

Nova Scotia Energy Board

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

M12600

Cybersecurity Accountability

Nova Scotia Power
Rebuttal

August 10, 2026

REDACTED

TABLE OF CONTENTS

1.0	INTRODUCTION	3
2.0	BACKGROUND	4
3.0	ADDITIONAL RELEVANT RECORDS	18
4.0	EVIDENCE OF INTERGROUP CONSULTANTS	21
5.0	EVIDENCE OF INQ LAW	42
6.0	PIPEDA AND THE ROLE OF THE OFFICE OF THE PRIVACY COMMISSIONER	58
7.0	NS POWER’S ENHANCED PRIVACY GOVERNANCE PROGRAM	60
8.0	CONCLUSION.....	65

**Cybersecurity Accountability
REDACTED**

1.0 INTRODUCTION

In a letter dated December 10, 2025, the Board initiated this matter (M12600) as a separate matter from the ongoing cybersecurity inquiry (M12273). The Board confirmed it would determine a process to consider M12600 upon receipt of the Board-directed NS Power's Cybersecurity Incident Report due by December 31, 2025. NS Power's Cybersecurity Incident Report was filed with the NSEB in M12773 on December 22, 2025, (Incident Report).¹ On February 9, 2026, via Hearing Order, the Board determined that this matter (M12600) would be addressed in an oral hearing.

On June 2, 2026, the Board issued an Amended Hearing Order. In accordance with the Amended Order, NS Power received Information Requests (IRs) on April 22, 2026. NS Power provided responses to those IRs on June 9, 2026. Evidence was received on July 8, 2026, from the Consumer Advocate's (CA) Consultant, Ed Mollard of InterGroup Consultants² (InterGroup Evidence) and from Board Counsel Consultant, Tricia Ralph, of INQ Law³ (INQ Evidence). No other parties filed evidence in this proceeding.

The following is NS Power's response to the findings and recommendations made in the InterGroup and INQ Evidence. In order to respond to the matters raised in the InterGroup and INQ evidence, NS Power retained Jena Valdetero of GreenbergTraurig, an expert in privacy breach management and legal response, to provide rebuttal evidence (Valdetero Evidence). The Valdetero Evidence is appended to this submission as Attachment 1.

NS Power has additionally provided evidence of its enhanced privacy governance program for the Board's consideration.

¹ M12600, Exhibit N-3, Incident Report (Exhibit N-3 from M12273).

² M12600, Exhibit N-13, Evidence – InterGroup, on behalf of CA, June 23, 2026

³ M12600, Exhibit N-14, Evidence – Tricia Ralph INQ Law/Consulting, June 23, 2026

**Cybersecurity Accountability
REDACTED**

2.0 BACKGROUND

The cybersecurity attack (Attack) has been described in the Incident Report, included as N-3 in M12600.

As described therein, the breach was discovered on April 25, 2025, when NS Power's employees reported that certain applications were not functional, which was as a result of the ransomware attack.

In response, NS Power undertook two separate work streams with third party experts to analyze the impacted data and determined that overall, approximately 375,000 of its current customers and approximately 540,000 former customers for a total of 915,000 customers were affected by the breach.

The compromised personal information varied by affected individual but included names, phone numbers, email addresses, mailing addresses, dates of birth, customer account histories (including customer payment/billing/credit history/bank account numbers), driver's license numbers, and in some instances, social insurance numbers (SINs).

NS Power's Response and Communications with Customers

As noted above, the Company became aware of the Attack on Friday, April 25. The Company did not know of the threat actor's existence until that day. On the next business day, Monday, April 28, 2025, NS Power informed customers that it was actively responding to a cybersecurity Attack 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 Attack, and promptly updated customers to inform them that they had identified that certain customer personal information had been impacted in the Attack and again encouraged them to remain vigilant and cautious of unsolicited communications and potential scams. The Company informed

**Cybersecurity Accountability
REDACTED**

1 customers that it was working urgently to determine the full nature and scope of the data that may
2 have been affected. The Company also initiated the process of notifying affected individuals,
3 including retaining third-party service providers to assist with this effort.
4

