In the Matter of

Nova Scotia Power Incorporated (NSPI)

AN INQUIRY ABOUT THE IMPACT OF THE CYBER INCIDENT ON NSPI'S COLLECTION AND RETENTION OF CUSTOMER INFORMATION, CUSTOMER SERVICE AND COMMUNICATIONS, BILLING PROCESSES AND REGULATORY MATTERS

Matter No: M12600

Pre-Filed Testimony - Redacted

Submitted to: Nova Scotia Energy Board

On behalf of: The Consumer Advocate

Prepared by: Ed Mollard, InterGroup Consultants Ltd.

June 23, 2026

InterGroup CONSULTANTS

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

LIST OF FIGURES

1.0 INTRODUCTION

This testimony has been prepared for the Consumer Advocate ("CA") by or under the direction of Ed Mollard of InterGroup Consultants Ltd. ("InterGroup").

This report reviews the Nova Scotia Power ("NSP", "NSPI", "NS Power") Cybersecurity Incident submitted to the Nova Scotia Energy Board ("NSEB" or "Board") Proceeding M12600.

Mr. Mollard notes the following:

- Mr. Mollard is an independent witness and his CV is provided in Appendix A. Mr. Mollard has 25 years of experience in the regulated electricity industry in Canada, including 16 years as Chief Financial Officer at a mid-sized northern Crown Utility. In addition to traditional CFO duties, Mr. Mollard was the senior executive responsible for revenue requirement and rate-related matters in front of the territorial regulator. Mr. Mollard also acted as the Privacy Officer for the Corporation for several years in accordance with the provisions of the PIPEDA.
- InterGroup's scope of work and instructions were to review the Incident report, specifically the circumstances surrounding the cybersecurity breach and impact on customers. The scope of review focuses particularly on matters of interest to residential customers consistent with the CA's mandate. Mr. Mollard understands the scope to encompass all normal regulatory fairness considerations and to treat customers fairly over time, not just to focus on the lowest possible rates at a given point in time.
- Mr. Mollard acknowledges his role is to provide opinion evidence to the Board that is fair, objective and non-partisan.
- Mr. Mollard has endeavoured to ensure all factual assumptions and specific information relied upon are expressly cited in his testimony.

1.1 SOURCES OF INFORMATION

This testimony relies primarily on exhibits on the record of Proceeding M12600 and M12273 including Nova Scotia Power report and responses to information requests. Other publicly available information is occasionally referenced, including other proceedings before the NSEB. References are provided in footnotes throughout the document.

2.0 SUMMARY OF RECOMMENDATIONS

Based on the analysis summarized in this report, InterGroup makes the following recommendations to the Board:

- **Recommendation 1:** InterGroup recommends NSPI be directed to update its staff training policies and targets to ensure employee cybersecurity and phishing awareness. This update should remove the averaging formula and should consider computer system access restrictions as part of the consequence for employees failing to meet the policy standard.
- **Recommendation 2:** InterGroup recommends NSP be directed to update its privacy policy to clearly specify the business purpose of collecting each type of customer information (e.g. names, birthdates, SINs, addresses, billing and consumption history), the appropriate retention period, whether the data needs to remain accessible by internet connection or can be stored offline, and the process for destroying customer information when it is no longer needed.
- **Recommendation 3:** InterGroup recommends NSP be directed to retain a third-party to conduct a compliance audit at least every three years to confirm NSP is adhering to its privacy policies. Results of these reviews should be provided to the Board.
- **Recommendation 4:** InterGroup recommends the Board direct NSP to update its Communications Policy to include a minimum of 2-3 direct notifications to all customers, not only those potentially affected, in the event of future privacy breaches.
- **Recommendation 5:** InterGroup recommends NSP be directed to undertake a further review of the specific nature of personal information breached for each customer category; residential, commercial, industrial customers and notify customers once completed.
- **Recommendation 6:** InterGroup recommends NSP be directed to review options to reach former customers who may have relocated outside the province.
- **Recommendation 7:** InterGroup recommends NSP be directed to monitor customer uptake of the credit monitoring service and explore options to improve uptake. NSP should report annually to the Board on uptake and methods implemented to improve uptake for at least the next three years.
- **Recommendation 8:** InterGroup recommends NSP be directed to offer cost reimbursement mechanisms up to the value of the service offered by NSP for customers who already had subscriptions in place or for customers who choose alternative accredited monitoring services upon provision of an invoice.
- **Recommendation 9:** InterGroup recommends NSP be directed to examine longer-term options for credit monitoring and provide a report with options to the Board.

- **Recommendation 10:** InterGroup recommends that the Board direct NSP to prioritize accelerated implementation of photo meter reads should an incident of this nature reoccur in the future.
- **Recommendation 11:** InterGroup recommends the Board directs NSP to implement a more robust contingency method for estimating customer bills in the event of a similar future incident.
- **Recommendation 12:** InterGroup recommends NSP be directed to provide a report to the Board that specifies all the costs associated with the Incident, in as much detail as possible, through 2026 and confirm NSP will not seek to recover such costs from customers. Intervenors in the current proceeding should be provided the opportunity to comment on the report.
- **Recommendation 13:** InterGroup recommends that NSP be directed to isolate any future increases in premiums related to the incident, to the extent feasible, and not pass on such higher premiums to customers through rates.

3.0 OVERVIEW OF INCIDENT

The NSPI Incident Report[1] dated December 22, 2025, states that on or around March 19, 2025 a Nova Scotia Power employee visited a website and clicked on a pop-up link which resulted in malware being downloaded and installed on Nova Scotia Power's systems. The Incident was discovered on April 25, 2025, when NS Power employees reported certain applications on the Company's systems were not functional.

