Request IR-1:

Cyber Security Program Effectiveness

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 18, ll 1-4

Quote:

> **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.**

Question

(a) For the twelve-month period ending March 2025, please provide the results of the quarterly cyber training and monthly phishing simulation testing.

(b) Please describe NSPI's training standards for cybersecurity. How frequently are employees required to be tested?

(c) What percentage of NSPI's employees had completed training consistent with NSPI's standards at the time of the Incident and as of the most recent date available.

(d) What are NSPI's targets and/or metrics for cybersecurity readiness; for example, what is the target for phishing success?

(e) Please provide a summary of the number and types of cyber incidents NSPI recorded in the last 5 years? What improvements have been made to systems and practices as a result of these events.

Response IR-1:

Response

(a) **Training:**

- Q1 01/17/2024 - 03/15/ 2024: 99% Completion
- Q2 04/17/2024 – 06/15/2024: 99% Completion
- Q3 07/09/2024 – 09/15/2024: 99% Completion
- Q4 10/07/2024 – 12/13/2024: 99% Completion
- Q1 01/10/2025 – 03/15/2025: 99% Completion

Phishing Failure Rate NSPI – March 2024-March 2025

2024												
	Jan	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
			1.7%	**3.7%**	**1.1%**	**2.5%**	**4.7%**	**0.2 %**	**0.5%**	**0.7%**	**14.3%**	**0.7 %**
2025												
	6.4%	**3.3%**	**0.5%**									

(b) NSPI's current cybersecurity training standards require all eligible employees to complete mandatory quarterly cybersecurity training, with a 100 perent completion rate. In addition, employees are tested through monthly phishing simulations.

(c) Approximately 99 percent at the time of the incident and 100 percent for the most recent training campaign in Q1 2026.

(d) Threshold for phishing is <= 3 percent Cyber Security phish failure rate following the removal of the best and worst month with a target of <= 1.5percent.

Request IR-2:

Customer Data Retention

Reference: NSPI Customer Privacy Policy

Quote:

> **The length of time we keep your information varies depending on the product or service in question and the nature of the information. We have retention standards that allow us to meet customer service, legal and regulatory needs. As a result, it may be necessary for us to keep some of your information on record even after the end of your relationship with us. When the information is no longer required, it is destroyed or anonymized.**

Question

(a) Please provide the retention standards referenced in the above quote.

(b) Please confirm that these standards are compliant with the Personal Information Protection and Electronic Documents Act (PIPEDA).

Response IR-2:

Please refer to NSEB IR-9.

Request IR-3:

Customer Data Retention

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 40, ll. 10-24

Quote:

> **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."**
>
> **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.**

Question

(a) Please confirm that NSPI has purged all customer SINs from NSPI systems.

(b) Based on the above quote, NSPI was aware in 2018 the Company had collected customer SIN without a valid business reason as required by PIPEDA. Please explain why, as of the date of the incident, NSPI had not expunged this data from its systems.

(c) Please provide the number of closed accounts for which NSPI still had customer SIN information at the time of the incident in the following categories:

(i) Account closed less then one year before the Incident

(ii) Account closed between one and two years before the Incident

(iii) Account closed between two and five years before the Incident

(iv) Account closed between 5 and ten years before the Incident

(v) Account closed more than 10 years before the Incident

Response IR-3:

(a) As noted in the question above, NS Power publicly committed to initiating a process to identify and remove instances of customer social insurance numbers (SINs) from its systems, subject to legal requirements to retain such information, as soon as its investigation allowed.

NS Power engaged a third-party expert to verify that customer SINs had been deleted from the systems and applications that had been determined to have previously stored customer SINs (Customer SIN Deletion), and received certification from the third-party expert of the Customer SIN Deletion on March 27, 2026.

NS Power subsequently learned that, despite this certification, there were SINs remaining in the Customer Information System (which is housed in a legacy system and was not impacted by the Incident) that had not been detected by the verification process. NS Power immediately thereafter took steps to purge these remaining SINs from those records.