5 On May 13, 2025, NS Power sent direct notification via letter mail to approximately 277,000
6 current customers whose personal information the Company was able to determine had been
7 impacted in this incident.
8

9 The following morning (May 14, 2025), the Company also issued a press release and provided a
10 detailed update on its website⁴ and social media pages, all of which received widespread coverage
11 in the local and national media. Senior Company personnel participated in multiple media
12 interviews to ensure that the public remained informed about the Attack. The May 14, 2025, update
13 stated (among other things):
14

15 While the investigation remains ongoing, we have determined that on or around
16 March 19, 2025, certain customer information stored on the impacted servers was
17 accessed and later taken by an unauthorized third party.
18

19 NS Power notes that this disclosure caused some confusion among customers. Based on the
20 customer complaints included in this record, most directly notified customers received their
21 notification letters, dated May 10, 2025, via Canada Post on or about May 13, 2025. As a result,
22 some customers appear to have concluded that NS Power was aware of the threat actor's presence
23 as early as March 19, 2025, and delayed notification for nearly eight weeks. This is not the case.
24 To restate, NS Power first became aware of the Attack on April 25, 2025. Within 18 days of
25 discovering the Attack, NS Power identified and directly notified the approximately 277,000
26 affected current customers referenced above. The March 19, 2025 date referenced in the update
27 reflects the Company's subsequent determination, through its investigation, of when unauthorized
28 access initially occurred, not when the Attack was discovered by NS Power.
29

⁴ See nspower.ca/cyber for all updates posted online.

**Cybersecurity Accountability
REDACTED**

1 The process to identify what data was impacted is extremely complex. As stated in the notices sent
2 to impacted customers, the impacted data would have varied by customer, and depended, in part,
3 on the information a customer would have provided NS Power (i.e. not all personal information
4 elements listed in the direct notification letter would have been impacted for all notified
5 customers).

6
7 The Company stated in its notice to impacted customers that the unauthorized third party gained
8 access to various types of personal information of NS Power customers that included the
9 following: name, phone number, email address, mailing and service addresses, NS Power program
10 participation information, date of birth, and customer account history (such as power consumption,
11 service requests, customer payment, billing, and credit history, and customer correspondence),
12 driver's license number, and social insurance number. For some customers, bank account numbers
13 (for pre-authorized payment) may also have been impacted if this information was provided by
14 these customers. With respect to direct notifications, the Company sent two versions of letters to
15 impacted current customers, samples of which were included in response to NSEB IR-1.⁵ The
16 notices are identical, except that one of the notices indicates that based on the investigation, the
17 customer's social insurance number may have been impacted in the Attack.

18
19 In addition to direct notification via letter mail, NS Power issued communications and releases to
20 media which occurred on the following dates:

- 21
22 • Monday, April 28, 2025
23 • Thursday, May 1, 2025
24 • Wednesday, May 14, 2025
25 • Friday, May 23, 2025
26 • Wednesday, June 4, 2025
27 • Wednesday, June 25, 2025
28

⁵M12600, Exhibit N-2, NSPI (NSEB) IR-1 Attachments 1 and 2 (Exhibit N-2 in M12773).

**Cybersecurity Accountability
REDACTED**

Customers can still access these public/media updates on NS Power’s website at nspower.ca/cyber. There are “[Cyber Incident Updates](#)”, which directs viewers to the dedicated subpage where the updates are listed in chronological order.

NS Power’s notice to impacted customers also included guidance for steps customers could take to reduce any risk of harm resulting from the Attack (including steps to protect themselves from fraud or potential identity theft). This notice initially included an offer for two years of complimentary credit monitoring for impacted individuals with TransUnion. As the investigation continued and NS Power recognized the challenges associated with discerning what Personally Identifiable Information (PII) the threat actor obtained, out of an abundance of caution, the Company extended the offer of complimentary credit monitoring to five years and expanded eligibility to all current and former customers on June 25, 2025.

