of birth, and customer account history (such as
15 power consumption, service requests, customer payment, billing, and credit history, and
16 customer correspondence), driver's license number, and social insurance number. For
17 some customers, bank account numbers (for pre-authorized payment) may also have been
18 impacted if this information was provided by these customers. With respect to direct
19 notifications, the Company sent two versions of letters to impacted current customers,
20 samples of which are attached. Please refer to Attachments 1 and 2. The notices are
21 identical, except that one of the notices indicates that based on the investigation, the
22 customer's social insurance number may have been impacted in the Incident.

23
24 NS Power's notice to impacted customers also included guidance for steps they could take
25 to reduce any risk of harm resulting from the incident (including steps to protect themselves
26 from fraud or potential identity theft). This notice included an offer for two years of
27 complimentary credit monitoring and identity monitoring services for impacted
28 individuals. The Company subsequently extended the offer of complimentary credit
29 monitoring to five years on June 25, 2025.

REDACTED

1 The credit monitoring service offered to customers is provided by TransUnion and has been
2 specifically designed to protect individuals in the case of a data breach, and offers them
3 access to the following protective features:

- 4
5 • Unlimited online access to their TransUnion Canada credit report, updated daily,
6 which offers individuals access to the individual's financial history and is one of
7 the primary tools leveraged for determining credit-related identity theft or fraud.
8
- 9 • Unlimited online access to their credit score, updated daily.
10
- 11 • Credit monitoring, which provides individuals with email notifications to key
12 changes on an individual's TransUnion Canada credit report. These credit alerts
13 help protect individuals against identity theft, enable quick action against
14 potentially fraudulent activity and provide them with additional reassurance.
15
- 16 • Access to online educational resources concerning credit management, fraud victim
17 assistance and identity theft prevention.
18
- 19 • Access to Identity Restoration agents who are available to assist individuals with
20 questions about identity theft. In the unlikely event that an individual becomes a
21 victim of fraud, a personal restoration specialist will help to resolve any identity
22 theft.
23
- 24 • Up to \$1,000,000 of expense reimbursement insurance related to identity theft.
25
- 26 • Dark Web Monitoring, which monitors surface, social, deep, and dark websites for
27 potentially exposed personal, identity and financial information and helps protect
28 individuals against identity theft.
29

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

1 Thereafter, NS Power continued to keep customers updated regarding the ongoing incident
2 and investigation.

3
4 On May 22, 2025, after discovering that the threat actor had published data on the dark
5 web, NS Power promptly provided an update to customers through the same channels as
6 previous updates.

REDACTED

1 **Former Customers**

2
3 As the Company continued its investigation of the impacted data, NS Power determined
4 that personal information relating to former customers had also been impacted by the
5 Incident.

6
7 On June 25, 2025, NS Power notified the public that information related to former
8 customers had also been impacted in the Incident. In addition, out of an abundance of
9 caution, and in the interest of assisting customers further to mitigate the potential harm to
10 current and former customers arising from the Incident, NS Power proactively extended
11 the credit monitoring offer to five years for all current and former customers.

12
13 Given that NS Power does not have updated contact information for its former customers,
14 and given that NS Power was still working to determine the full scope of the data that may
15 have been impacted, the Company worked to share this indirect notification as broadly as
16 possible. In addition to its website, NS Power actively shared this information with media,
17 on social media, with stakeholders, through paid advertising, as well as national paid search
18 optimization, to reach as many current and former customers as possible.

19
20 **Customer Support and Dedicated Call Centres**

21
22 Promptly upon becoming aware of the Incident, NS Power established a dedicated call
23 centre where individuals could receive more information about the Incident, and support
24 for credit monitoring sign-ups, whose number was included in the notice letters and made
25 available to customers.

26
27 As is standard in incidents of this nature, to ensure that the call centre had sufficient
28 capacity to handle the volume of calls and allow NS Power's customer service team to
29 focus on a subset of escalated queries, this call centre was staffed by TransUnion

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

1 employees who had been provided with prepared responses from NS Power, and instructed
2 to escalate any queries that could not be addressed to the Company so that customers could
3 receive a call-back from the NS Power customer service team. This also allowed customers
4 to connect directly with TransUnion for assistance in signing up for credit monitoring (and
5 a dedicated phone line for questions about the credit monitoring process was included with
6 the instructions provided to customers in their letter).

7
8 Having TransUnion operate the call centre enabled flexible staffing to accommodate the
9 initial high volume of calls, and reassignment of call centre staff as call volumes dropped.

10
11 When a customer requested a call back, or had questions that could not be answered by the
12 prepared information provided to the call centre staff, a list of customer call back requests,
13 with relevant information, was provided to NS Power on a daily basis, whose customer
14 care team would reach out to these customers.

15
16 To assist current and former customers with the sign-up process, guidance on registering
17 for credit monitoring has been posted online and made available in locations throughout
18 the province. This guidance includes information on additional measures customers can
19 take to protect themselves against identity theft, as well as details on other available
20 services.

21
22 A fact sheet was also created with information about the service and tips for signing up.
23 Thousands of paper copies were distributed and available to customers across the province
24 through customer support sessions at community locations. In addition, the fact sheet was
25 available at NS Power local depots and provided to MLAs and local councilors. NS Power
26 has also actively encouraged customers and its employees to reach out to their family and
27 neighbours to encourage them to sign up. Please refer to Attachment 3.

REDACTED

1 In addition, the Company deployed dozens of employees to communities across the
2 province to provide hands-on support for customers who prefer assistance in person,
3 recognizing that not all customers may be comfortable registering online, and to ensure
4 that customer needs are being met and access to services being granted. More than 30 of
5 these community sessions have been held to date, and have assisted hundreds of customers
6 in signing up for the service. The NS Power website also has been updated with additional
7 tips and tools to help customers navigate support services.

8
9 **Existing Safeguards**

10
11 At the time of the Incident, NS Power had implemented a common set of cybersecurity
12 standards and policies that are informed, in part, by the National Institute of Standards and
13 Technology's (NIST) Cybersecurity Framework, and the Company regularly reviews and
14 makes continuous improvements to its cybersecurity programs to ensure it is in line with
15 the latest guidance. In connection with these efforts, NS Power has recently completed an
16 extensive two-year update to its cybersecurity practices to comply with current policies
17 and anticipated changes in standards communicated by NIST.

18
19 NS Power's cybersecurity framework (which applies to its information technology
20 program more generally) includes specific policy and control standards aligned with
21 NIST's Core Functions as noted below.

22
23 In relation to NS Power's operational program, NS Power's core energy operations are
24 designed to comply with other industry-specific rules and standards relating to
25 cybersecurity and IT including, but not limited to, those mandated by the North American
26 Electric Reliability Corporation (NERC). NERC conducts extensive periodic audits
27 (including security) of the Company's Energy Operations to ensure effective compliance.
28

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

1 NS Power maintains a cybersecurity training and awareness program and conducts
2 mandatory quarterly cyber training and monthly phishing simulation testing exercises with
3 all employees to educate employees about NS Power's information security policies and
4 common risks, and to help them understand their information security responsibilities.
5

REDACTED

Incident Response and Remediation:

Immediately following detection of unauthorized access, NS Power activated its incident response and business continuity protocols, engaged leading third-party cybersecurity experts, and took actions to contain and isolate the affected servers and prevent further intrusion.

Since the discovery of the event, NS Power has mobilized a team of internal and external specialists to support the recovery effort. The Company's immediate priorities have focused on containment, eradication and remediation of the threat, and conducting a thorough analysis to understand the full scope and nature of the Incident.

Immediate remediation actions were taken, including:



Further intermediate remediation steps that have been taken include:



Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

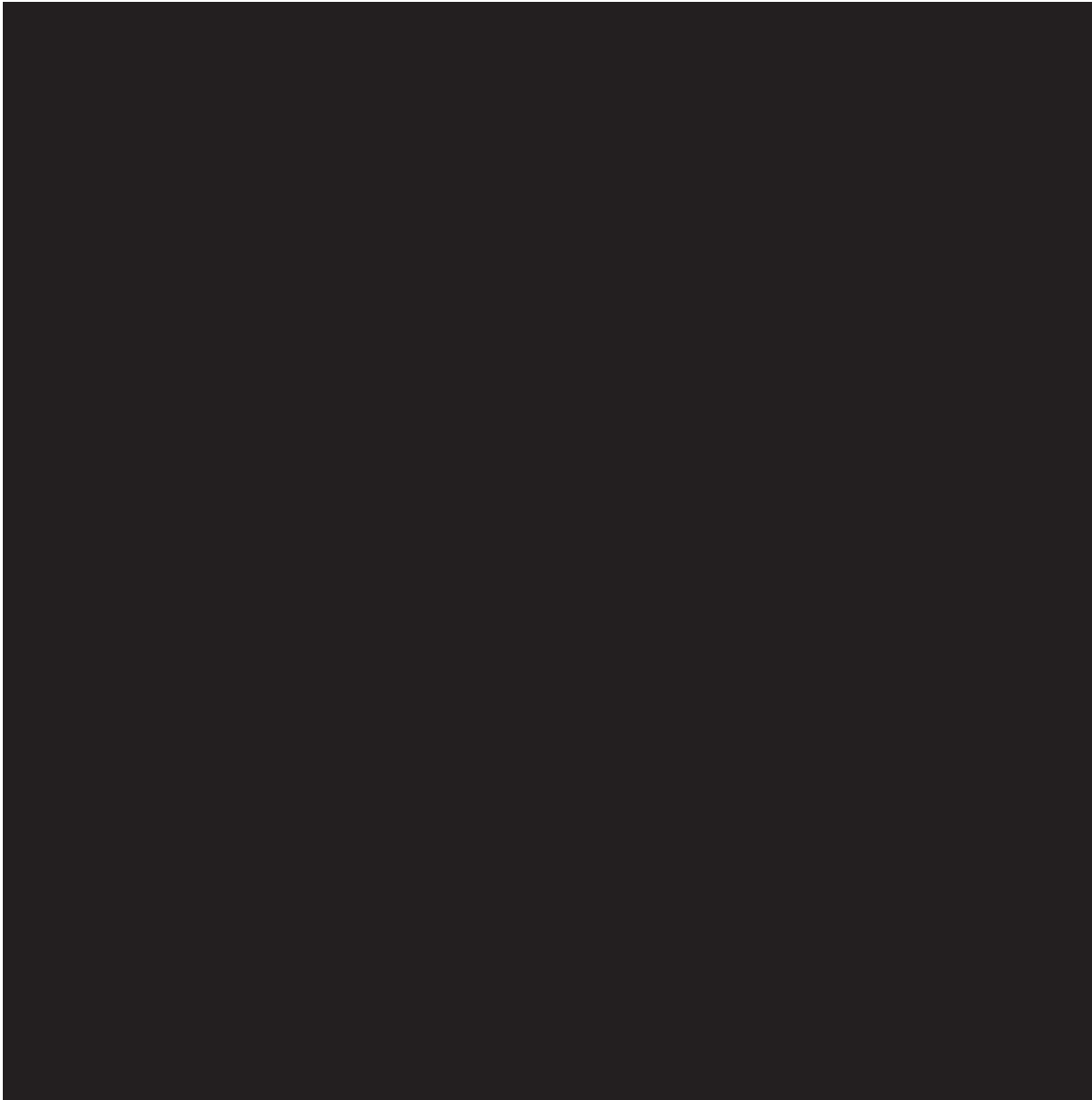
Ongoing remediation steps include:

NS Power is also advancing efforts to restore and, where necessary, rebuild core business applications and infrastructure—including finance, human resource, procurement, and customer billing systems, and integrations between those systems and other supporting systems—by leveraging secure backups and reestablishing security and monitoring protocols across their systems. These recovery efforts are focused on ensuring continuity and stability for the Company's business operations and customers.

To coordinate work streams on business restoration and information security strengthening efforts, a business restoration process office has been established within NS Power. Restoration efforts are continuing, and [REDACTED] has been retained as a strategic partner and systems integrator to assist in this process.

Key additional remediation and restoration efforts related to strengthening the Company's cyber security systems include:

REDACTED



(e) NS Power initially notified customers of the Incident on Monday, April 28, 2025 as noted above.

NS Power continued to provide regular notifications and updates to customers throughout the next several weeks of response efforts.

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

1 These communications and releases to media occurred on the following dates:

- 2
- 3 • Monday, April 28, 2025
 - 4 • Thursday, May 1, 2025
 - 5 • Wednesday, May 14, 2025
 - 6 • Friday, May 23, 2025
 - 7 • Wednesday, June 4, 2025
 - 8 • Wednesday, June 25, 2025
- 9

10 Customers can access these public/media updates via a banner on the NS Power homepage
11 labeled “[Cyber Incident Updates](#)”, which directs viewers to a dedicated subpage where the
12 updates are listed in chronological order. Please refer to Attachment 4.

13

14 These updates were communicated through various channels, including social media, the
15 Company website, direct notification to officials and other stakeholders and direct email
16 through the Company’s provincial media distribution list. This provincial media
17 distribution list includes roughly 140 addresses reaching media outlets (television, radio,
18 print and digital) as well as individual reporters and various assignment desks across the
19 province.

20

21 On June 4, 2025, Peter Gregg, NS Power President & CEO, was joined by Chris Lanteigne,
22 NS Power Director of Customer Care and Chris Heck, the Chief Digital Officer of NS
23 Power’s parent company, Emera, to appear before the Standing Committee on Public
24 Accounts at the NS Legislature to answer questions about the Cyber Incident in a live
25 streamed session. Following this two-hour session with elected officials, Peter Gregg made
26 himself available and spoke to media gathered outside the legislative chamber.

27

REDACTED

1 Additionally, proactive notifications went to the following local media outlets to share
2 information about upcoming customer support sessions in local communities to help
3 customers sign up for the free credit monitoring being offered by the company.
4

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

Cape Breton – Monday, June 30, 2025

- The Coast 89.7FM Radio - Sydney - news@coastalradio.ca
- MBS Radio – Sydney - cbmail@mbsradio.com
- New Country 103.5FM - news@newcountry1035.ca
- CBC CB – Info Morning – Sydney - nicole.maclennan@cbc.ca; with an offer to interview our Director of Customer Care

Springhill, Cumberland County – Thursday, July 3, 2025

- 101.7 FM CKDH
- CFTA Tantramar 107.9 FM - cfta@eastlink.ca

Yarmouth - Tuesday, July 8

- Outlets: CJLS Radio - news.cjls@radioabl.ca

Bridgewater – Wednesday, July 9

- Outlets: CKBW Radio – ckbwnews@radioabl.ca; northupk@radioabl.ca and CJHK 100.7FM Country (Atlantic Broadcasting)

Millbrook – Thursday, July 10

- Outlets: CKYT Cat Country (MBS Radio) – MNN@MBSradio.com
- CKTO EZ Rock (MBS Radio)

From July 8-11, 2025, NS Power responded to several media inquiries about customer bills and meter readers being hired to manually read meters at homes and businesses across the province. This media response included NS Power's Director of Customer Care, Chris Lanteigne participating in interviews with CBC NS and CBC Information Morning Mainland (noted in chart below), as well as information being shared with AllNovaScotia.com, Global Halifax, MBS Radio, Halifax Examiner and the Chronicle Herald.

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests**REDACTED**

The Company also initiated proactive outreach to local radio stations across the province to advise customers of this work and avoid any confusion or concern about meter readers entering their properties to read meters. Below is the list of stations that were contacted with a response rate of 60 percent.

Station	Contact
WEST	
Bridgewater: CKBW Country 100.7FM	ckbwnews@radioabl.ca ; northupk@radioabl.ca
Yarmouth: CJLS	news.cjls@radioabl.ca
Liverpool: QCCR 99.3 FM	news@qccrfm.com
Kentville/New Minas: 89.3 Rewind 94.9 Magic (MBS) 97.7 AVR (MBS)	info@rewind893.ca mnn@mbsradio.com / mbsnews@mbsradio.com mnn@mbsradio.com / mbsnews@mbsradio.com
EAST	
Antigonish: CJFX-FM 98.9 Antigonish	news@989xfm.ca Ken Kingston, News Director
Port Hawkesbury: 101.5FM	news@1015thehawk.com
Sydney: The Coast 89.7FM Radio (CKOA) MBS Radio New Country 103.5FM	news@coastalradio.ca - cbmail@mbsradio.com news@newcountry1035.ca
NORTHEAST	
Amherst: CFTA Tantramar 107.9 FM	cfta@eastlink.ca
Truro: CKYT Cat Country (MBS Radio)	MNN@MBSradio.com or: mbsnews@mbsradio.com

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

Station	Contact
& CKTO EZ Rock (MBS Radio)	
New Glasgow: CKEZ 97.9FM	newglasgownews@stingray.com
Pictou County: CKEC 94.1FM The Breeze	sgeorge@stingray.com
METRO	
Halifax: Surge 105FM (CKHY) & Hot Country 103.5FM	news.CKHZ@radioabl.ca (both newsrooms)
Eastern Passage: Seaside FM	news@seasidefm.com
Hubbards: COVE FM (88.7) Community Radio Station	info@covefm.com

Advertisements were also placed in approximately 15 local and provincial newspapers across the province to ensure broader reach to demographics within the province. A sample ad is provided below.

Meter Reading in Your Community

Over the summer you may see members of the Nova Scotia Power team reading meters on homes and businesses in your community.

Meters have continued to accurately record energy use throughout the cyber incident but are unable to send that information back to our billing systems right now. As a result, when billing resumed, most customers started receiving estimated bills based on past use. To provide customers with a bill based on actual energy use, rather than an estimate, Nova Scotia Power has temporarily returned to physical meter reading.



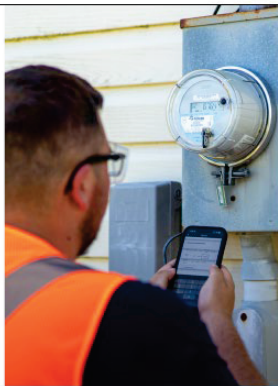
Meter readers wear Nova Scotia Power branded clothing and carry an ID badge. You do not need to be home for your meter to be read.



For more information visit
nspower.ca/billing



Nova Scotia
POWER
An Entera Company



Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests**REDACTED**

(f) Please see the following table for details on public interviews provided:

Date	Media Outlet	Format	Reporter	Member of NSP senior leadership team	Topic
May 23, 2025	CBC	TV	Amy Smith, Anchor recorded sit-down interview	Peter Gregg, President and CEO	Cyber incident update
May 23, 2025	CBC Mainstreet	Radio	Jeff Douglas (live/on air)	Peter Gregg, President and CEO	Cyber incident update
May 23, 2025	allnovascotia.ca	Print/Online	Gillian Cormier	Peter Gregg, President and CEO	Cyber incident update
May 29, 2025	Canadian Press	Print/Online	Mike Tutton	Peter Gregg, President and CEO	Cyber incident update
May 29, 2025	CTV	TV	Todd Battis	Peter Gregg, President and CEO	Cyber incident update
May 30, 2025	CBC Info Morning	Radio	Portia Clarke	Peter Gregg, President and CEO	Cyber incident update
June 17, 2025	CTV	TV	Ryan MacDonald	Chris Lanteigne, Director Customer Care	Cyber incident update Customer support sessions in communities across NS
June 17, 2025	CBC Information Morning Mainland (recorded to air June 18)	Radio		Chris Lanteigne, Director Customer Care	Billing/customer support sessions for credit monitoring

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

REDACTED

July 9, 2025	CBC Nova Scotia	Radio	Elizabeth McMillan	Chris Lanteigne, Director Customer Care	Cyber incident update Billing concerns Customer support sessions in communities across NS
July 11, 2025	CBC Nova Scotia – Information Morning Mainland (to air Monday, July 13)	Radio	Taryn Grant	Chris Lanteigne, Director Customer Care	Meter Readers & Community Sessions (also asked about cyber incident)



PO Box 910 Halifax,
Nova Scotia B3J 2W5



00766-ADFSON L001 AUTO *000001



Re: Important Notice About Your Personal Information

Dear Valued Customer:

We are writing to provide you with information about the recent cyber incident impacting Nova Scotia Power.