Upon 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. The Company continues to have no evidence the threat actor accessed any operational technology or energy delivery systems.[2]

The attack affected a number of systems including Enterprise Resource Planning (ERP) systems, Customer Billing and related systems, Cybersecurity systems and tools and Data centre Technology.[3] In addition, investigations concluded that certain personal customer information was exfiltrated from the system. Depending on the nature of the customer account, this data included names, phone numbers, email and mailing addresses, account history, payment and billing information and in some cases Social Insurance Numbers.[4]

Since the event was discovered, the Utility has taken the following steps:[5]

1) Mitigation and Restoration – containment, eradication and remediation with external assistance, rebuild core business applications and infrastructure and review privacy policy.
2) Communications with Current Customers – with respect to stolen customer data, NSPI identified 277,000 accounts after initial investigations; an additional 97,000 affected accounts were identified after further investigations; total customers directly contacted ~375,000 impacted by data breach; customer billing not functional until June.
3) Other Stakeholders – notified 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, NERC, the Electricity Information Sharing and Analysis Center (E-ISAC), Canadian Centre for Cybersecurity (CCCS), the Royal Canadian Mounted Police, the Canadian Security Intelligence Service (CSIS), Federal Bureau of Investigation and the Office of the Privacy Commissioner.
4) Response Analysis – NSP states its belief that response was sufficient and appropriate in the circumstances; some policy/procedure review identified as potential for improvement.

[1] M12273, Exhibit N-5 Refiled Incident Report, Section 2, Pg 8-10.
[2] M12273, Exhibit N-5 Refiled Incident Report, Section 6.1, Pg 33.
[3] M12273, Exhibit N-5 Refiled Incident Report, Section 3.1, Pg 12.
[4] M12273, Exhibit N-5 Refiled Incident Report, Section 3.2, Pg 14.
[5] M12273, Exhibit N-5 Refiled Incident Report, Section 4.

The Nova Scotia Energy Board initiated a proceeding to review the incident and NSP's response (M12273). NSP was directed to prepare and file by December 31, 2025 an incident report detailing how the incident occurred, the impacts and the response by the utility. In addition, the Board issued a series of interrogatories to which NSP provided responses by the end of 2025.

Further, in response to a request from the Minister of Energy on December 3, 2025, the Board created a separate proceeding M12600 to investigate customer-service related issues with respect to the 2025 NSP Cybersecurity incident.[6] The issues identified by the Board for this proceeding include:

a) Privacy Policies and procedures relating to privacy training, responding to privacy complaints, breach response plan, retention and destruction policies

b) Governance and risk management processes addressing privacy risks

c) Collection and retention of customer information

d) Measures implemented to mitigate risk to customers from fraud and identity theft following the cybersecurity incident

e) Impact on billing accuracy, estimates and alternative measures for billing customers

f) The impact on NS Power's ability to accurately measure and bill customers under rate designs requiring real or near real time measurements, such as time of use/day rates, net-metering billing arrangements, single-phase meters without a physical demand reset feature for demand billing customers

g) Communications with customers relating to these issues and about the cybersecurity incident

h) Business and regulatory impacts

InterGroup understands the Incident has led to the following major impacts on customers:

- Data theft- Approximately one million customers comprising of current (375,000) and former (540,000) customers had their information stolen and published on the dark web.[7]
- Customer Care Service Interruptions- While NSP indicates there were no impacts on its ability to provide electricity, customers experienced service disruptions to online self-service functions and as a result could only engage with NSP through call centre channels where online options were limited.[8] Additionally, customers reported they had difficulty in reaching NSP customer call centres during the early phase of the incident.[9]

[6] M12600, Exhibit 101377 Board Letter re: Final Issues List.
[7] Compliance Letter to OPC by Nova Scotia Power Compliance Letter to the Office of the Privacy Commissioner of Canada ("OPC") By Nova Scotia Power - Office of the Privacy Commissioner of Canada.
[8] M12273, Exhibit 99535, NSP Cybersecurity Incident - Monthly Update 2, pg 3.
[9] M12273, Exhibit N-2, NSEB IR-10 (a-b).

- Billing Issues- Disruptions to customers billing processes and meter data integration, thereby leading NSP to adopt estimated billing[10] for customers above the Corporation's performance standard[11] up until March 2026.[12]

This report focuses on the scope of issues identified by the Board for proceeding M12600 and provides InterGroup's assessment of NSP's response to the cybersecurity breach specifically as it relates to impacts on customers. Recommendations on a go forward basis have been included to support NSP's preparedness for future cyber attacks, and in particular mitigate negative impacts to customers from future events.

[10]M12273, Exhibit 99535 NSP Cybersecurity Incident Monthly Update 2, Customer Billing and Customer Systems, pg 3.
[11]M12451, Exhibit N-93, NSEB IR-1(a). Performance Standard 11 – Customer Bills Estimated: As a percentage of total bills, no more than 2 percent of customer bills shall be estimated annually. This benchmark shall be fixed for the 2022 to 2026 period (M12784).
[12]M12600, Exhibit N-6, CA IR-10 (a).

4.0 CYBERSECURITY AWARENESS TRAINING

NS Power indicates at the time of the incident, its approach to privacy compliance was documented through its privacy policies and procedures.[13] We understand that NSP maintains thirteen (13) privacy policies/procedure/guidelines on personal information management, breach response procedures, records management standards, privacy training, customer privacy and impact assessment.[14] NSP states it is in the process of enhancing its overall privacy governance framework in light of the cyber incident.

NSP notes that it maintains a cybersecurity training and awareness program and conducts mandatory quarterly cyber training and monthly phishing simulation testing exercises with all employees. NSP also keeps a customer data privacy awareness and training guidelines document.[15]

According to NSP, the 2024 quarterly cyber training results for NSP employees showed 99% completion.[16] Figure 4-1 shows the results of NSP's monthly phishing simulation testing from March 2024 through March 2025. NSP's notes its target threshold for phishing is <= 3% for its cyber security phish failure rate following removal of best and worst month with a target of <=1.5%.[17] Our understanding is that NSP targets a monthly phishing failure rate of less than 3% with a target of less than 1.5% excluding the best and worst months.