NS Power confirms that, to the best of its knowledge, as of the date of this IR response, customer SINs have been purged from its systems, subject to legal requirements to retain such information (e.g., pursuant to a legal hold, or tax reporting obligations).

However, as a matter of prudence, NS Power is engaging a separate third-party expert with specialized legacy system expertise to further validate that no additional customer SINs remain in the environment (subject to the retention requirements outlined above). NS Power will maintain a program of periodic review of its records and systems to confirm that no customer SINs are present in its systems (outside of the retention requirements set out above).

(b) Please refer to Section 8.5 of the Incident Report, and SBA IR-16.

(c) Due to the nature of the records, and the complexity of the data, it is not possible for NS Power to determine this information with certainty.

Request IR-4:

Data Retention Policy Compliance with Legislation

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 40, ll 3-5

Quote:

> **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.**

Question

(a) Please explain the process NSPI uses to determine what personal information can legally be collected from customers?

(b) Please provide the results of the last available audit or review conducted by an independent third party on NSPI data collection and retention policies; if no such audit or review exists, please explain how NSPI assesses the legality of data collection practices and the frequency for this assessment.

(c) Please explain, with reference to appropriate authorities, on what legal basis NSPI retains customer data after the closure of accounts.

(d) What personal information does NSPI currently collect from customers and for what reason?

(e) Please provide the number of closed accounts for which NSPI had retained customer information at the time of the Incident.

(f) Were NSPI's customer information records in compliance with all of NSPI's relevant privacy and security policies and procedures at the time of the incident? If not, please provide a detailed discussion of the areas that were not in compliance and the steps taken since the Incident to bring the customer information records into compliance and ensure compliance going forward.

(g) What personal information currently collected from customers by NSPI is retained?

(i) For how long and for what reason?

Response IR-4:

(a) Please refer to NSEB IR-9.

(b) NS Power internally reviews its practices in relation to the processing of personal information on an ongoing basis, with consideration to evolving regulatory guidance and standards, including with respect to alignment with guidance from the Canadian privacy law regulatory guidance on privacy management programs (and related personal information practices). See response to NSEB IR-9 above for additional information on NS Power's ongoing efforts to enhance its existing privacy governance program.

(c) Please refer to NSEB IR-9.

(d) Please refer to NSEB IR-9 and INQ IR-5.

(e) Please refer to NSEB IR-21.

(f) Please refer to NSEB IR-9.

(g) Please refer to NSEB IR-9

Request IR-5:

Customer Account Collections

Reference: Exhibit 100853 - NS Power's Monthly Update #2, page 7

Quote:

> **In acknowledging that customers' billing experience was impacted by the Incident, NS Power has waived all late fees and paused collections activity since the Incident.**
> **Question**

(a) Please provide NSPI's customer account collection policies that were in effect as of the date of the incident.

(b) Please confirm that no customer accounts have been sent to credit collection agencies since the date of the incident. If not confirmed, please provide the number of accounts that have been sent to credit collection agencies since the Incident and explain why some accounts continued to be sent for collection.

(c) Has NSPI received any complaints from customers about late fee charges or referrals to collection agencies? If yes, please quantify the number of complaints and describe NSPI's actions to address these complaints.

Response IR-5:

(a) NS Power will work with customers to find a solution to manage their outstanding balances, and under normal conditions many months would pass with customer follow ups before any customer is disconnected for non-pay. NS Power will make repeated attempts to contact customers to work out a solution as we want to help customers who are struggling with an outstanding balance. Collection attempts are triggered according to a NS Power

Dunning Matrix. If a customer has been identified as high risk (high score), collection attempts will differ than for a low-risk customer (lower score).

A customer can obtain a high score and be identified as high risk if they have had issues in the past such as NSF, previous disconnect notices, final notices, broken payment terms or identified as high risk due to other means. NSP's Customer Information System calculates customer scores with each billing cycle frequently.