On April 25, 2025, Nova Scotia Power discovered that an unauthorized third party had gained access to certain parts of its Canadian network and servers.

Immediately following detection of the external threat, we activated our incident response and business continuity protocols, engaged external cybersecurity experts, commenced a thorough investigation, and took actions to contain and address the unauthorized activity. We have also notified law enforcement and regulatory authorities about this cyber incident.

While the investigation remains ongoing, we have determined that on or around March 19, 2025, certain customer information stored on the impacted servers was accessed and later taken by an unauthorized third party. Your personal information was stored on the impacted servers.

The types of impacted personal information varied by individual customer and depended, in part, on the information provided by each customer. This may have included one or more of the following: name, phone number, email address, mailing and service addresses, Nova Scotia Power program participation information, date of birth, and customer account history (such as power consumption, service requests, customer payment, billing, and credit history, and customer correspondence) and driver's license number. For some of our customers, bank account numbers (for pre-authorized payment) may also have been impacted, if this information was provided by these customers.

While we have no evidence of misuse of your personal information, as a precautionary measure, arrangements have been made with the consumer reporting agency, TransUnion, to provide you with a two-year subscription to a comprehensive credit monitoring service (TransUnion *myTrueIdentity*) at no cost to you. Please refer to the attachments included with this notice for additional information about TransUnion *myTrueIdentity*, including details about how to **activate your subscription**. We have also attached an "Additional Guidance" page with steps you can take to further protect your personal information.

00766-ADFSON-187441-L001 AUTO_000001-000001-000-1/2



We encourage you to remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts or phone calls), including messages that appear to be from Nova Scotia Power, asking you to provide your personal information. Please avoid clicking on suspicious web links or downloading attachments without confirming they are from a legitimate source. We have established a dedicated number 1-844-818-0376 for customers who have questions about this incident.

We sincerely apologize that this issue has occurred. Protecting the privacy and security of information held by Nova Scotia Power is something we take very seriously. We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future.

Sincerely,

Peter Gregg

President & CEO

Nova Scotia Power

Services Description

We have retained the assistance of Trans Union of Canada, Inc. ("TransUnion Canada"), one of Canada's leading consumer reporting agencies and arranged a **24-month** subscription to *myTrueIdentity*®, an online credit monitoring and identity restoration service, at no cost to you.

We encourage you to take advantage of this service by enrolling online. To activate your service, please visit:

<https://www.mytrueidentity.ca>

You will be prompted to enter the following activation code: [REDACTED]

Please ensure that you redeem your activation code before 9/30/2025 to take advantage of the service.

Upon completion of the online activation process, you will have access to the following features:

- ✓ Unlimited online access to your TransUnion Canada credit report, updated daily. A credit report is a snapshot of your financial history and one of the primary tools leveraged for determining credit-related identity theft or fraud.
- ✓ Unlimited online access to your CreditVision® Risk credit score, updated daily. A credit score is a three-digit number calculated based on the information contained in your TransUnion Canada credit report at a particular point in time.
- ✓ Credit monitoring, which provides you with email notifications to key changes on your TransUnion Canada credit report. In today's virtual world, credit alerts are a powerful tool to help protect you against identity theft, enable quick action against potentially fraudulent activity and provide you with additional reassurance.
- ✓ Access to online educational resources concerning credit management, fraud victim assistance and identity theft prevention.
- ✓ Access to Identity Restoration agents who are available to assist you with questions about identity theft. In the unlikely event that you become a victim of fraud; a personal restoration specialist will help to resolve any identity theft. This service includes up to \$1,000,000 of expense reimbursement insurance¹.
- ✓ Dark Web Monitoring, which monitors surface, social, deep, and dark websites for potentially exposed personal, identity and financial information and helps protect you against identity theft.

Should you require technical support with *myTrueIdentity*®, please contact TransUnion Canada at 1-877-884-3441.

¹Expense reimbursement insurance is only available upon successful enrollment in the online credit monitoring service.



Additional Guidance

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent institution or any suspected incidence of identity theft to law enforcement authorities.

Obtain a Copy of Your Credit Report

Order a copy of your credit report from both TransUnion Canada and Equifax Canada. Each credit bureau may have different information about how you have used credit in the past. Ordering your own credit report has no effect on your credit score. TransUnion Canada refers to your credit report as “consumer disclosure”. Equifax Canada refers to your credit report as “credit file disclosure”. You can make the request by contacting the two credit bureaus as indicated below. You will need to follow the instructions provided and also confirm your identity by providing identification or answering a series of questions.

	TransUnion	Equifax
By mail or fax	Consumer Relations Centre 3115 Harvester Road, Suite 201 Burlington, Ontario L7N 3N8	National Consumer Relations P.O. Box 190, Station Jean Talon Montreal, Quebec H1S 2Z2 or by fax to: 514-355-8502
By telephone	Tel: 1-800-663-9980	1-800-465-7166
Online	https://ocs.transunion.ca	https://www.consumer.equifax.ca/personal/

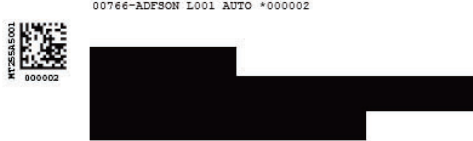
Place a Fraud Alert on Your Credit Report

You can also place a fraud alert on your credit report. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact TransUnion Canada and Equifax Canada using the information above.



PO Box 910 Halifax,
Nova Scotia B3J 2W5

May 10, 2025



Re: Important Notice About Your Personal Information

Dear Valued Customer:

We are writing to provide you with information about the recent cyber incident impacting Nova Scotia Power.

On April 25, 2025, Nova Scotia Power discovered that an unauthorized third party had gained access to certain parts of its Canadian network and servers.

Immediately following detection of the external threat, we activated our incident response and business continuity protocols, engaged external cybersecurity experts, commenced a thorough investigation, and took actions to contain and address the unauthorized activity. We have also notified law enforcement and regulatory authorities about this cyber incident.

While the investigation remains ongoing, we have determined that on or around March 19, 2025, certain customer information stored on the impacted servers was accessed and later taken by an unauthorized third party. Your personal information was stored on the impacted servers.

The types of impacted personal information varied by individual customer and depended, in part, on the information provided by each customer. This may have included one or more of the following: name, phone number, email address, mailing and service addresses, Nova Scotia Power program participation information, date of birth, and customer account history (such as power consumption, service requests, customer payment, billing, and credit history, and customer correspondence), driver's license number, and Social Insurance Number. For some of our customers, bank account numbers (for pre-authorized payment) may also have been impacted, if this information was provided by these customers.

While we have no evidence of misuse of your personal information, as a precautionary measure, arrangements have been made with the consumer reporting agency, TransUnion, to provide you with a two-year subscription to a comprehensive credit monitoring service (TransUnion *myTrueIdentity*) at no cost to you. Please refer to the attachments included with this notice for additional information about TransUnion *myTrueIdentity*, including details about how to **activate your subscription**. We have also attached an "Additional Guidance" page with steps you can take to further protect your personal information.

00766-ADFSON-L001 AUTO_000002-000005-000-1/2



We encourage you to remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts or phone calls), including messages that appear to be from Nova Scotia Power, asking you to provide your personal information. Please avoid clicking on suspicious web links or downloading attachments without confirming they are from a legitimate source. We have established a dedicated number 1-844-818-0376 for customers who have questions about this incident.

We sincerely apologize that this issue has occurred. Protecting the privacy and security of information held by Nova Scotia Power is something we take very seriously. We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future.

Sincerely,

Peter Gregg

President & CEO

Nova Scotia Power

Services Description

We have retained the assistance of Trans Union of Canada, Inc. ("TransUnion Canada"), one of Canada's leading consumer reporting agencies and arranged a **24-month** subscription to *myTrueIdentity*®, an online credit monitoring and identity restoration service, at no cost to you.

We encourage you to take advantage of this service by enrolling online. To activate your service, please visit:

<https://www.mytrueidentity.ca>

You will be prompted to enter the following activation code: [REDACTED]

Please ensure that you redeem your activation code before 9/30/2025 to take advantage of the service.

Upon completion of the online activation process, you will have access to the following features:

- ✓ Unlimited online access to your TransUnion Canada credit report, updated daily. A credit report is a snapshot of your financial history and one of the primary tools leveraged for determining credit-related identity theft or fraud.
- ✓ Unlimited online access to your CreditVision® Risk credit score, updated daily. A credit score is a three-digit number calculated based on the information contained in your TransUnion Canada credit report at a particular point in time.
- ✓ Credit monitoring, which provides you with email notifications to key changes on your TransUnion Canada credit report. In today's virtual world, credit alerts are a powerful tool to help protect you against identity theft, enable quick action against potentially fraudulent activity and provide you with additional reassurance.
- ✓ Access to online educational resources concerning credit management, fraud victim assistance and identity theft prevention.
- ✓ Access to Identity Restoration agents who are available to assist you with questions about identity theft. In the unlikely event that you become a victim of fraud; a personal restoration specialist will help to resolve any identity theft. This service includes up to \$1,000,000 of expense reimbursement insurance¹.
- ✓ Dark Web Monitoring, which monitors surface, social, deep, and dark websites for potentially exposed personal, identity and financial information and helps protect you against identity theft.