[13] M12273, Exhibit N-3 Section 5.0, para 10-14.
[14] M12600, Exhibit N-10, NSEB IR-9 (a).
[15] M12273, Exhibit N-3, Section 4.1, pg 18.
[16] M12600, Exhibit N-6, CA IR-1 (a).
[17] M12600 Exhibit N-6, CA IR-1(a).

Figure 4-1: NSPI Phishing Failure Rate- March 2024 – March 2025[18]

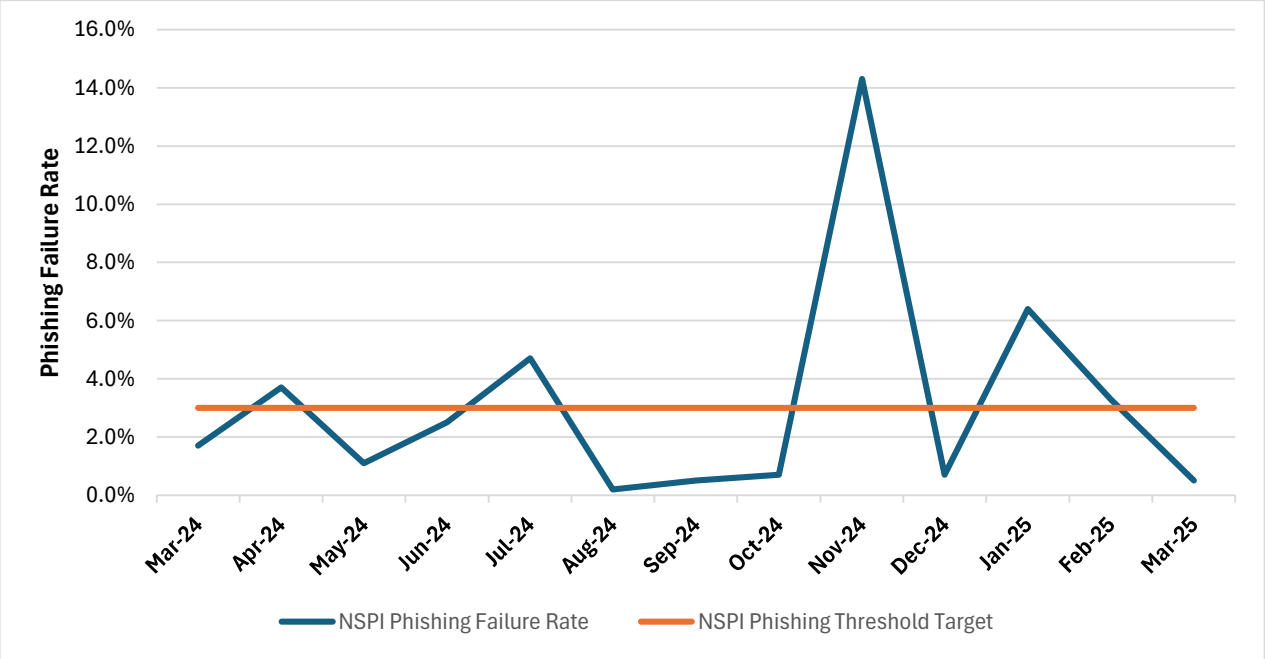

Figure 4-1 shows several months where the results exceeded the 3% target with the failure rate peaking in November 2024 at 14%. Similarly, in January 2025, the phishing failure rate was high at 6%. InterGroup calculates that NSP's average phishing failure rate was 2.3% between March 2024 and March 2025, excluding the best and worst months, in excess of the 1.5% target.[19] This indicates NSP was not meeting the targets it set for itself over this period. NSPI has indicated that certain policy guidance on how the utility reacts to unfavorable results have been enhanced.[20]

In InterGroup's view, the NSPI policy on cybersecurity awareness training needs to be amended for several issues:

1) Failure thresholds – given the nature of cybersecurity threats (i.e. single point of failure can lead to catastrophic consequences), the use of averaging formula does not appropriately measure the state of readiness to address this risk. A hacker only needs one loophole or unsuspecting employee to disrupt an organization's systems. In InterGroup's view such testing should be used to identify employees who have consistent testing failures and target those employees for additional training or other remedial measures. As well, for the same reason, it is unclear why the averaging excludes high and low results from the calculation. NSPI should investigate high results to determine

[18] M12600, Exhibit N-6, CA IR-1 (a), Table re NSPI Phishing Failure Rate- March 2024-March 2025.
[19] InterGroup's calculation excludes best month (August 2024) and worst month (November 2024) phishing failure rates.
[20] M12600, Exhibit N-11, SBA IR-9(f).

the cause. For example, if the audit used a different phishing technique, there could be legitimate issues that require rectification. For these reasons, this formula should be removed from the policy and focus solely on individual results;

2) Consequences – NSPI has indicated continued failures could affect staff STIP awards.[21] While economic impacts may be motivational for some staff, InterGroup believes NSPI should look at additional sanctions around computer system access for employees failing to meet the standard.

Recommendation 1: InterGroup recommends NSPI be directed to update its staff training policies and targets to ensure employee cybersecurity and phishing awareness. This update should remove the averaging formula and should consider computer system access restrictions as part of the consequence for employees failing to meet the policy standard.

[21] M12600, Exhibit N-11, SBA IR-9(e).