Example timeline of the Dunning matrix collection actions below for reference:

- Low Risk Bi-Monthly Billing collection timeline of a minimum of 170 days from the past due bill with 6 CIS notifications and 3 auto calls / emails prior to the Disconnection action start.

- High Risk Bi-Monthly Billing collection timeline of a minimum of 67 days with 2 notifications and 2 calls / emails prior to the Disconnection action start.

Further details on minimum notice required are outlined in NS Power Regulation 6.

(b) No Active customer accounts have been sent to any credit collection agencies.

- A business decision was made to resume closed account internal collections only in early September 2025 with the first account being released on October 1, 2025.

- An average of 752 accounts closed accounts per month (Oct 2025-April 2026) that did not respond to NSP's Closing Bills, emails, or phone calls, were released to an External Collection Agency.

(c) There have been no documented complaints about late fees charges (No late interest charges have been applied since NSP stopped the collection process in May 2025).

Request IR-6:

Treatment of Incident Costs

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 14, ll 18-25

Quote:

> **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.**

Question

(a) Please quantify the costs incurred to date to respond to the Incident and provide a forecast of any remaining costs NSPI anticipates incurring through December 31, 2027. Please include both internal costs and any external contracting costs

(b) Please explain how NSPI is isolating the costs associated with the incident to ensure that ratepayers will not be required to pay any of these costs now or in the future.

(c) Please discuss how many staff (FTEs) were reassigned from regular duties to respond to the Incident. Please comment on the implications for operations and customer service levels as a result of any staff being reassigned.

(d) How many staff (FTEs) originally reassigned from regular duties to respond to the Incident are still being reassigned?

Response IR-6:

(a) Please refer to CONFIDENTIAL Attachment 1. NS Power is not anticipating any costs beyond Decemeber 31, 2026.

(b) NS Power is isolating costs associated with the incident through project codes created specifically to track expenses for restoration activities, similar to how NS Power would track storm specific costs.

(c) NS Power employees shifted their capacity to support similar functions during the cyber incident. Two examples include: 1. Employees from Customer Care Credit Services, who typically support collections activity, shifted to support inbound calls where customers were calling about the cyber incident, their bills and other matters. 2. Additionally, Human Resources employees shifted to support payroll duties as workload increased there and more employees were required to help.

In both of these circumstances, work volumes had increased in one area and a different department was able to support efforts to respond to work demands.

(d) These employees described in c) have all returned to their regular duties. While collections activity has not returned to normal, these employees are still following up with customers to help find solutions on outstanding balances.

Cybersecurity Accountability CA IR-6 Attachment 1 has been removed due to confidentiality.

Request IR-7:

Cybersecurity Risk Management

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 17, ll 11-24

Quote:

> **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.**

Question

(a) Does NSPI carry insurance for cybersecurity events

(i) If yes, please provide copy of policy documents and claims documents, if any;

(ii) If not, please explain why not.

(b) Please explain the steps by which the unauthorized third party was able to gain access to NSPI's information technology systems.

(c) What was the triggering event that allowed the unauthorized third party access?

(d) What measures have been put in place that will prevent unauthorized third party access to NSPI's information and technology systems if the triggering event was to be repeated?

Response IR-7:

(a) Yes, NS Power has insurance against cyber incidents.

The company maintains cyber insurance coverage applicable to this incident. The policy is subject to confidentiality obligations owed to its insurer, and disclosure of its terms could prejudice the Company's coverage position in connection with a claim arising from the Incident. Accordingly, NS Power is not in a position to provide a copy of the complete policy. However, NS Power has provided a formal "Confirmation of Coverage" letter from the insurer setting out key information relating to this policy as Confidential Attachment 1.

(b-c) See Section 2.0 of the Incident Report provided to the Board for additional detail relating to the timeline of the Incident.