Should you require technical support with *myTrueIdentity*®, please contact TransUnion Canada at 1-877-884-3441.

¹Expense reimbursement insurance is only available upon successful enrollment in the online credit monitoring service.



Additional Guidance

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent institution or any suspected incidence of identity theft to law enforcement authorities.

Obtain a Copy of Your Credit Report

Order a copy of your credit report from both TransUnion Canada and Equifax Canada. Each credit bureau may have different information about how you have used credit in the past. Ordering your own credit report has no effect on your credit score. TransUnion Canada refers to your credit report as “consumer disclosure”. Equifax Canada refers to your credit report as “credit file disclosure”. You can make the request by contacting the two credit bureaus as indicated below. You will need to follow the instructions provided and also confirm your identity by providing identification or answering a series of questions.

	TransUnion	Equifax
By mail or fax	Consumer Relations Centre 3115 Harvester Road, Suite 201 Burlington, Ontario L7N 3N8	National Consumer Relations P.O. Box 190, Station Jean Talon Montreal, Quebec H1S 2Z2 or by fax to: 514-355-8502
By telephone	Tel: 1-800-663-9980	1-800-465-7166
Online	https://ocs.transunion.ca	https://www.consumer.equifax.ca/personal/

Place a Fraud Alert on Your Credit Report

You can also place a fraud alert on your credit report. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact TransUnion Canada and Equifax Canada using the information above.

Did you receive a letter from Nova Scotia Power about the cyber incident and your personal data? Wondering what to do next?

Here are some next steps and tips to help secure your personal information.

Signing up for TransUnion's Credit Monitoring, myTruIdentity®

Notifications have been mailed to customers that have been impacted by the cyber incident, which include detailed information about resources and support. We encourage you to sign up for the free subscription to TransUnion's comprehensive credit monitoring service, myTruIdentity®.



What you need to know



Have your letter handy when you start the sign-up process online via the TransUnion myTruIdentity® website—you'll need to enter the **unique activation code** provided in the letter to get started.



Be ready to answer security questions about yourself. To confirm your identity, myTruIdentity® will ask security questions to ensure your protection. These are based on your own financial history and could include questions about the bank you use, a previous address, or where you have a credit card. These **questions** offer multiple options to choose from, and you pick the correct one.

Examples of security questions:

- Where did you last receive credit?
- What was your last address?
- What financial institution do you bank with?



Important: Please complete the myTruIdentity® enrolment process in one session. For security reasons, the enrolment process cannot be paused or resumed after periods of inactivity. If you aren't able to complete the enrolment process in one session, you will have to call TransUnion to complete the process.

Dark Web Monitoring: Once you've signed up, go to "Alerts" in the navigation, click "Dark Web Monitoring", and fill out the fields you would like monitored for activity on the **dark web**. This is an optional process, but one that is helpful to better track your information.

What is the dark web?

These threat actors, and other cyber criminals, use a hidden part of the internet that is only accessible through special software—it is commonly referred to as the "dark web" and is known to be used by cyber criminals as a place to store and trade data.



Should you require technical support with myTruIdentity®, please contact TransUnion Canada directly via the 1-877 phone number provided in your letter.



Further Protection

Here's are some additional steps you can take to further protect your personal information:

1

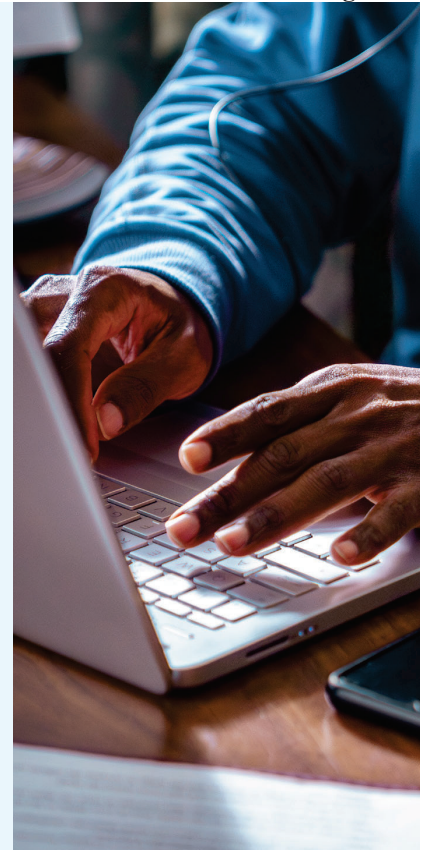
Service Canada advises individuals affected by a breach to contact both TransUnion and Equifax for file monitoring and to regularly review banking and credit card statements. If you notice any suspicious activity related to your Social Insurance Number, report it to the police and contact the **Canadian Anti-Fraud Centre at 1-888-495-8501**.

2

Sign up for **Equifax's fraud alerts** and security freezes through their free "myEquifax" account. Visit my.equifax.ca to sign-up or call **1-800-465-7166**.

3

Contact your financial institution to discuss account monitoring and any additional protection support they may be able to offer.



We're Here to Help

We know this has been a scary and frustrating time for our customers, and we are sincerely sorry that this has happened. To better assist you, we will be visiting communities in Nova Scotia to offer in-person support.

Our team can help answer questions or provide guidance on the credit monitoring registration process (you must bring your letter with the code along), answer questions about estimated bills, or anything else you need extra support with. **If you're unable to join us, you can always call our Customer Care Centre.**



**Nova Scotia Power
Customer Care Centre**
1-800-428-6230



**Find a location
nearest you**
nspower.ca/cyberhelp

Stay alert. During cyber incidents like the one we're currently experiencing; malicious actors may attempt to take advantage of the situation. Be cautious of suspicious emails, texts, or calls claiming to be from Nova Scotia Power, and don't click on unknown links or share personal information unless you're sure it's legitimate.



For more information,
please visit nspower.ca/cyber



NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

CYBER INCIDENT UPDATES

NEWS

July 8, 2025

Since the cyber incident discovered on April 25, power meters have continued to function and gather accurate energy usage data from homes and businesses across the province. However, due to the cyber incident, the meters have not been able to communicate that data to our systems. As a result, we initially paused customer billing and have recently resumed billing with most customers receiving estimated bills until our systems are restored and meters begin communicating again.

Starting this month, you will begin to see meter readers in your community. To provide you with a bill based on your actual energy usage, meter readers began gathering energy use data from meters earlier this month. In most cases, meter readers will need to access the meter on your property—this will only take a few minutes, and you do not need to be home for your meter to be read.

Meter readers will be wearing Nova Scotia Power branded clothing and will carry identification badges with the word "Contractor" at the bottom. If meter readers are unable to access your meter due to vegetation, pets, fencing, etc., you will receive an estimated bill based on an average of the previous energy used at your property during a similar time of year.

Learn more about our adjusted billing process [here >](#)

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Wednesday, June 25, 2025 Update

A dedicated team within Nova Scotia Power, along with third-party cybersecurity experts, are continuing the investigation into the recent ransomware attack that has impacted our customers and our company. Today, we are providing an update on the recent cyber incident and impacts to the personal data of former customers. We are also announcing an expansion of credit monitoring.

Beginning today, we will be offering five years of free credit monitoring to all customers of Nova Scotia Power—past and present—regardless of whether you received a letter from us about the incident. Customers will not pay for any costs incurred by Nova Scotia Power for credit monitoring resulting from this incident.

We have determined through our investigation that the personal information of former customers was also accessed on or around March 19, 2025, and later taken by an unauthorized third-party, in addition to the personal information of the current customers to whom notifications have already been sent.

We are working to determine the full scope of data that may be impacted but we cannot rule out the possibility that some or all of the following personal information has been impacted: name, phone number, email address, mailing and service addresses, Nova Scotia Power program participation information, date of birth, and customer account history (such as power consumption, service requests, customer payment, billing and credit history, and customer correspondence), and driver's license number. For some of our former customers, bank account numbers (for pre-authorized payment) and Social Insurance Numbers may also have been impacted.

We intend to do everything we can to support current and former customers, which includes expanded access to credit monitoring.

Those who want to sign up for the credit monitoring service can click [here](#) to validate and secure a unique code for the service. Anyone who has already signed up for credit monitoring will automatically be extended to five years.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

We are focused on supporting our customers. We are here for regular business from 8 AM–6 PM, Monday through Friday. Please contact us at [1-800-428-6230](tel:1-800-428-6230).

To make it easier to help all customers through the sign-up process, tips on registering for credit monitoring can be found [here](#) and will be included in upcoming bills, as well as available in locations throughout the province. This includes information on additional steps customers can take to protect themselves from identity theft. We are also deploying employee volunteers to communities across the province to provide hands-on support for customers who prefer assistance in person.

We encourage customers to remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts, or phone calls), including messages that appear to be from Nova Scotia Power asking you to provide your personal information. Please avoid clicking on suspicious links or downloading attachments without confirming they are from a legitimate source.

We have heard concerns about SINs, which we historically collected for customer authentication purposes. We are committed to permanently deleting all instances of SINs from our systems as soon as our investigation allows.

Nova Scotia Power is continuing to take steps to fully understand what happened in this matter and to prevent a recurrence of this issue. Additionally, we are fully cooperating with the Office of the Privacy Commissioner of Canada and the Nova Scotia Energy Board, which have both announced investigations into this incident.

We recognize that this incident may have shaken the confidence of some of our customers. We are working hard to do everything we can to regain your confidence.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Wednesday, June 4, 2025 Update

Following the recent ransomware attack and its effect on our customers, we've been invited to speak with members of the Nova Scotia Public Accounts Committee at their meeting today.

While recognizing that the investigation and response efforts remain ongoing, we have committed to be as open and transparent as possible. This meeting today is a part of that transparency.