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

- Unlimited online access to their TransUnion Canada credit report, updated daily, which offers individuals access to their financial history and is one of the primary tools leveraged for determining credit-related identity theft or fraud.
- Unlimited online access to their credit score, updated daily.
- Credit monitoring, which provides individuals with email notifications to key changes on their TransUnion Canada credit report. These credit alerts help protect individuals against identity theft, enable quick action against potentially fraudulent activity and provide them 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 individuals with questions about identity theft. In the unlikely event that an individual becomes a victim of fraud, a personal restoration specialist will help to resolve any identity theft.

**Cybersecurity Accountability
REDACTED**

- Up to \$1,000,000 of expense reimbursement insurance related to identity theft.
- Dark Web Monitoring, which monitors surface, social, deep, and dark websites for potentially exposed personal, identity and financial information and helps protect individuals against identity theft.

Following the May 10, 2025 letters, NS Power continued to keep customers updated regarding the ongoing response to the Attack and investigation through a multi-tiered communications strategy explained further below.

On May 22, 2025, after discovering that the threat actor had published data on the Dark Web, NS Power promptly provided an update to customers through the same channels as previous updates identified above.

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 Attack. On June 25, 2025, NS Power notified the public that information related to former customers had also been impacted in the Attack and as noted above, extended an offer of five years of credit monitoring.

Given that NS Power does not have updated contact information for its former customers and given that NS Power was still working to determine the full scope of the data that may have been impacted, 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 and urged its customers who had family members that were former customers to spread the message.

**Cybersecurity Accountability
REDACTED**

Additional Current Customers Identified

NS Power's efforts to determine what data was accessed by the threat actor remained ongoing. On October 31, 2025, NS Power discovered that approximately 97,000 additional customers were impacted and sent direct notices to those customers. Identifying the approximately 97,000 additional affected customers required continued forensic analysis across multiple data systems, including environments that had been encrypted during the ransomware Attack and required extensive data recovery before their contents could be fully assessed.

Customer Support and Dedicated Call Centres

Promptly upon becoming aware of the Attack, NS Power established a dedicated call centre where individuals could receive more information about the Attack and its impacts, and support for credit monitoring sign-ups. The call centre phone 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.

When 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

**Cybersecurity Accountability
REDACTED**

1 information, was provided to NS Power on a daily basis, whose customer care team would reach
2 out to these customers.

3
4 To assist current and former customers with the sign-up process, guidance on registering for credit
5 monitoring was posted online and made available in locations throughout the province. This
6 guidance includes information on additional measures customers can take to protect themselves
7 against identity theft, as well as details on other available services.

8
9 A fact sheet was also created with information about the service and tips for signing up.⁶
10 Thousands of paper copies were distributed and available to customers across the province through
11 customer support sessions at community locations. In addition, the fact sheet was available at NS
12 Power local depots and provided to MLAs and local councilors. NS Power has also actively
13 encouraged customers and its employees to reach out to their family and neighbours to encourage
14 them to sign up.

15
16 In addition, the Company deployed dozens of employees to communities across the province to
17 provide hands-on support for customers who prefer assistance in person, recognizing that not all
18 customers may be comfortable registering online, and to ensure that customer needs are being met
19 and access to services being granted. More than 30 of these community sessions have been held to
20 date and have assisted hundreds of customers in signing up for the service. The NS Power website
21 also has been updated with additional tips and tools to help customers navigate support services.

22
23 **Existing Safeguards**

24
25 At the time of the Attack, NS Power had a common set of cybersecurity standards and policies that
26 are informed, in part, by the National Institute of Standards and Technology's (NIST)
27 Cybersecurity Framework in place. Furthermore, the Company regularly reviews and makes
28 continuous improvements to its cybersecurity programs to ensure it was and continues to be in line

⁶ M12600, Exhibit N-2, NSPI (NSEB) IR-1 Attachment 3 (Exhibit N-2 in M12773).

**Cybersecurity Accountability
REDACTED**

1 with the latest guidance. In connection with these efforts, NS Power has recently completed an
2 extensive two-year update to its cybersecurity practices to comply with current policies and
3 anticipated changes in standards communicated by NIST.