(d) See Section 8.1 of the Incident Report provided to the Board for details on the steps NS Power has taken since the Incident to enhance its existing safeguards.

Cybersecurity Accountability CA IR-7 Attachment 1 has been removed due to confidentiality.

Request IR-8:

Customer Risk Mitigation

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 38, ll 25-28, Page 39, ll 1-3

Quote:

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

Question

(a) Does NSPI view the provision of credit monitoring services as fulfilment of any future liability to customers for damages resulting from the loss of customer data from NSPI systems?

Response IR-8:

(a) NS Power continues to have no evidence that this information has been further misused, or of any financial harm to customers resulting from this Incident. NS Power's provision of complimentary credit monitoring and identity theft protection/insurance to all current and past customers, regardless of whether they have been impacted, reflects a widely recognized best practice in incident response, and in providing 5 years of protection and offering this protection broadly, exceeds the standard time offered for such incidents. The offer is not merely remedial; it is proactive, giving affected individuals meaningful tools

to monitor for and respond to potential misuse of their information. In that spirit, NS Power arranged for complimentary access to a comprehensive protection service offered by TransUnion that includes dark web monitoring as well as identity theft insurance coverage of up to $1 million.

See Section 4 of the Incident Report for additional detail on the steps taken by NS Power to mitigate potential harm to affected customers.

Request IR-9:

Data Breach Mitigation

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 38, ll 25-28

Quote:

> **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.**

Question

(a) How did NSPI determine this approach was "best-practice"?

(b) Please provide a list of mitigation measures that were considered but not implemented and explain why.

(c) Did NSPI consider financial relief, credits or bill smoothing options for the affected customers?

(i) If not, why not?

Response IR-9:

(a) Plese refer to NSEB IR-15.

(b) As noted in response to CA IR-8, NS Power adopted an approach to mitigating harm to customers that adhered to, and in many cases exceeded, the standard recommended measures that organizations across all industries take in reducing harm to customers. These measures were carefully designed to reduce the potential risk of harm to individuals following a cyber security incident. Additional detail on the measures implemented are set out in Section 4 of the Incident Report.

(c) To minimize the impact to customers, including financially, in the immediate response to the Incident, NS Power committed and confirmed that customers would not be charged late fees or interest on overdue amounts as a result of this Incident.

(d) NS Power also has not disconnected any customers for non-pay since the incident was detected. Furthermore, NS Power has actively promoted Equal Billing and up to 24-month interest free payment plans for customers who required support managing any outstanding balance.

Request IR-10:

Customer Impacts

Question

(a) For each month following the Incident up to and including the most recent month of actuals available, please provide:

(i) The total number and percentage of customer bills that were estimated.

(ii) The number of customer complaints received related to estimated bills.

(iii) Any customer service metrics tracked by NSPI such as time on hold, dropped calls or other similar metrics.

Where data for a particular month are not available either due to the impact of the Incident or other reasons, please provide an explanation.

(b) Please provide any policies or procedures NSPI had in place for responding to customer complaints with respect to estimated or inaccurate bills.

(c) What method was employed to estimate bills for customers?

(d) What, if any, changes were made to the methods used to estimate customer bills since the discover of the cyber incident. If no changes were made, does NSPI intend to undertake a review to inform future potential changes? Why or why not?

(e) For customers whose estimated bills resulted in material overpayments, does NSPI credit customers for interest on credit balances? If not, why not?

Response IR-10:

(a)

(i)

Month	% Estimated	Estimated Bills	Total Bills Issued*
May-25	73.20%	2,387	3,261
Jun-25	72.92%	491,994	674,742
Jul-25	58.71%	206,762	352,195
Aug-25	40.96%	136,366	332,912
Sep-25	52.42%	180,222	343,774
Oct-25	47.58%	160,523	337,361
Nov-25	52.39%	179,001	341,641
Dec-25	45.97%	157,290	342,168
Jan-26	15.42%	52,354	339,509
Feb-26	7.66%	25,771	336,577
Mar-26	5.02%	17,927	357,212
Apr-26	1.70%	3,963	233,273

*Note that June 2025 totals include bills from May bill cycles that were delayed by cyber incident impacts; these bills were issued in June, but reflected charges for the normal bill periods ending in May. April 2026 totals are as of bills issued through April 22, 2026.