Opening remarks by Peter Gregg, President & CEO

On behalf of our entire team at Nova Scotia Power, thank you for the invitation to attend today's committee meeting. Cybersecurity is a critical issue facing private, public, and government organizations right now and we all need to work together to protect the security of Nova Scotians. I am here today with two colleagues, Chris Lanteigne, Nova Scotia Power's Director of Customer Care, and Chris Heck, the Chief Digital Officer from our parent company, Emera. We appreciate the opportunity to discuss this issue with you today and how we can get stronger together as we move forward.

I would like to begin with reiterating our sincere apologies to all our customers that they have been impacted by this cyber incident. We understand it is very concerning and we're working hard to address customer issues and to continue to strengthen our systems as we work to restore and rebuild.

As we begin, it's important to remind people of the sensitivity of the incident and the fact that it is ongoing. This was a sophisticated attack on Nova Scotia Power and our customers by a criminal who has stolen data from our systems. We are committed to being as open and transparent as possible, as we have been since the beginning of the incident—our investigation and response efforts remain ongoing.

Maintaining the integrity of the active investigation, under the careful guidance of leading cybersecurity experts, is essential. We have also notified and sought input from law enforcement.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

The privacy commissioner of Canada stated last week that: “Data breaches have surged over the past decade, and this incident highlights the growing risks of cyberattacks for all organizations.”

Despite this reality, we know that to our customers, Nova Scotia Power is not just any organization. We are a vital part of their every day lives and we take that responsibility very seriously. And we take cybersecurity very seriously and work every day to manage threats and continually evolving risks.

I want to assure the committee that before this attack we invested heavily in keeping our network and information secure. We implement measures and controls designed to align with the National Institute of Standards and Technology and the North American Electric Reliability Corporation (NERC), organizations that set standards for electric utilities across North America. However, as we know, the cyber criminals are getting more and more sophisticated and we continue to focus our efforts and make investments to address these growing threats.

No payment has been made to the criminal. This reflects our careful assessment of applicable sanctions laws and alignment with law enforcement guidance. It was illegal to make a payment.

Immediately after detecting unusual activity on our network on April 25, we activated our existing cyber incident response and business continuity protocols. These included engaging leading third-party cybersecurity experts and taking swift actions to contain and isolate the affected systems to prevent further intrusion. Our cybersecurity program ensured that our operations systems and electric grid continue to perform as usual.

As you know, the criminals stole data, which unfortunately includes the personal data of customers. We’ve sent notifications to those impacted existing account holders and encouraged them to sign up for free credit monitoring service and are continuing to investigate the full scope of the impact of the data. And this investigation is complex, extremely detailed, and will take time.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

I am also encouraging all impacted customers to sign up for complimentary credit monitoring and identity protection services. We have updated our [website](#) to include tips on some of the common issues customers have had in signing up.

Additionally, for anyone experiencing challenges, we will start providing in-person support in various communities across the province starting later this week to assist our customers. Signing up online remains the best path for customers, but we plan to provide some in-person support for those who are less comfortable with the online process or have questions. More details will be communicated in the coming days.

I want to assure you that we are cooperating at all levels on the investigation of this criminal attack. As you are aware, formal investigations of the incident have been initiated by both the Nova Scotia Energy Board and the Office of the Privacy Commissioner of Canada. Nova Scotia Power will fully cooperate with both of these proceedings.

You have my commitment that our team is focused on the continued investigation of our restoration efforts. We will continue to be open and transparent as we move through this process. We know that our customers feel we have let them down and we are doing everything we can to support them. We thank all our customers for their patience as we continue to work through this very difficult and active situation.

Thank you. We look forward to the discussion.

Peter Gregg, President & CEO, Nova Scotia Power

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Friday, May 23, 2025 Update

We wanted to provide an update on Nova Scotia Power's ongoing cyber incident. Today, we are confirming we have been the victim of a sophisticated ransomware attack.

Since the incident began several weeks ago, Nova Scotia Power has been actively working with the assistance of third-party cyber security experts to restore our systems safely and investigate the incident. We have also been working to further strengthen our systems and add additional security protections.

No payment has been made to the threat actor. This decision reflects our careful assessment of applicable sanctions laws and alignment with law enforcement guidance.

We have learned that the threat actor has published data that was stolen from our systems. We are actively working with cybersecurity experts to assess the nature and scope of the information that may have been impacted.

Notifications have been mailed to impacted account holders, which include detailed information about resources and support. Arrangements have been made with the consumer reporting agency, TransUnion, to provide impacted individuals with a two-year subscription to a comprehensive credit monitoring service (TransUnion *myTrueIdentity*®) at no cost.

We encourage customers who receive a notification to enroll in the TransUnion credit monitoring service and otherwise remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts, or phone calls), including messages that appear to be from Nova Scotia Power asking you to provide your personal information. Please avoid clicking on suspicious links or downloading attachments without confirming they are from a legitimate source.

We remain sincerely sorry that this issue has occurred. Protecting the privacy and security of information held by Nova Scotia Power is something we take very seriously.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Wednesday, May 14, 2025 Update

Nova Scotia Power continues to investigate a cyber incident that has impacted certain IT systems in our network. We are working with external cybersecurity experts to determine the scope of the impact and safely and securely restore and rebuild our impacted systems.

While the investigation remains ongoing, we have determined that on or around March 19, 2025, certain customer information stored on the impacted servers was accessed and later taken by an unauthorized third party.

Notifications are in the process of being mailed to impacted account holders, which includes detailed information about resources and support. While we have no evidence of misuse of your personal information, as a precaution, arrangements have been made with the consumer reporting agency, TransUnion, to provide impacted individuals with a two-year subscription to a comprehensive credit monitoring service (TransUnion *myTrueIdentity*®) at no cost.

The types of impacted personal information varied by individual customer and depended, in part, on the information provided by each customer. This may have included one or more of the following: name, phone number, email address, mailing and service addresses, Nova Scotia Power program participation information, date of birth, and customer account history (such as power consumption, service requests, customer payment, billing, and credit history, and customer correspondence), driver's license number, and Social Insurance Number. For some of our customers, bank account numbers (for pre-authorized payment) may also have been impacted, if this information was provided by these customers.

We encourage customers to remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts, or phone calls), including messages that appear to be from Nova Scotia Power asking you to provide your personal information. Please avoid clicking on suspicious links or downloading attachments without confirming they are from a legitimate source.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Any customer who receives a letter in the mail from Nova Scotia Power will be provided with a phone number to call with any questions and to activate their two year subscription for credit monitoring.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Thursday, May 1, 2025 Update

Nova Scotia Power is providing important information about the recent cyber incident affecting our company.

On April 25, we detected unusual activity on our network and immediately initiated our incident response plan. This included taking steps to contain the incident, launching a thorough investigation with the help of external cybersecurity experts, and working to restore affected systems safely and securely. We have also notified law enforcement.

While our investigation is ongoing, we have identified that certain customer personal information was accessed and taken by an unauthorized third party.

Rest assured, we are treating this situation very seriously. The security of your information is our top priority. We are working urgently to determine the full nature and scope of the data that may have been affected, and individuals impacted.

If we determine that your data was affected, we will send you notice with further details including about the affected information, along with resources and support.

We encourage you to remain vigilant and cautious about any unsolicited communications (such as emails, text, social posts, or phone calls) that appear to be from Nova Scotia Power asking you to provide your personal information. Please avoid clicking on suspicious links or downloading attachments without confirming they are from a legitimate source.

We are committed to providing further updates as our investigation progresses. Our team asks for your patience as we work to understand the specific details of this unfortunate cyber incident.

There remains no disruption to Nova Scotia Power's generation, transmission, and distribution facilities, and the incident has not impacted on our ability to safely and reliably serve customers in Nova Scotia.

We appreciate your patience and trust as we work to address this situation.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Monday, April 28, 2025 Update

Emera Inc. and Nova Scotia Power today announced on April 25, 2025 they discovered and are actively responding to a cybersecurity incident involving unauthorized access into certain parts of its Canadian network and servers supporting portions of its business applications.

Immediately following detection of the external threat, the companies activated their incident response and business continuity protocols, engaged leading third-party cybersecurity experts, and took actions to contain and isolate the affected servers and prevent further intrusion. Law enforcement officials have been notified.

There remains no disruption to any of our Canadian physical operations, including at Nova Scotia Power's generation, transmission and distribution facilities, the Maritime Link or the Brunswick Pipeline, and the incident has not impacted the utility's ability to safely and reliably serve customers in Nova Scotia. There has been no impact to Emera's U.S. or Caribbean utilities.

Emera will release its Q1 Financial Statements and Management Disclosure and Analysis on May 8, 2025, as planned. At this time, the incident is not expected to have a material impact on the financial performance of the business.

Our IT team is working diligently with cyber security experts to bring the affected portions of our IT system back online.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

LATEST UPDATES

July 8, 2025

- Power meters have continued to function and gather accurate energy usage data from homes and businesses across the province. However, due to the cyber incident, the meters have not been able to communicate that data to our systems.
- As a result, we initially paused [customer billing](#) and have recently resumed billing with most customers receiving estimated bills until our systems are restored and meters begin communicating again.
- Starting this month, you will begin to see meter readers in your community. To provide you with a bill based on your actual energy usage, meter readers began gathering energy use data from meters earlier this month. In most cases, meter readers will need to access the meter on your property.
- Meter readers will be wearing Nova Scotia Power branded clothing and will carry identification badges with the word "Contractor" at the bottom. If meter readers are unable to access your meter due to vegetation, pets, fencing, etc., you will receive an estimated bill based on an average of the previous energy used at your property during a similar time of year.