4 NS Power's cybersecurity framework includes specific policy and control standards aligned with
5 NIST's Core Functions as noted below.

6
7 In relation to NS Power's operational technology program, in addition to the NIST Cybersecurity
8 Framework, technology for NS Power's core energy operations is designed to comply with other
9 industry-specific rules and standards relating to cybersecurity and IT, including, but not limited to,
10 those mandated by the North American Electric Reliability Corporation (NERC). NERC conducts
11 extensive periodic audits (including security) of the Company's Energy Operations to ensure
12 effective compliance.

13
14 Prior to the Attack, NS Power had implemented and maintained a cybersecurity training and
15 awareness program, including mandatory quarterly cybersecurity training and monthly phishing
16 simulation testing exercises with all employees to educate employees about NS Power's
17 information security policies and common risks, and to help them understand their information
18 security responsibilities. NS Power continues to maintain and enhance this program.

19
20 While it is understood that the foregoing cybersecurity discussion is applicable to M12273, not
21 M12600, NS Power has included these high-level details herein to aid in the Board's understanding
22 of how the two proceedings may relate.

23
24 **Attack Response and Remediation**

25
26 Immediately following detection of unauthorized access, NS Power activated its incident response
27 and business continuity protocols, engaged leading third-party cybersecurity experts, and took
28 actions to contain and isolate the affected servers and prevent further intrusion.

**Cybersecurity Accountability
REDACTED**

1 When the event was discovered, NS Power mobilized a team of internal and external specialists to
2 support the recovery effort. The Company's immediate priorities focused on containment,
3 eradication and remediation of the threat, and conducting a thorough analysis to understand the
4 full scope and nature of the Attack.

5
6 Specific details of the actions undertaken are set out in Section 4.1 of the Incident Report.

7
8 **Indirect Customer Communications and Media Outreach**

9
10 The website and media updates noted above were communicated through various channels,
11 including social media, the Company website, direct notification to officials and other stakeholders
12 and direct email through the Company's provincial media distribution list. This provincial media
13 distribution list includes roughly 140 addresses reaching media outlets (television, radio, print and
14 digital) as well as individual reporters and various assignment desks across the province.

15
16 On June 4, 2025, Peter Gregg, NS Power President & CEO, was joined by Chris Lanteigne, NS
17 Power Director of Customer Care and Chris Heck, the Chief Digital Officer of NS Power's parent
18 company, Emera, to appear before the Standing Committee on Public Accounts at the NS
19 Legislature to answer questions about the Cyber Incident in a live streamed session. Following
20 this two-hour session with elected officials, Peter Gregg made himself available and spoke to
21 media gathered outside the legislative chamber.

22
23 Additionally, proactive notifications went to the following local media outlets to share information
24 about upcoming customer support sessions in local communities to help customers sign up for the
25 free credit monitoring being offered by the company.

26
27 Cape Breton – Monday, June 30, 2025

28 The Coast 89.7FM Radio - Sydney - news@coastalradio.ca

29 MBS Radio – Sydney - cbmail@mbsradio.com

30 New Country 103.5FM - news@newcountry1035.ca

**Cybersecurity Accountability
REDACTED**

1 CBC CB – Info Morning – Sydney - nicole.maclennan@cbc.ca; with an offer to interview our
2 Director of Customer Care

3
4 Springhill, Cumberland County – Thursday, July 3, 2025

5 101.7 FM CKDH

6 CFTA Tantramar 107.9 FM - cfta@eastlink.ca

7
8 Yarmouth - Tuesday, July 8

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

10
11 Bridgewater – Wednesday, July 9

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

14
15 Millbrook – Thursday, July 10

16 Outlets: CKYT Cat Country (MBS Radio) – MNN@MBSradio.com

17 CKTO EZ Rock (MBS Radio)

18
19 From July 8-11, 2025, NS Power responded to several media inquiries about customer bills and
20 meter readers being hired to manually read meters at homes and businesses across the province.
21 This media response included NS Power’s Director of Customer Care, Chris Lanteigne
22 participating in interviews with CBC NS and CBC Information Morning Mainland (noted in chart
23 below), as well as information being shared with AllNovaScotia.com, Global Halifax, MBS Radio,
24 Halifax Examiner and the Chronicle Herald.