5.0 COLLECTION AND RETENTION OF CUSTOMER INFORMATION

NS Power's cybersecurity incident investigations showed that certain personal customer information for both current and former customers was exfiltrated from the system. Depending on the nature of the customer account, this data included names, phone numbers, email and mailing addresses, program participation information, date of birth, account history, driver's license number, payment and billing information, bank account details and in some cases social insurance numbers (SINs).

InterGroup notes that section 4.2 of Schedule 1 to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) sets out the principle that the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected and that where such information is used for a purpose not previously identified or required by law, that the consent of the individual is required before the information can be used for that purpose.[22]

NSP states it maintains a range of information management policy and records management standards as part of its privacy policy and procedures. However, in response to an information request,[23] NSP notes that it internally reviews its data collection and personal information practices with consideration given to regulatory provisions. The cyber incident event revealed existing issues with NSP's privacy policies and data collection retention standards which are further discussed below.

5.1 CUSTOMER SOCIAL INSURANCE NUMBERS (SINS)

NS Power states its past practice of collecting customer SINs as part of its business identification process ended in 2018 except where required for legal purposes.[24] NSP states it commenced the process of deleting customer SIN data from its Customer Information System (CIS) in 2019 whenever a SIN was encountered, but this process had not been completed at the time of the Cybersecurity incident (March 2025).[25] NSP also notes that in May 2024 it introduced a structured process to delete customer SINs but that this process also did not result in complete removal of customer SIN data by the time of the incident.

In InterGroup's view, the fact that more than 5-years after NSP began removing customer SINs from its system, such data was still stored at the time of the incident, raises concerns with the effectiveness of NSP's privacy standards and procedures.

In its March 2026 incident updates,[26] NS Power confirmed it had completed deletion of all customer SINs from the Company's database except where required for legal purposes. This was further verified by a third-party expert with a completion certification issued to NSP on March 27,

[22] Schedule 1, Section 4.2 PIPEDA. Available at: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html#h-417659.
[23] M12600, Exhibit N-6, CA IR-4(b).
[24] M12273 Exhibit N-3, NSP Incident Report, section 8.5, para 16-18.
[25] M12273 Exhibit N-3, NSP Incident Report, section 8.5, para 21-24, pdf pg 44, para 16-21.
[26] Cyber Incident Updates (March 31, 2026). Available at: Cyber Updates| Nova Scotia Power.

2026. In its information request response,[27] NSP however notes that despite the third-party review, it has discovered additional customer SINs within its legacy system which were not captured during the review process.

Although, NSP notes that these remaining SINs have been purged, in InterGroup's view, customers have a reason to be concerned with NSP's collection, storage and handling of customer information.

5.2 FORMER CUSTOMER DATA

NS Power retained personal information relating to former customers within its CIS system and these were also impacted by the cybersecurity breach. NSP states approximately 540,000 former customers were affected by the breach.[28] It is unclear what NS Power's policy is regarding retention and disposal of former customer data despite several information requests on this subject. According to NSP's Customer Privacy Policy:[29]

"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."

NSP notes that it maintains internal records-management retention standards specifying timelines for retaining records. We understand that the Information Management Policy and Records Management Standard[30] which NSP adopts is owned by Emera, the parent company. While these policies provide general guidelines on the company's records management and compliance standards, it does not contain clear disclosures regarding specific data retention or disposal timelines for each type of customer information that is collected. NSP provided a general reference to a "Records Retention Schedule[31] maintained by Emera but no further specific information was provided.

InterGroup's review of NSP's customer data retention process indicates a number of concerns:

1. Lack of transparency in NSP's internal records-management retention standards and privacy policy relating to data retention timelines. NSP currently adopts its parent company's (Emera) Information Management Policy and Records Management Standards. As noted under PIPEDA[32] principles 1 and 8, an organization is responsible for personal information under its control and should make readily available information about its policies relating to personal information management.
2. No documentation was provided supporting NSP's referenced "Records Retention Schedule". This creates a grey area to customers on how long their data is retained

[27] M12600, Exhibit N-6, CA IR-3 (a).
[28] Compliance Letter to the OPC by Nova Scotia Power, Compliance Letter to the Office of the Privacy. Commissioner of Canada ("OPC") By Nova Scotia Power - Office of the Privacy Commissioner of Canada.
[29] NSPI Customer Privacy Policy, Correcting and retaining you information available at: Privacy Statement| Nova Scotia Power.
[30] M12600 Exhibit N-10 NSEB IR-9 (a), Attachment 9 and 10.
[31] M12600 Exhibit N-10 NSEB IR-9 (a), Attachment 10, section 4, R4.
[32] PIPEDA Principle 1 (4.1) and 8 (4.8) Personal Information Protection and Electronic Documents Act.

before disposal. The general notice NSP provides to customers stating that the length of time for which information is kept varies, is quite vague and avoids accountability.

InterGroup's review of practices adopted by some other utilities indicates an average of 6 to 7 years retention period for customers data following the end of a customer's contract. NB Power generally retains customer account information for a period of 7 years after account closure.[33] PG&E typically retains customer data for an additional 5 years after end of customer relationship.[34] The Ontario Energy Board prescribes a mandatory retention period of at least 6 years for regulatory records.[35] In line with general accounting policies for data retention, the Canada Revenue Agency (CRA) also requires that records be kept for a period of six years from the end of the last period they relate to.[36]

However, InterGroup notes that while this may be required for some types of customer information, it may not be necessary for all customer information fields. Further, some information may need to be retained in a reasonably accessible format, but other sensitive data could be stored more securely offline.

3. NSP acknowledges it failed to comply with its own internal retention standards thereby exposing former customers to unnecessary risks (see response to NSEB IR-9 (b)). When further asked to provide a breakdown of the number of former customers by year based on when they ceased to be customers, NSP response was that due to the nature of the impacted records, it is unable to determine when such individuals ceased to be customers.[37]

Based on this review, InterGroup makes the following recommendations.