Wednesday, June 25, 2025

- Beginning today, we will be offering five years of free credit monitoring to all customers of Nova Scotia Power, past and present, regardless of whether you received a letter from us about the incident. Anyone who has already signed up for credit monitoring will automatically be extended to five years.
- We have determined through our investigation that the personal information of former customers was also accessed on or around March 19, 2025, and later taken by an unauthorized third-party, in addition to the personal information of the current customers to whom notifications have already been sent.
- We are working hard to do everything we can to support current and former customers, which includes expanded access to credit monitoring for all Nova Scotia Power customers—past and present.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

- Those who want to sign up for the credit monitoring service can use our [Customer Verification Form](#) to validate and secure a unique code for the service.
- Customers will not pay for any costs incurred by Nova Scotia Power for credit monitoring resulting from this incident.
- We are focused on supporting our customers. We are here for regular business from 8 AM–6 PM, Monday through Friday. Please contact us at [1-800-428-6230](tel:1-800-428-6230).

Wednesday, June 5, 2025

- Nova Scotia Power leadership appeared before the Nova Scotia Public Accounts Committee as part of our ongoing commitment to transparency following the recent ransomware attack.
- Immediately after detecting the cyberattack on April 25, we activated our response protocols, engaged cybersecurity experts, and have continued to work closely with law enforcement and regulators. The attack was sophisticated and resulted in stolen customer data; no ransom payment was made.
- We've notified impacted customers, offered free credit monitoring and identity protection, and will begin providing in-person support in communities across the province to assist those facing challenges with the process.
- We continue to invest in cybersecurity and are cooperating fully with ongoing investigations. We deeply regret the impact on our customers and remain focused on rebuilding trust and strengthening our systems.

Friday, May 23, 2025

- Nova Scotia Power confirms we been the victim of a sophisticated ransomware attack.
- No payment has been made to the threat actor. This decision reflects our careful assessment of applicable sanctions laws and alignment with law enforcement guidance.
- We have learned that the threat actor has published data that was stolen from our systems. We are actively working with cybersecurity experts to assess the nature and scope of the information that may have been impacted.
- Since the incident began several weeks ago, we have been actively working with the assistance of third-party cyber security experts to restore our systems safely

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

and investigate the incident. We have also been working to further strengthen our systems and add additional security protections.

- Notifications have been mailed to impacted account holders, which include detailed information about resources and support. Arrangements have been made with the consumer reporting agency, TransUnion, to provide impacted individuals with a two-year subscription to a comprehensive credit monitoring service (TransUnion *myTrueIdentity*®) at no cost.
- We remain sincerely sorry that this issue has occurred. Protecting the privacy and security of information held by Nova Scotia Power is something we take very seriously.

Wednesday, May 14, 2025

- Nova Scotia Power continues to investigate a cyber incident that has impacted certain IT systems in our network.
- While the investigation remains ongoing, we have determined that on or around March 19, 2025, certain customer information stored on the impacted servers was accessed and later taken by an unauthorized third party.
- Notifications are in the process of being mailed to impacted account holders, which includes detailed information about resources and support.
- While we have no evidence of misuse of your personal information, as a precaution, arrangements have been made with the consumer reporting agency, TransUnion, to provide impacted individuals with a two-year subscription to a comprehensive credit monitoring service (TransUnion *myTrueIdentity*®) at no cost.
- The types of impacted personal information varied by individual customer and depended, in part, on the information provided by each customer.
- Any customer who receives a letter in the mail from Nova Scotia Power will be provided with a phone number to call with any questions and to activate their two year subscription for credit monitoring.

Thursday, May 1, 2025

- We are actively responding to a cyber incident that has impacted certain IT systems in our network.
- While our investigation is ongoing, we have identified that certain customer personal information was accessed and taken by an unauthorized third party.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

- If we determine that your data was affected, we will send you notice with further details including about the affected information, along with resources and support.
- We encourage you to remain vigilant and cautious about any unsolicited communications (such as emails, text, social posts, or phone calls) that appear to be from Nova Scotia Power asking you to provide your personal information. Please avoid clicking on suspicious links or downloading attachments without confirming they are from a legitimate source.

Monday, April 28, 2025

- Emera and Nova Scotia Power discovered and are actively responding to a cybersecurity incident involving unauthorized access into certain parts of our network and servers supporting portions of our business applications.
- Immediately following detection of the external threat, we activated incident response and business continuity protocols, engaged leading third-party cybersecurity experts, and took actions to contain and isolate the affected servers and prevent further intrusion.
- There remains no disruption to any physical operations, including our generation, transmission, and distribution facilities, the Maritime Link or the Brunswick Pipeline, and the incident has not impacted our ability to safely and reliably serve our customers.
- Our customers can continue to report outages or emergencies through our outage line at [1-877-428-6004](tel:1-877-428-6004).
- This incident does not affect our ability to safely and reliably deliver electricity to all of our customers.
- Please be vigilant and report any suspicious emails or phone calls.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

FAQS

What happened?

Last updated: Tuesday, June 24, 2025

On April 25, we discovered and began actively responding to a cybersecurity incident involving unauthorized access into certain parts of our network and servers. Upon further investigation with external cybersecurity experts, we identified that certain customer personal information was accessed and taken by an unauthorized third-party.

This was a result of a sophisticated ransomware attack. In compliance with sanctions laws and law enforcement guidance, no ransom was paid; it was illegal to pay a ransom.

Our investigation remains ongoing, and we are committed to providing accurate and timely information to our customers and partners. Our website remains the best source of information and updates relating to the cybersecurity incident.

What is Nova Scotia Power doing to address this cyber incident?

Last updated: Tuesday, June 24, 2025

While our investigation remains ongoing, we have taken the following steps:

- Engaged third-party cybersecurity experts to help us investigate, remediate, and recover the affected systems. We have also notified law enforcement and regulators.
- Conducted a detailed review of what data has been accessed and taken. This remains an ongoing, complex effort. We have confirmed that certain customer personal information was taken.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

- Informed impacted customers via mail and provided a free subscription to TransUnion’s credit monitoring service, *myTrueIdentity*®.
- Organized in-person support for customers in communities across the province.
- Resumed billing through an [estimated billing](#) approach; customers can now access their bills through [MyAccount](#).

Was customer information or confidential business information accessed?

Last updated: Tuesday, June 24, 2025

While our investigation is ongoing, we have identified that certain customer personal information was accessed and taken by the threat actor. Some of this information was also published to the dark web.

Impacted customers have received a letter from us in the mail with resources and support.

Was my data impacted?

Last updated: Wednesday, June 25, 2025

Anyone who received a letter from us did receive information about what personal data may have been impacted in that letter.

Our investigation remains ongoing. The ransomware attack was sophisticated, with the cybercriminal encrypting and locking numerous files and systems. The process of restoring access is complex and will require time.

At this time we are unable to confirm specifics regarding the precise impact on individual customers’ data. That is why, out of an abundance of caution and to ensure a level of protection and reassurance for our customers, we are expanding our offer of free credit monitoring. It will be available to all customers of Nova Scotia Power—past and present—regardless of whether you received a letter from us about the incident.

I’m a current customer, but I did not get a letter. Does that mean I was not affected?

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Last updated: Wednesday, June 25, 2025

Our investigation is ongoing, and we sent letters to customers we determined to have been impacted in the incident. Out of an abundance of caution and to ensure a level of protection and reassurance for our customers, we are expanding our offer of five years of free credit monitoring. We are expanding our offer of five years of free credit monitoring to all current and past customers regardless of whether you received a letter or not.

I didn't get a letter and I am a Nova Scotia Power customer or former customer. How do I get an activation code to sign up for credit monitoring?

Last updated: Wednesday, June 25, 2025

To receive your unique activation code that will enable you to sign up for credit monitoring, please use our [Customer Verification Form](#). You will be asked to share the first name, last name, and birth year of the primary account holder to receive your code (your information will not be stored).

I've already signed up for the two years of credit monitoring. Do I need to sign up again to get five?

Last updated: Wednesday, June 25, 2025

No. Anyone who has already signed up for credit monitoring will automatically be extended to five years of credit monitoring. If you received a letter from us with a code and already signed up for two years of monitoring, you will be automatically extended to five years.

Why didn't you offer credit monitoring to everyone right away when this happened? Why now?

Last updated: Wednesday, June 25, 2025

Our initial focus was on customers that were confirmed to have their personal data impacted by the breach. As our investigation evolved, we learned that the personal data of former customers was similarly impacted. Out of an abundance of caution and to ensure a level of protection and reassurance for our customers, we are expanding our offer of free credit monitoring. It will be available to all customers of Nova Scotia

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

Power—past and present—regardless of whether you received a letter from us about the incident.

I haven't been a customer for 10 years? Do you still have my data?

Last updated: Wednesday, June 25, 2025

This is a really important question to be answered as part of the investigation into the incident.

What are you doing to reach former customers who no longer live in the province to provide the credit monitoring?

Last updated: Wednesday, June 25, 2025

Former customers for whom we have contact information will be sent a written notification. In cases where we don't have contact information, we are working to share notification as broadly as possible. We are actively sharing this information with media, on social media, with stakeholders, and through paid advertising to reach as many current and former customers as possible.

We strongly encourage anyone who is concerned about their protection to sign up for the free five-year credit monitoring service. We also encourage our current customers to share this information with friends, family, and neighbours who are former Nova Scotia Power customers.

What services have been affected?

Last updated: Tuesday, June 24, 2025

Initially, there was disruption to our internal IT and customer care systems, which affected our billing processes and access to our online customer portal, MyAccount. We have been working around the clock to restore all systems for our customers and are now able to provide estimated bills to customers and restore their access to MyAccount.

MyEnergy Insights and Efficiency Insights are not currently available through MyAccount.