25
26 The Company also initiated proactive outreach to local radio stations across the province to advise
27 customers of this work and avoid any confusion or concern about meter readers entering their
28 properties to read meters. Below is the list of stations that were contacted:

**Cybersecurity Accountability
REDACTED**

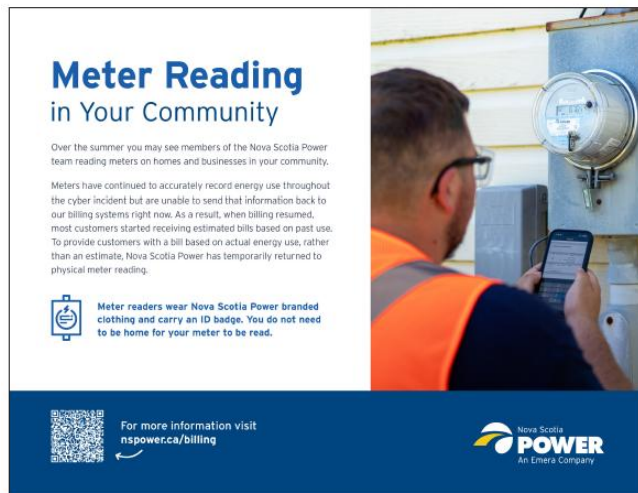
Station	Contact
WEST	
Bridgewater: CKBW Country 100.7FM	ckbwnews@radioabl.ca ; northupk@radioabl.ca
Yarmouth: CJLS	news.cjls@radioabl.ca
Liverpool: QCCR 99.3 FM	news@qccrfm.com
Kentville/New Minas: 89.3 Rewind 94.9 Magic (MBS) 97.7 AVR (MBS)	info@rewind893.ca mnn@mbsradio.com/mbsnews@mbsradio.com mnn@mbsradio.com/mbsnews@mbsradio.com
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

**Cybersecurity Accountability
REDACTED**

Station	Contact
NORTHEAST	
Amherst: CFTA Tantramar 107.9 FM	cfta@eastlink.ca
Truro: CKYT Cat Country (MBS Radio) & CKTO EZ Rock (MBS Radio)	MNN@MBSradio.com or: mbsnews@mbsradio.com
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

1
2 Advertisements were also placed in approximately 15 local and provincial newspapers across the
3 province to ensure broader reach to demographics within the province. A sample ad is provided
4 below.
5

Cybersecurity Accountability
REDACTED



The following public interviews were given by NS Power representatives:

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

**Cybersecurity Accountability
REDACTED**

Date	Media Outlet	Format	Reporter	Member of NSP senior leadership team	Topic
					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
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)

1
2 Taken altogether, any discussions surrounding the contents or timeliness of communications to
3 current and former customers must consider the substantial effort taken by the Company to ensure
4 all customers and former customers, near and far, knew that the Attack occurred and could take
5 steps to protect themselves from harm.
6

**Cybersecurity Accountability
REDACTED**

3.0 ADDITIONAL RELEVANT RECORDS

Retention Schedule and Personal Information Inventory

In response to NSEB IR-9(a) and INQ IR-4(a), NS Power provided a copy of the key policies and procedures related to its privacy framework at the time of the Attack. Given the evidence and IR responses put forth by Ms. Ralph and to ensure completeness of the record, NS Power is including its Records Retention Schedule in place at the time of the Attack, which is included as Attachment 2, as well as its Personal Information Inventory in place at the time of the Attack, which is included as Confidential Attachment 3.

December 2024 Privacy Audit of Data Lake

Additionally, NS Power wishes to raise a point of clarification, in response to INQ Law's IR-2, NS Power was asked for "(g) Privacy audit plan and dates of any audits of access to personal data of customers implemented by Nova Scotia Power in the 2 years leading up to the cybersecurity incident". NS Power interpreted this IR as related to an audit conducted on internal controls arising from access having occurred.