(ii) Tracking of complaints can only be detailed to the broader category of " Billing". These are totaled below by month; a subset within each are likely specific to estimation, but that precise subset cannot be counted

Month	Supervisor Escalation (Billing)	DRO Case Opened (Billing)	Formal Escalation (through NSEB) (Billing)	DRO Appeal (Billing)
May-25	18	5		
Jun-25	33	12		1
Jul-25	118	19		3
Aug-25	90	16		3
Sep-25	69	15	2	3
Oct-25	105	34	2	3
Nov-25	101	34	8	4
Dec-25	76	11	2	3
Jan-26	101	21	2	1
Feb-26	152	50	2	1
Mar-26	162	67	7	7
Apr-26	84	18	2	2

(iii) Call statistics on billing-related calls as of April 23, 2026:

Month	Customer Billing-Related Calls	Calls Answered	% Answered within 30 seconds	Average Speed of Answer	Calls Abandoned	Average Call Length
May-25	14,883	10,661	55.30%	0:02:55	4,222	0:07:37
Jun-25	33,628	23,971	35.00%	0:05:43	9,657	0:08:22
Jul-25	36,541	26,094	22.20%	0:08:44	10,447	0:10:07
Aug-25	26,644	19,184	19.10%	0:10:29	7,460	0:10:57
Sep-25	24,769	19,025	21.40%	0:08:56	5,744	0:11:11
Oct-25	32,998	19,787	9.80%	0:17:31	13,211	0:11:40
Nov-25	31,570	18,739	6.00%	0:25:41	12,831	0:12:39
Dec-25	20,919	18,226	52.40%	0:05:51	2,693	0:11:39
Jan-26	23,762	20,627	53.60%	0:05:23	3,135	0:10:56
Feb-26	32,292	23,344	35.80%	0:13:30	8,948	0:10:55
Mar-26	34,460	24,442	29.60%	0:10:42	10,018	0:11:36
Apr-26	16,892	13,892	42.10%	0:06:49	3,000	0:10:58

(b) Please refer to Confidential Attachment 1.

(c) When NS Power lost the ability to communicate with the Advanced Metering Infrastructure (AMI) network through the cyber incident, bill estimation logic reverted to a contingency CIS subroutine which uses seasonal logic. When a bill read is missing, CIS estimates a reading using the average usage per day on bills at the specific property in the last 12 months that are considered of the same season. CIS considers two seasons – warm usage (May-Oct) and cold usage (Nov-Apr).

(d) In regular business operation, missing reads are estimated within the AMI Meter Data Management System (MDMS) when necessary. CIS estimation logic is strictly for business continuity purposes , for opt-out customers as needed and, as a legacy platform, has limited opportunity for adjustment. No review is intended, as the logic is a back-up only and the CIS platform requires replacement.

(e) Interest is not paid on payment amounts above actual usage; account credits are automatically applied to the customer's subsequent bill for ongoing energy use. However, for customers who prefer a refund, refunds by cheque are available upon request. In Q4 of 2025, NS Power supported customers with 2,080 refund requests, down from 2,268 in Q4 of 2024 and 2,542 in Q4 of 2023. Refunds can be issued for a variety of issues, including customers who might have entered a larger amount when paying through their bank, or customers who have closed an account that had a credit balance on it.

Cybersecurity Accountability CA IR-10 Attachment 1 has been removed due to confidentiality.