NS Power – Cyber Incident Updates (Website Excerpts – September 5, 2025)

NON-CONFIDENTIAL

Request IR-3:

NS Power, in its Thursday, May 14, 2025, cybersecurity update letter stated:

Beginning today, we will be offering five years of free credit monitoring to all customers of Nova Scotia Power—past and present—regardless of whether you received a letter from us about the incident. Customers will not pay for any costs incurred by Nova Scotia Power for credit monitoring resulting from this incident

[Cyber] Nova Scotia Power: Wednesday, May 14, 2025 Update]

- (a) How did the utility determine that there was no evidence of misuse of personal information for all the customers?**
- (b) When did the utility start sending out the notice letters?**
- (c) How can the utility ensure that all impacted customers or former customers have received the notice letters or any form of communication?**
- (d) If applicable, please explain the delay between identifying the data breach and sending out the notices.**
- (e) Did different customers receive different notice letters?**
- (i) If yes, how many different letters were sent out, and provide samples of each different version sent out to customers.**
- (ii) How did the utility determine which letter customers would receive?**
- (f) Why did the utility select TransUnion myTrueIdentity® services?**

(b) NS Power began mailing letters to impacted customers on May 13, 2025.

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

NON-CONFIDENTIAL

1 (c) Please refer to IR-1 for additional details about NS Power's extensive efforts to ensure that
2 impacted customers have received prompt notice about the incident.

3
4 (d) The Company adopted a best-practices approach to its response to the Incident grounded
5 in transparency and timely communication to impacted customers.

6
7 The process to identify what data was impacted has been extremely complex, but from the
8 outset, NS Power worked urgently to determine the full nature and scope of the data and
9 individuals that may have been affected.

10
11 Once NS Power identified that certain personal information was accessed and taken, the
12 Company notified the public on May 1, 2025, and immediately began coordinating direct
13 notifications to individuals it determined at that time were impacted. The notification effort
14 is a highly time-intensive process, and included the necessary preparation working with
15 credit monitoring service TransUnion to ensure it could be fully staffed and call centre
16 representatives trained and ready to manage the significant volume of incoming calls,
17 questions and requests. The Company began mailing notices to affected individuals on
18 May 13, 2025 (i.e. 12 calendar days after determining the impact to affected individuals).

19
20 As the company continued its investigation of the impacted data, NS Power determined
21 that personal information relating to former customers had also been impacted by the
22 Incident. On [June 25, 2025](#), NS Power notified the public that information of former
23 customers had also been impacted in the Incident.

24
25 (e) As set out above, the Company's approach to transparent communications about the impact
26 of the Incident on NS Power customers principally consisted of direct notifications to active
27 impacted customers, and public postings to the Company website, supported by media
28 outreach and social media engagement.

29
30 With respect to direct notifications, the Company sent two versions of letters to impacted
31 current customers, samples of which are attached as Attachments 1 and 2 to IR-1. The

NON-CONFIDENTIAL

1 notices are identical, except that one of the notices indicates that based on the investigation,
2 the customer's social insurance number may have been impacted in the incident.

3
4 (f) TransUnion's myTrueIdentity® service offering is a highly regarded credit monitoring and
5 identity protection service, and TransUnion has extensive experience providing customer
6 notification and call centre services to companies which have been the victim of security
7 incidents. The credit monitoring service offered to customers is provided by TransUnion
8 and has been specifically designed to protect individuals in the case of a data breach, and
9 offers them access to the following protective features:

- 10
- 11 • Unlimited online access to their TransUnion Canada credit report, updated daily,
12 which offers individuals access to the individual's financial history and is one of
13 the primary tools leveraged for determining credit-related identity theft or fraud.
14
 - 15 • Unlimited online access to their credit score, updated daily.
16
 - 17 • Credit monitoring, which provides individuals with email notifications to key
18 changes on an individual's TransUnion Canada credit report. These credit alerts
19 help protect individuals against identity theft, enable quick action against
20 potentially fraudulent activity and provide them with additional reassurance.
21
 - 22 • Access to online educational resources concerning credit management, fraud victim
23 assistance and identity theft prevention.
24
 - 25 • Access to Identity Restoration agents who are available to assist individuals with
26 questions about identity theft. In the unlikely event that an individual becomes a
27 victim of fraud, a personal restoration specialist will help to resolve any identity
28 theft.
29
 - 30 • Up to \$1,000,000 of expense reimbursement insurance related to identity theft.
-

NON-CONFIDENTIAL

- 1 • Dark Web Monitoring, which monitors surface, social, deep, and dark websites for
2 potentially exposed personal, identity and financial information and helps protect
3 individuals against identity theft.

4
5 Nova Scotia Power anticipates that a portion of the cost for credit monitoring will be
6 covered by insurance, and has committed that customers will not pay for any costs incurred
7 by Nova Scotia Power related to the free credit monitoring service being provided.

- 8
9 (g) NS Power's initial decision to offer two years of free credit monitoring service aligns with
10 standard industry practice across North America for organizations across industries
11 (financial services, healthcare, retail, telecommunications, education, etc.) when they
12 suffer a ransomware or other data breach involving sensitive personal information. The
13 two-year time frame is widely considered by experts to be sufficient to detect potentially
14 fraudulent activity that may arise following a cyber incident, as it provides a window for
15 potentially affected individuals to monitor their credit information, receive alerts on
16 changes to their credit file, and take steps to protect their information if needed.

- 17
18 (h) On June 25, 2025, NS Power announced that it was extending its offering to five years of
19 complimentary credit monitoring and other services under the TransUnion
20 myTrueIdentity® offering, and made the services available to all past and current
21 customers.

22
23 The Company initially offered impacted active customers a two-year complimentary
24 subscription to TransUnion's myTrueIdentity® service, as a two-year time period for a
25 credit monitoring service has become a well-established, common practice for
26 organizations across industries (financial services, healthcare, retail, telecommunications,
27 education, etc.) when they suffer ransomware or other data breaches involving sensitive
28 personal information.

NON-CONFIDENTIAL

1 NS Power's decision to expand credit monitoring beyond standard practice to five years
2 reflects careful consideration of feedback and concerns expressed by its customers. NS
3 Power listened to customer feedback that additional credit monitoring protection would
4 provide more reassurance and decided to offer five years of coverage to all current and past
5 NS Power customers.

6
7 (i) Customers can protect themselves through a comprehensive set of services provided
8 by myTrueIdentity® that allows them to closely monitor their credit and personal
9 information. The components of the service, which are listed below, provide a strong
10 framework to help safeguard personal and financial information that are aligned with
11 current best practices in identity protection and credit monitoring.

12
13 • Unlimited online access to their TransUnion Canada credit report, updated daily,
14 which offers individuals access to the individual's financial history and is one of the
15 primary tools leveraged for determining credit-related identity theft or fraud.

16
17 • Unlimited online access to their TransUnion CreditVision® Risk credit score,
18 updated daily.

19
20 • Credit monitoring, which provides individuals with email notifications to key
21 changes on an individual's TransUnion Canada credit report. These credit alerts help
22 protect individuals against identity theft, enable quick action against potentially
23 fraudulent activity and provide them with additional reassurance.

24
25 • Access to online educational resources concerning credit management, fraud victim
26 assistance and identity theft prevention.

27
28 • Access to Identity Restoration agents who are available to assist individuals with
29 questions about identity theft. In the unlikely event that an individual becomes a
30 victim of fraud, a personal restoration specialist will help to resolve any identity theft.

Board Inquiry into Nova Scotia Power's Cybersecurity Incident (NSEB M12273)
NSPI Responses to NSEB Information Requests

NON-CONFIDENTIAL

- 1 • Up to \$1,000,000 of expense reimbursement insurance related to identity theft.

- 2
- 3 • Dark Web Monitoring, which monitors surface, social, deep, and dark websites for
- 4 potentially exposed personal, identity and financial information and helps protect
- 5 individuals against identity theft.

6

7 (j) What NS Power implemented a best-practices approach in response to the incident.

8 Specifically, the Company:

- 9
- 10 • Communicated in a transparent and timely manner with impacted individuals,
- 11 consistent with industry expectations and regulatory guidance.

- 12
- 13 • Offered an extended period of complimentary credit monitoring and identity
- 14 protection services that exceeded the widely recognized two-year industry standard.

- 15
- 16 • Provided practical steps and resources that individuals could take independently to
- 17 further protect themselves from potential misuse of their personal information.

18

19 This approach reflects NS Power's commitment to supporting and protecting its customers,

20 even though—like any organization—it cannot predict or categorically rule out possible

21 actions by malicious actors in the future.

Osler, Hoskin & Harcourt LLP
Box 50, 1 First Canadian Place
Toronto, Ontario, Canada M5X 1B8
416.362.2111 MAIN
416.862.6666 FACSIMILE

OSLER

Toronto

August 8, 2025

Montréal

Adam Kardash
Direct Dial: 416.862.4703
akardash@osler.com
Our Matter Number: 1268459

Calgary

***** CONFIDENTIAL *****

Ottawa

Sent by Email

Vancouver

Nova Scotia Energy Board
3rd Floor, 1601 Lower Water Street
Halifax, Nova Scotia B3J 3P6

New York

Attention: Crystal Henwood, Clerk of the Board

Dear Ms. Henwood:

M12273 – Inquiry of the Nova Scotia Energy Board (the Board) into Cybersecurity Incident of Nova Scotia Power (NS Power)

Title: Confidential Submissions in Support of Application for Procedural Order

1. NS Power delivers these Confidential Submissions in support of its application for a procedural order, filed concurrently. As set out in NS Power's application for a procedural order, NS Power requests that these Confidential Submissions be held in confidence by the Board and made available for review only by panel members involved in the Inquiry; the Clerk of the Board; and counsel to the Board.

A. Background Facts

2. NS Power has been the victim of a highly sophisticated ransomware attack. While the attack did not affect NS Power's infrastructure relating to the provision of power to its customers, the incident has caused some disruption to NS Power's internal IT and customer care systems. In the course of the incident, the threat actor also exfiltrated certain data, including customer information. Consistent with the aggressive tactics of ransomware attackers, the threat actors have already posted certain NS Power data on the dark web.

3. In line with recognized best practices, NS Power has worked closely with leading cybersecurity experts to develop and implement a carefully calibrated response to the

attack.



4. There are highly sensitive and confidential details relating to NS Power's incident response that the company intends to share with the Board, including in the Report.