To clarify, an Information Protection Audit of NS Power's Data Lake was conducted in December 2024 as part of the Company's annual audit program. This report is attached as Confidential Attachment 4.

[REDACTED]

[REDACTED]

**Cybersecurity Accountability
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

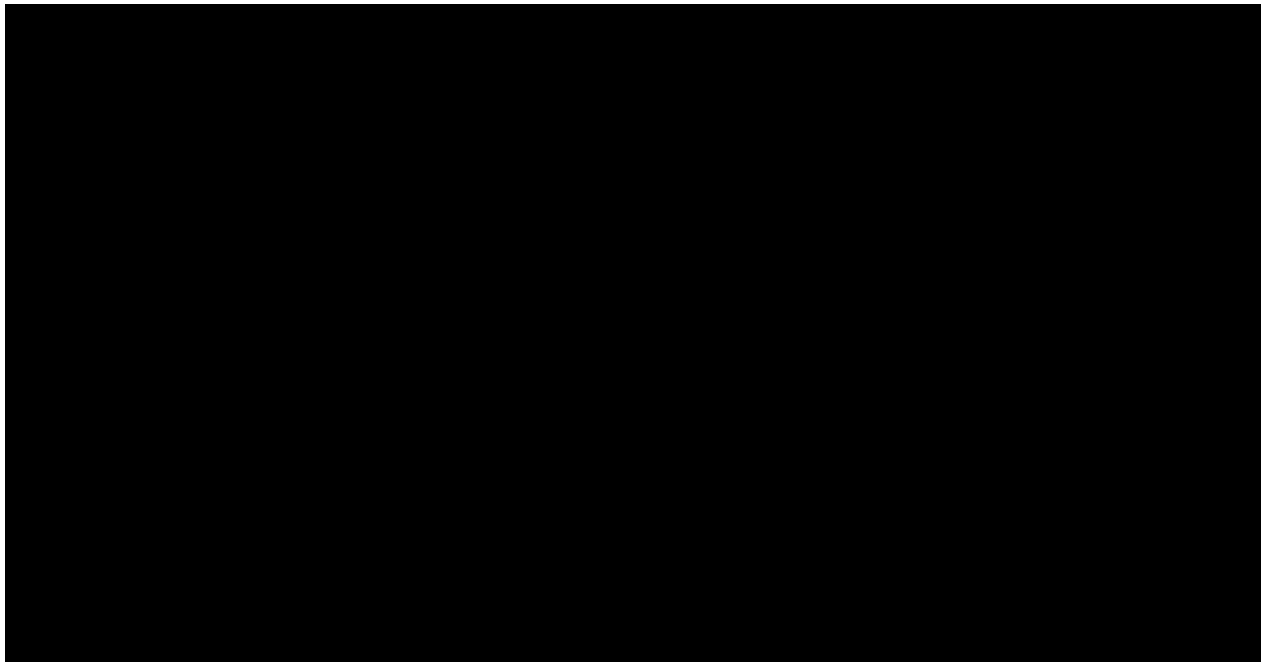
[REDACTED]

[REDACTED] Following the Attack, the Data Lake became locked under legal hold. Should NS Power establish a new Data Lake, NS Power management will ensure enhanced security monitoring and alerting is implemented.

[REDACTED]

**Cybersecurity Accountability
REDACTED**

1
2
3
4
5
6
7
8
9
10
11
12
13



Cybersecurity Accountability
REDACTED

4.0 EVIDENCE OF INTERGROUP CONSULTANTS

The InterGroup Evidence makes 13 recommendations focused on areas where NS Power's cybersecurity, privacy, communications, customer notification, billing contingency, and governance practices could be strengthened. NS Power agrees that continually enhancing cybersecurity, privacy, customer communication, and business continuity practices is critical and the Company has demonstrated throughout this process a willingness to learn from the Attack and implement enhancements where appropriate. With that said, recommendations 1, 2, 3, 4, and 6 appear to mirror existing OPC guidance that NS Power has committed to compliance with. Further, several aspects of the InterGroup Evidence would benefit from additional context and clarification from NS Power. The Company therefore addresses each of the thirteen recommendations below, noting where it agrees, where initiatives are already in place, and where further explanations or considerations may assist the Board in its assessment of reasonableness and help customers better understand the Attack, the actions taken by NS Power in response, and the enhancement that have followed.