Recommendation 2: InterGroup recommends NSP be directed to update its privacy policy to clearly specify the business purpose of collecting each type of customer information (e.g. names, birthdates, SINs, addresses, billing and consumption history), the appropriate retention period, whether the data needs to remain accessible by internet connection or can be stored offline, and the process for destroying customer information when it is no longer needed.

InterGroup notes that the appropriate retention period and storage requirements may not be the same for each field or types of customer information. For example, driver's licences or SINs may be required for initial identity verification or tax purposes but may not need to be retained for the same duration as account billing and consumption data. Where such data is required for statistical comparison or other corporate level analysis, every effort should be made to anonymize the data. Historical customer data that is not anonymized should be firewalled or otherwise made inaccessible from the internet. These data could either be destroyed once the purpose for their collection has been fulfilled or moved into secured storage with limited access.

[33] Energie NB Power Privacy Notice, https://www.nbpower.com/en/privacy.
[34] PG&E Privacy Policy Privacy Policy | PG&E.
[35] Ontario Energy Board Mandatory Record Retention Period Policy for Regulated Entities, Letter - Mandatory Record Retention Period Policy for Regulated Entities (June 3, 2016).
[36] Canada Revenue Agency Where to keep your records, for how long and how to request the permission to destroy them early - Canada.ca.
[37] M12600 Exhibit N-6, CA IR-3(c); Exhibit N-11, SBA IR-16 (b-c).

Therefore, NSP's policy should be specific with respect to the treatment of each individual piece of customer information.

PIPEDA provides that organizations must destroy or erase personal information that is no longer required to fulfil the purpose for which it was collected.[38] A proactive approach towards deletion of sensitive customer information rather than a reactive approach should have been adopted prior to the incident and could have mitigated its impact.

Secondly, it appears NSP is not certain and cannot confidently conclude that customer SINs have truly been removed from its systems. As noted in the information request response SBA IR-16(b-c), NSP is unable to determine how many customer SINs were deleted or the percentage reduction between 2019 and April 2025. In addition, NSP plans to further engage another third-party expert to verify no additional customers SINs remain in the legacy system environment.[39] It therefore seems prudent that NSP conduct ongoing compliance audits to ensure NSP is collecting, retaining and storing customer information consistent with its policies and to identify where remedial actions are required to maintain compliance with NSP's policies.

Recommendation 3: InterGroup recommends NSP be directed to retain a third-party to conduct a compliance audit at least every three years to confirm NSP is adhering to its privacy policies. Results of these reviews should be provided to the Board.

[38]PIPEDA Schedule 1 - Principle 5 (section 4.5.3) Personal Information Protection and Electronic Documents Act.
[39] M12600 Exhibit N-6, CA IR-3 (a).

6.0 STAKEHOLDER COMMUNICATION

NS Power states that its incident response and business continuity processes were activated following the detection of the Cybersecurity breach.[40] NS Power notified relevant law enforcement agencies including the CCCS, RCMP, CSIS, and the FBI about the Incident on April 27, 2025[41], two days after its discovery. NS Power further notified the Office of the Privacy Commissioner of Canada (OPC) on May 1, 2025 (with an update on May 14, 2025) which subsequently initiated an investigation into the incident.[42]

NS Power notes that a multi-channel approach was developed and implemented for public communications to customers and other stakeholders.[43] In response to NSEB IR-3(e)[44], NS Power notes its communication approach principally consisted of direct notice to active impacted customers and public postings. This involved postings on the Company website and social media channels, notice to local media and communications directly to key account/business customers, government and other stakeholders in addition to employees.[45]

NS Power Customer Notification Timeline:[46]

- April 28, 2025: NS Power initially notified customers about the cybersecurity incident via its general public platform- website, company's social media channels and paid media.[47]
- May 1, 2025: A determination and public update notification that customers personal information was impacted was concluded by NSP.
- May 13, 2025: Direct mail notices were sent to approximately 277,000 current customers whose personal information had been impacted. This was followed by a press release and an update via NS Power website and social media channels on May 14, 2025.
- May 22, 2025: Further customer update notification provided via general public platform after discovery that customers data had been published on the dark web.
- June 25, 2025: NS Power public notification confirming that personal information relating to former customers had been impacted was released.
- October 31, 2025: Direct mail notices issued to additional 97,000 customers identified to have been impacted by the incident.

6.1 TIMING OF INCIDENT DETECTION AND INITIAL CUSTOMER NOTIFICATION

NS Power discovered the incident on April 25, 2025, over a month after the breach first occurred (March 19, 2025) and subsequently issued a public notice on April 28, 2025. This initial public

[40] M12273, Exhibit N-5 Section 2.0, pdf pg 8 para 1-3.
[41] M12273, Exhibit N-5 Section 2.0, pdf pg 8 para 19-25.
[42] M12273, Exhibit N-5 Section 2.0, pdf pg 8 para 27-28.
[43] M12273, Exhibit N-5 Section 4.2, pdf pg 19 para 24-25.
[44] M12273, Exhibit N-2, NSEB IR 3(e).
[45] M12273, Exhibit N-5 Section 4.2, pdf pg 19 para 24-28.
[46] M12273, Exhibit N-5 Section 4.2, pdf pg 20-24.
[47] M12600, Exhibit N-11 SBA IR-11 (a).

notification was done thirty-nine (39) days after the cyber breach occurred. The delay in the Company's detection of the cybersecurity breach caused harm which could have been avoided if earlier detection systems were in place. According to NSP, the technique and malware used by the threat actor could not be detected by NSPI's security detection systems.[48] NS Power's delay in detecting the breach contributed to a loss of customer trust, increased customer complaints, time lost to the breach instead of enhancing business operations, service disruptions and unplanned remediation costs amongst others. As noted by NS power, customers were unable to reach the Company's customer care team for issues other than power outages and emergency situations in the early phase of the incident.[49]

Based on this, it is important that NSP update its security detection solutions and prevention systems to deter reoccurrence of such breaches and improve the ability to detect them when they occur. InterGroup understands technical improvements in NSP's cybersecurity systems are a matter to be reviewed as part of Proceeding M12273, with a report to be provided by MNP, the Board's consultants.