Request IR-11:

Customer Notification

Reference: Response to NSEB IR-1 in Proceeding M12273

Quote:

> **"NS Power developed and implemented a consistent multi-channel approach throughout the response efforts for all public communications. For each update, the transparency effort involved postings on the Company 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."**

Question

(a) Please describe any specific methods or communication channels NSPI used to try to reach former customers, particularly customers whose contact information in NSPI's records may no longer be up to date and/or who may no longer live in Nova Scotia to alert them about the Incident.

(b) Did NSPI adapt or modify its communications plan based on customer feedback at any point? If so, please describe changes made based on customer feedback.

(c) Has NSPI undertaken a review the effectiveness of its communication methods? If so, please provide a summary of any key findings. If not, does NSPI plan to complete such a review? Why or why not?

Response IR-11:

(a) A robust multi-channel approach was used to reach former customers regarding the cyber incident, to encourage them to sign up for five years of complimentry credit monitoring services. In addition to the established approach of other public communications related to the cyber incident (notice through social media channels, online paid ads, to local media, to government, key account customers and other stakeholders), communications were also shared and picked up by national media, including the Canadian Press. Advertisements were also placed in local papers across the province that included a link (QR code) to a newly created online form. This form was created specifically for former customers to validate their information as a former customer and be provided with a unique code to sign up for free credit monitoring services. The link to the form was also promoted in content across all owned, earned and paid communication channels as part of the established multi-channel approach, which included national media.

(b) Our communication plan and approach was regularly influenced, updated and modified based on feedback from customers. Based on customer feedback on difficulty signing up for credit monitoring, additional information was shared via the Nova Scotia Power website and media interviews, and more than 20 in-person community sessions were organized throughout the province to help customers with the sign up process. The locations of community information sessions were selected based on direct feedback from customers calling in to our customer care centre as well as from local government officials. Based on feedback from the in-person customer community sessions, the language in the letters to customers was simplified to focus on the steps to sign up for credit monitoring and common challenges and solutions. Additional community information sessions were also organized based on positive feedback from customers, and government officials about how helpful the sessions were to the sign up process. Additionally, based on social media monitoring and online engagements with customers, the cyber incident webpage (nspower.ca/cyber) was regularly modified, rearranged and updated to reflect and address the most current

customer questions and concerns, including the Frequently Asked Questions section of the page. Drawing on insights from online monitoring and customer-reported scams—particularly search results surfacing fraudulent emails and phone numbers—we implemented a search engine optimization (SEO) strategy to ensure accurate information and official links appeared prominently at the top of customer search results.

(c) Nova Scotia Power has undertaken to review the effectiveness of its communication efforts and strategy and make changes or adjustments based on learnings. In addition to consistently adapting and modifying its approach to reaching customers with the latest updates based on regular feedback from customers, government and other stakeholders, a pulse survey was conducted in July 2025 to assess how customers were hearing and accessing information about the cyber incident, including if they had heard about and made efforts to sign up for the free credit monitoring services being offered.

Results showed that the cybersecurity incident achieved a near-total awareness among 85 percent of Nova Scotians. Television was the primary source of initial information (24 percent). However, for those directly impacted, the company's direct communication was most effective, with 22 percent first learning of the incident via a letter from Nova Scotia Power.

After becoming aware, Nova Scotians shifted to official sources for ongoing information. The company's letter (33 percent) and website (33 percent) became the primary resources for updates. Those impacted by the breach also showed a higher need for direct support, with 13% contacting the customer care center for more information.

Among those impacted by the incident, awareness of the credit monitoring offer was very high at 84 percent. However, this awareness has not fully translated into action. The most cited reasons for delays in signing up for credit monitoring were uncertainty about where to register (29 percent), not having an access code (22 percent), and experiencing technical

issues (18 percent). The in-person community support sessions to help customers sign up for credit monitoring. mentioned in response (b) above were implemented in part due to this feedback

Based on the results, efforts were also increased to communicate with customers through paid channels to encourage sign up for credit monitoring, including ads in local papers with a quick link (QR code) for more information and to sign up. Bill inserts were also used consistently throughout the incident to update customers with the latest information.