B. Special circumstances requiring procedural order



6. The Board has requested, and NS Power intends to provide to the Board in the Report, highly sensitive information regarding the security of NS Power's information technology systems and other details related to the ransomware attack. NS Power is committed to collaboration and cooperation with the Board throughout the process, and it intends to provide all information that the Board requires to resolve its inquiries. It is imperative that this information remains highly confidential and closely guarded.



7. The subject matter of the Board's inquiry is unlike typical proceedings before the Board. While an open and transparent process, with input from intervenors, is appropriate for most proceedings before the Board, the *Board Regulatory Rules* are not designed and structured for the highly sensitive nature of privacy or cybersecurity investigations.





9. Should the Board require further information regarding these special circumstances (including the detailed basis for the credible risks described above), we respectfully request that the Board panel considering this matter convene an *in-camera* meeting with NS Power.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Adam Kardash', is written above the typed name.

Adam Kardash
Partner and Co-Chair, Privacy and Data Management

- c. W. David Rankin, *Osler*
Judith Ferguson, Executive Vice President, Regulatory, Legal, and Government
Relations, *Nova Scotia Power*

Osler, Hoskin & Harcourt LLP
Box 50, 1 First Canadian Place
Toronto, Ontario, Canada M5X 1B8
416.362.2111 MAIN
416.862.6666 FACSIMILE

OSLER

Toronto

August 20, 2025

Montréal

Adam Kardash
Direct Dial: 416.862.4703
akardash@osler.com
Our Matter Number: 1268459

Calgary

***** BOARD CONFIDENTIAL *****

Ottawa

Sent by Email

Vancouver

Nova Scotia Energy Board
3rd Floor, 1601 Lower Water Street
Halifax, Nova Scotia B3J 3P6

New York

Attention: Crystal Henwood, Clerk of the Board

Dear Ms. Henwood:

M12273 – Inquiry of the Nova Scotia Energy Board (the Board) into Cybersecurity Incident of Nova Scotia Power (NS Power)

Thank you for your correspondence dated August 12, 2025. On behalf of our client, we reiterate that NS Power remains committed to working collaboratively and cooperatively with the Board to ensure that the Board receives all information needed for the Inquiry. We also thank the Board for the further information in your letter setting out the nature of the Inquiry and matters of concern to the Board.

A. Clarification of the Procedural Order Sought

NS Power understands that the Board applies the “open courts” principle, which allows for proportionate, public interest-based exceptions.¹ Our client appreciates the Board’s recognition that some of the information likely to be exchanged in this matter will be quite sensitive and require particularly strict confidentiality protection, and may warrant that it be provided only to the Board and no other parties in the proceeding.

Investigations into cybersecurity incidents generally occur within the proportionate exceptions to the “open courts” principle. By default, information received by regulatory authorities during an investigation of a cybersecurity incident is treated as confidential, including documents filed by parties. Disclosure is allowed in limited circumstances, including as part of the regulatory authority’s published report of findings. This is the nature of privacy regulatory authorities’ investigatory procedures referenced in paragraph 4(b) and footnote 1 of NS Power’s letter of August 8, 2025. Given privacy regulatory authorities’ extensive experience investigating cybersecurity incidents, we view their investigative procedures as being helpful and informative to the Board as it determines the

¹ *Sherman Estate v. Donovan*, 2021 SCC 25, at para 38.

process it will adopt for this matter. Excerpts of sample statutory provisions under Canadian and foreign privacy legislation are attached as **Appendix A**.

At the same time, NS Power expects that the Board will review claims of confidentiality throughout the Inquiry and will not automatically approve those claims without appropriate scrutiny.² To the extent that the Board has questions about NS Power's claims and rationale for confidentiality, NS Power respectfully requests the opportunity to further explain to the Board why it is necessary to hold the designated information in confidence, including, if necessary, through an oral hearing with the assistance of cybersecurity experts.

NS Power appreciates the Board will work with technical and professional advisors, including MNP Digital, to support its regulatory function. It was not NS Power's intention to prevent the Board from disclosing "Board Confidential" information to the Board's advisors. NS Power appreciates the point in your letter that the Board will consider the sensitive nature of the information in accessing its internal resources and external advisors, and assumes that any such external advisors will execute a confidentiality undertaking prior to their receipt of such confidential data.

Similarly, NS Power is assuming that all Intervenors in the Inquiry will execute a confidentiality undertaking prior to receiving any confidential data, as per the Board's normal process. Given the unique circumstances applicable to this cybersecurity incident, NS Power will have concerns regarding the highly sensitive nature of certain confidential data being disclosed in this proceeding, and, in relation to such information, will provide the appropriate justification to explain to the Board why it is necessary for the Board to hold such information in strict confidence and/or seek additional assurance as to the manner in which the information would be protected under a confidentiality undertaking, including the systems and protections that will be in place to safeguard this information.

Regarding the Board's requests for information issued on July 24, 2025 (the **IRs**), NS Power appreciates the extension granted by the Board on August 15, 2025, permitting the responses to be delivered on or before September 5, 2025. NS Power will endeavor to prioritize its efforts to respond to the IRs earlier than September 5, 2025, if possible.

NS Power also confirms that it will provide monthly progress reports regarding the Company's continuing response to the incident, and progress on the Incident Report requested by the Board. The Company will be sending the initial progress report to the Board today under separate cover. NS Power confirms that it will be in a position to file the Incident Report no later than December 31, 2025 (as required in your letter, dated July 14, 2025), and will endeavour to complete and submit the report earlier, if possible.

² Consistent with Rule 12 of the *Board Regulatory Rules*.

B. Request for Confidentiality

Further to the Board's request, attached to this letter as **Appendix B** are detailed reasons why NS Power's confidential submission of August 8, 2025 (the **Confidential Submission**) should be held in confidence by the Board. NS Power requests that Appendix B be held in confidence by the Board pursuant to Rule 12(2) of the *Board Regulatory Rules*. That said, NS Power is prepared to consent to the Board disclosing Appendix B and the Confidential Submission to the Intervenor to whom the Board has already granted standing, pursuant to the Board's normal process of requiring a confidentiality undertaking.

NS Power would be pleased to provide any further information that may assist the Board. We reiterate NS Power's commitment to working cooperatively and collaboratively with the Board throughout the Inquiry.

Sincerely,



Adam Kardash
Partner and Co-Chair, Privacy and Data Management, *Osler*

- c. W. David Rankin, *Osler*
Judith Ferguson, Executive Vice President, Regulatory, Legal, and Government
Relations, *Nova Scotia Power*

Appendix “A”

Statutory Excerpts

Federal: [*Personal Information Protection and Electronic Documents Act \(PIPEDA\)*, SC 2000, c 5, ss. 20\(1\) -\(1.1\)](#)

Confidentiality

20 (1) Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner’s duties or powers under this Part other than those referred to in subsection 10.1(1) or 10.3(2).

Confidentiality — reports and records

(1.1.) Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information contained in a report made under subsection 10.1(1) or in a record obtained under subsection 10.3(2).

* * *

British Columbia: [*Personal Information Protection Act \(PIPA BC\)*, SBC 2003, c 63, s. 41\(1\)](#)

Restrictions on disclosure of information by commissioner and staff

41 (1) The commissioner and anyone acting for or under the direction of the commissioner must not disclose any information obtained in performing their duties or exercising their powers and functions under this Act, except as provided in subsections (2) to (6).

* * *

Alberta: [*Personal Information Protection Act \(PIPA Alberta\)*, SA 2003, c P-6.5, s. 41\(1\)](#)

Restrictions on disclosure of information

41 (1) The Commissioner and anyone acting for or under the direction of the Commissioner shall not disclose any information obtained in performing their duties, powers and functions under this Act, except as provided in subsections (2) to (4).

* * *

United Kingdom: [Data Protection Act 2018, \(ICO Data Protection Act\) UK Public General Acts, 2018 c. 12, s. 132\(1\)](#)

Confidentiality of information

132 (1) A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—

(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,

(b) relates to an identified or identifiable individual or business, and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources,

unless the disclosure is made with lawful authority.

* * *

France: [Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés \(French Data Protection Act\), Chapter II, Article 11](#)

Art. II Les agents de la commission sont astreints au secret pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, sous peine des sanctions prévues à l'article 413-10 du code pénal et, sous réserve de ce qui est nécessaire à l'établissement du rapport annuel, à l'article 226-13 du même code.

Unofficial Translation

Art II The commission's agents are bound to secrecy with regard to facts, acts or information of which they may have become aware by reason of their functions, under penalty of the sanctions provided for in Article 413-10 of the Penal Code and, subject to what is necessary for the establishment of the annual report, in Article 226-13 of the same Code.

* * *

Appendix “B”
***** CONFIDENTIAL *****

NS Power’s Confidential Submission, particularly in respect of paragraphs 3-8, as well as the last sentence of paragraph 2, requires confidentiality protection because the information — when taken collectively —



NS Power has been the target of a highly sophisticated and severe criminal ransomware attack. As is typical for attacks of this nature, the threat actor employed aggressive extortion tactics—including theft and dark web posting of customer personal information—to coerce ransom payment. As publicly stated by NS Power on May 25, 2025, after careful assessment of applicable sanctions laws and alignment with law enforcement guidance, no payment has been made—or will be made—to the threat actor.



³ Sophos X-Ops, “[Press and pressure: Ransomware gangs and the media](#)”

⁴ Canadian Centre for Cyber Security, “[Ransomware playbook \(ITSM.00.099\)](#)”, at paragraph 3



In sum, there is a strong public interest in maintaining the confidentiality and limiting the distribution of certain details relating to the ransomware attack, including as found in the Confidential Submissions.



* * *

⁵ Alison Wikoff, Global Threat Intelligence – Americas Lead, PWC, ([The Crucial Role of Threat Intelligence in Risk Assessment and Incident Response Under the SEC - FEI](#)).