In response to the M12273 NSEB's IR-9, NS Power confirmed it maintains a Cyber Incident Communication Playbook policy which details the Company's communications response approach in the event of a cyber incident. Comments on elements of NSP's communication process are provided in the following sections.

6.2 FREQUENCY OF COMMUNICATIONS TO CURRENT CUSTOMERS

NSP issued only one direct notice to current customers (sent on May 13, 2025 to initially identified 277,000 customers[50] and October 31, 2025 to 97,000 additional customers[51]) whose personal information was impacted by the breach while all other communications was conducted through general public channels.[52] It appears customers did not receive the initial set of mailings until May 22 as noted in the letters of comments.[53]

"Nova Scotia Power didn't notify me of the breach or that my information had been stolen until May 23, 2025 – two months after the breach and almost one month after your organization knew about it."

"……The breach occurred March 19th and yet customers were not notified until May 23, 2025 – two months after the incident!..."

According to the pulse survey conducted by NSP in July 2025 to assess the effectiveness of its communication method, results indicated that the direct notifications to impacted current customers was the most effective communication method.[54] Many of the impacted customers first learned about the incident through the direct letters issued by NSP.

Given the extent of the breach and its potential impact, it may have been more appropriate for NS Power to issue multiple direct notices and provide regular direct updates to customers

[48] M12600, Exhibit N-11, SBA IR-07(b).
[49] M12273, Exhibit N-2, NSEB IR-10 (a-b).
[50] M12273, Exhibit N-5 Section 4.2 Customer Notification Timeline, pg 20.
[51] M12273, Exhibit N-5 Section 4.2 Additional Customer Notification, pg 23.
[52] M12273, Exhibit N-2 NSEB IR-3 (e).
[53] M12273, Exhibit N-1 Letters of Comment pdf pg 11.
[54] M12600 Exhibit N-6, CA IR-11 (c).

especially on key issues related to pausing customer billing, estimated bills issuance, introduction of manual meter readers.

Furthermore, it may have been reasonable for NSP to also directly notify customers who were not impacted by the breach to assuage concerns regarding their personal information. As noted in NSP's pulse survey results, the company's direct communication was "most effective" for directly impacted customers, with about 22% of customers first learning about the incident through NSP letter.[55]

Recommendation 4: InterGroup recommends the Board direct NSP to update its Communications Policy to include a minimum of 2-3 direct notifications to all customers, not only those potentially affected, in the event of future privacy breaches.

The generic nature of the direct mail notices and lack of clarity on the specific personal information theft for each affected customer creates uncertainty for both current and past customers as to the extent of the data breach exposure. As noted in the letters of comments, impacted customers are interested in knowing exactly which specific information of theirs was compromised. Excerpts of customers complaints are shown below:

"I want more detailed information about the breach including more specific information about my account. For example, if I don't use pre-authorized payments, do I need to worry about my bank information? Or, why would Nova Scotia Power store my social insurance number? And, anyone who had information stolen and released on the internet should receive financial compensation because if customers need to worry about identity theft, they're not receiving adequate service from Nova Scotia Power."[56]

"No specific information relating to my NS Power Personal Profile, nor my personal data stolen. As a victim of NS Power's security breach, and according to the Personal Information Protection and Electronic Documents Act (PIPEDA), I have a legal right to know the full scope of My Personal Data Theft."[57]

NS Power acknowledges that the impacted data varied by customer and not all personal information elements would have been impacted for notified customers[58]. In response to NSEB M12273 IR-6a, NS Power notes that it is unable to determine precisely on an individual basis what specific personal customer information was affected despite the Company's investigative efforts.

In InterGroup's view it is reasonable for customers to ask NSP to specify the information that was potentially accessed.

Recommendation 5: InterGroup recommends NSP be directed to undertake a further review of the specific nature of personal information breached for each customer category; residential, commercial, industrial customers and notify customers once completed.

[55] M12600 Exhibit N-6, CA IR-11 (c).
[56] M12273, Exhibit N-1 Letters of Comment pdf pg 8.
[57] M12273, Exhibit N-1, Letters of Comment pdf pg 11.
[58] M12600, Exhibit N-3, pg 13.

6.3 COMMUNICATION TO FORMER CUSTOMERS

NS Power determined that personal information of former customers was also impacted by the breach and provided a public notification on June 25, 2025.[59] With respect to communication to impacted former customers, NS Power states that an indirect notification to the general public was conducted on the incident via the company's website, national media, social media and through paid advertising.[60] Local papers advertisements across the province included a QR code link to a customised form for former customers to validate their information.[61]

No direct notification similar to the one prepared for impacted active customers was undertaken. NS Power states that its lack of access to updated contact information for its former customers prevented a direct notification process.[62]

In one of the website excerpts FAQs[63] as shown below, NS Power committed to sending written notifications to former customers where they had contact information. InterGroup is not aware of whether or to what extent this commitment was implemented.

"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…."

The importance of direct communications to impacted customers, both current and former customers cannot be overemphasized. As noted in NSP's pulse survey results[64], many impacted current customers first discovered the incident through the direct notification letters. As such, NSP's inability to directly communicate to former customers creates a gap in its communication method which should be prioritized and resolved.

For example, [redacted] allows NSP to notify organizations such as credit card companies, financial institutions or credit reporting agencies if necessary for contacting individuals affected by the breach. There has been no documentation on whether NSP attempted to use these or other methods in its efforts to directly reach former customers.

Recommendation 6: InterGroup recommends NSP be directed to review options to reach former customers who may have relocated outside the province.

[59] M12273 Exhibit N-3, pg 21.
[60] M12273 Exhibit N-5, Section 4.2 pdf pg 23; M12600 Exhibit N-6, CA IR-11 (a).
[61] M12600 Exhibit N-6, CA IR-11 (a).
[62] M12273 Exhibit N-2, IR-1(a-d), pg 7.
[63] M12600 Exhibit N-2, NSEB IR-1 Attachment 4, pg 19.
[64] M12600 Exhibit N-6, CA IR-11 (c).

7.0 CREDIT MONITORING

According to the Incident report,[65] NS Power adopted a best-practices approach to mitigate potential harm to customers arising from the Incident. An initial two years complimentary credit monitoring system and identity protection service was offered to impacted customers and subsequently extended to five years for past and current customers.[66] This service provided by Transunion Canada includes daily access to credit reports, credit monitoring, up to $1,000,000 expense reimbursement insurance for identity theft, online educational resources, access to identity restoration agents and dark web monitoring.[67] In addition, dedicated call centres and customer support were established to provide information and credit monitoring sign up assistance to customers.[68]

Customers have raised various concerns regarding NSP's mitigation strategies:

- Customers had no input in the service provider selection process, nor the range of credit monitoring services provided.[69] Some customers noted they already had other credit monitoring subscriptions and did not need an additional service while other customers expressed the need for financial compensation for damages rather than signing up for credit monitoring.[70]
- Customers were required to sign up for access. Many customers experienced difficulty in signing up for the service. As noted in the letters of comments,[71] customers complained about incorrect activation code provided by NSP, technical difficulties, broken links, cumbersome registration process for customers who already had credit monitoring.
- Customers complained about their inability to directly reach NSP customer service, rather they were automatically redirected to TransUnion staff for credit protection.[72]

As noted by NSP in M12600, Exhibit N-6, CA IR-11(c), customer awareness of the credit monitoring offer has not fully translated into increased uptake action for impacted customers with the majority of this delay attributed to uncertainty about registration process (29%), not having an access code (22%) and technical issues (18%). Furthermore, NSP has not maintained any "success rate" or "enrollment target" for the credit monitoring services offered.[73] In InterGroup's view, NSP should be directed to monitor customer uptake of the credit monitoring service and explore methods to increase uptake.

Recommendation 7: InterGroup recommends NSP be directed to monitor customer uptake of the credit monitoring service and explore options to improve uptake. NSP should report annually

[65] M12273 Exhibit N-5, Section 4.2, pdf pg 19 para 15-16.
[66] M12273 Exhibit N-5, Section 4.2, pdf pg 21-22, Exhibit N-, NSEB IR-3(h).
[67] M12273 Exhibit N-5, Section 4.2, pdf pg 21-22.
[68] M12273 Exhibit N-5, Section 4.2, pdf pg 25.
[69] M12273 Exhibit N-5, Section 4.2, pdf pg 21-22.
[70] M12273 Exhibit N-1, pdf pg 58, 104.
[71] M12273 Exhibit N-1, pdf pg 22-23, 45, 58.
[72] M12273 Exhibit N- 1, pdf pg 94,95.
[73] M12600 Exhibit N-8, DOE IR-4.

to the Board on uptake and methods implemented to improve uptake for at least the next three years.

In InterGroup's view, it is reasonable for customers to request reimbursement for existing credit monitoring services or alternative services. NSP should not unreasonably limit customer choice of monitoring services or penalize customers who already had such subscriptions.

Recommendation 8: InterGroup recommends NSP be directed to offer cost reimbursement mechanisms up to the value of the service offered by NSP for customers who already had subscriptions in place or for customers who choose alternative accredited monitoring services upon provision of an invoice.

In InterGroup's view, the provision of credit monitoring services does not fully resolve potential future liability damages which could occur after the expiry of the credit monitoring period. In information response M12273 Exhibit N-5, NSEB IR-3(j), NS Power acknowledges that the risk of malicious attacks in the future arising from the data breach cannot be ruled out post credit monitoring.

Recommendation 9: InterGroup recommends NSP be directed to examine longer-term options for credit monitoring and provide a report with options to the Board.

8.0 FINANCIAL IMPACTS ON CUSTOMERS

As a result of the breach, several customer care systems and processes were disrupted, resulting in significant impacts to billing processes, AMI readings, and access to the online customer portal.

NSP notes the Incident disrupted customer billing processes, online self-service functions and meter data integration. The billing of many customers was affected by the breach as the Company's internal billing system was unable to access actual energy usage for customer meters.

We understand that NSP temporarily paused issuance of customer bills from 25 April to 4 June and resumed customer billing in June 2025, issuing estimated bills to customers.[74] According to NSP, "its 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)."[75]

This estimation approach resulted in inaccurate billings with customers complaining of overbilling. NSP acknowledged that some customer bills did appear larger than anticipated, attributing this to a variety of reasons; payments had not been received and processed in some cases; some customers received bills closer together as NS Power caught up on billing; and estimated bills mean that changes customers have made at the premises may not be reflected.[76]

[74] M12273 Exhibit N-2, NSEB IR-12 (a).
[75] M12600 Exhibit N-6, CA IR-10 (c).
[76] M12273 Exhibit N-2, NSEB IR-12 (a).

Table 8-1: Number and Percentage of Estimated Customer Bills[77]

(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.

Table 8-1 shows the percentage of total estimated bills issued by NSP indicating over 50% of customers bills were estimated between May and November 2025. This is significantly higher than NSP performance standard of 2% estimated bills.

In response to the 2026-2027 GRA compliance filing information requests,[78] NS Power confirmed that its meter reading and billing processes have been restored to its pre-incident state. NSP notes its billing estimation is now performing within the performance standard at or below 2%. NSP meter connections to the billing system were fully restored by March 31.[79]

Customers raised complaints about the difficulty in reaching the NSP customer care team[80], thereby compounding issues on financial impact to customers. Table 8-2 below illustrates the large number of billing related calls from customers between May 2025 and April 2026, peaking in June and July when NSP began sending estimated bills. InterGroup calculates that on average, about 27% of billing related calls were abandoned during the period, with a hike in abandoned calls seen in October and November (with about 40% abandoned calls) during the response to the Incident.[81]

[77] M12600 Exhibit N-6, CA IR-10 (a).
[78] M12451 Exhibit N-93, NSEB IR-1(a).
[79] M12451 Exhibit N-93, NSEB IR-2(d).
[80] M12273 Exhibit N-2, NSEB IR-10 (a-b).
[81] Proportion of abandoned calls calculated based on NSP IR response, M12600, Exhibit N-6, CA IR-10 (a).

Table 8-2: NSP's Statistics on billing-related calls as of April 23, 2026 [82]

(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

In acknowledging the impact on the customer billing experience, NSP note that it waived late fees and interest and paused collections and disconnection activity for active customers.[83] NS Power deployed manual meter reading in July 2025 as a temporary measure to gather usage data for residential and business meters with the aim of using such actual data for billing customers.

As noted in NSP's monthly update 4, dated December 1, 2025, the Company introduced flexible payment options for customers such as equal billing, pay-what-you-can arrangements and photo meter reads.

In InterGroup's view, an earlier introduction of the photo meter reading system could have mitigated some of the billing issues or reduced the number of estimated bills. Many utility providers allow customers to provide photos of monthly meter reads thereby helping to ensure customer bills are based on actual consumption rather than estimates.

Recommendation 10: InterGroup recommends that the Board direct NSP to prioritize accelerated implementation of photo meter reads should an incident of this nature reoccur in the future.

In response to CA-IR 10, NSP notes the CIS estimation logic used for billing customers is mainly a back-up system used for opt-out customers and business continuity purposes. Given customer complaints about overestimated bills and inaccurate billings, it appears NSP's back up billing estimate methods should be further reviewed. We understand the CIS platform is due for replacement, and more robust contingency billing estimation methods should be incorporated into NSP's new systems.

[82] M12600 Exhibit N-6, CA IR-10(a).
[83] M12273 Exhibit 99535, NSP Cybersecurity Incident Monthly Update 2, pg 6.

Recommendation 11: InterGroup recommends the Board directs NSP to implement a more robust contingency method for estimating customer bills in the event of a similar future incident.

9.0 INCIDENT COST TREATMENT

NSP notes it activated its incident response and business continuity protocols, engaging both internal and external experts to support efforts on containment, eradication and remediation of the threat.[84] We understand that NSP has incurred costs related to its containment and restoration activities and is isolating such costs through separate project codes.[85]

NSP confirmed it maintains cyber insurance coverage which is applicable to the incident.[86] NS Power anticipates a portion of costs related to the credit monitoring will be covered by the organisation's insurance and has undertaken not to pass on any costs related to the credit monitoring service to customers rates.[87]

However, it is not clearly stated whether all other costs related to the security breach remediation such as the business restoration process office (RPO), ERP restoration, containment & investigation, insurance deductibles, dedicated call centres and customer communications will be passed on to customers. It is important that customers are not made to bear the cost burden arising from these other response and mitigation strategies.

Recommendation 12: InterGroup recommends NSP be directed to provide a report to the Board that specifies all the costs associated with the Incident, in as much detail as possible, through 2026 and confirm NSP will not seek to recover such costs from customers. Intervenors in the current proceeding should be provided the opportunity to comment on the report.

Further, the magnitude of this claim may have future implications on NSP's ability to access cybersecurity in the future including higher premiums, stricter underwriting terms and increased deductibles. In InterGroup's view, customers should not be made to bear any increased premiums that may arise as a result of NS Power's insurance claim.

Recommendation 13: InterGroup recommends that NSP be directed to isolate any future increases in premiums related to the incident, to the extent feasible, and not pass on such higher premiums to customers through rates.

[84] M12273 Exhibit N-3, section 4, pg 14, para 18-25.
[85] M12600 Exhibit N-6, CA IR-6(b).
[86] M12600 Exhibit N-6, CA IR-7(a).
[87] M12273 Exhibit N-2, NSEB IR-3 (f).

APPENDIX A: Resume

EMPLOYEE NAME: ED MOLLARD

PROFESSIONAL EDUCATION/DESIGNATION:

B.Comm(Hons) University of Manitoba 1991 Certified General Accountant designation 1993

EMPLOYMENT HISTORY:

2006 – 2023	Vice President Finance and Chief Financial Officer, Yukon Energy - Provide strategic leadership in managing the financial, treasury, risk management, regulatory affairs and procurement functions. Provided\ oversight with respect to Board of Director reporting and corporate financing. Strategic direction on risk management and corporate insurance program.
2001 – 2006	Supervisor, Financial & Risk Management - Primary responsibilities included preparation of quarterly reports to Board of Director, annual financial reports. Supervised customer service personnel; lead responsibility on corporate risk management committee and liaised with corporate brokers on corporate insurance program.
2000 – 2001	Financial Analyst, NWT Financial Analyst - As a member of the corporate regulatory affairs department, participated in the preparation of revenue requirement application to the Public Utilities Board.
1991 – 2000	Auditor, Office of the Auditor General of Canada - Primary responsibilities included management and participation in the attest audit of variety of government entities, with special focus on northern clients.

InterGroup

CONSULTANTS

300-259 Portage Avenue
Winnipeg, MB R3B 2A9
www.intergroup.ca