Recommendation 1: InterGroup recommends NS Power 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.

InterGroup suggests that NS Power remove the "averaging formula" from its cybersecurity/phishing policy because it "does not appropriately measure state of readiness," and suggests that NS Power add computer system access restrictions as a consequence beyond the existing STIP impact.⁷

Regarding employee training, NS Power maintains a cybersecurity training and awareness program and conducts mandatory quarterly cyber training and monthly phishing simulation testing

⁷ M12600, Exhibit N-13, Evidence InterGroup on behalf of CA, June 23, 2026, p. 8.

**Cybersecurity Accountability
REDACTED**

1 exercises with all employees to educate employees about NS Power's information security policies
2 and common risks, and to help them understand their information security responsibilities. This
3 mandatory training is focused on current threats and the most up-to-date training materials
4 available. In addition, NS Power requires mandatory cybersecurity training as part of employee
5 onboarding, as well as remedial training for employees who fail a phishing simulation.⁸

6
7 To clarify, NS Power's individual employee consequence mechanism does not use averaging. Per
8 NS Power's response to SBA IR-09(e), individual phishing failures are tracked on a pass/fail,
9 count-based basis - not averaged. Any employee who fails is automatically enrolled in remedial
10 training as noted above. Additionally, post-Attack, NS Power implemented an enhancement to its
11 training program which requires that employees with two or more failures face additional
12 management review and a 10% short-term incentive pay reduction. This is a discrete failure-count
13 threshold, not a statistical average. This mechanism already isolates and escalates in relation to
14 repeat individual offenders exactly as InterGroup recommends.

15
16 The averaging formula InterGroup criticizes is confined to the aggregate organizational phishing-
17 failure metric used for target-setting, which serves a different purpose (trend measurement) than
18 individual accountability. In NS Power's submission, InterGroup's concern is already addressed
19 by the existing count-based individual consequence regime, independent of the organization-wide
20 average.

21
22 Regarding computer system access controls, NS Power must balance risk with ensuring employees
23 have the tools they need to perform their job function. Further, access to NS Power's computer
24 systems and data are granted, limited, and maintained based on the requirements of each role.

25
26 To NS Power's knowledge, restricting computer system access is not currently a common
27 disciplinary or punitive practice. NS Power believes that the proposed 10% STIP impact would

⁸ M12600, Exhibit N-11, SBA IR-9 (a).

Cybersecurity Accountability
REDACTED

1 provide the most meaningful incentive for accountability while avoiding unintended consequences
2 that could impair employees' ability to perform their duties and serve customers effectively.
3

4 **Recommendation 2: InterGroup recommends NS Power be directed to update its privacy**
5 **policy to clearly specify the business purpose of collecting each type of customer information**
6 **(e.g. names, birthdates, SINS, addresses, billing and consumption history), the appropriate**
7 **retention period, whether the data needs to remain accessible by internet connection or can**
8 **be stored offline, and the process for destroying customer information when it is no longer**
9 **needed.**
10

11 NS Power is not aware of any other Canadian electric utility, including the Yukon Energy
12 Corporation where Mr. Mollard was employed from 2006-2023, that provides a customer-facing
13 privacy policy with a detailed, category-by-category data inventory that links each type of personal
14 information to a specific business purpose, retention period, method of accessibility, and
15 destruction process as contemplated by the recommendation.
16

17 As noted above, NS Power's information security safeguards, including a review of all the
18 Company's privacy policies, are currently under review by a reputable and independent external
19 security assessment firm approved by the OPC. NS Power will consider and report on its efforts
20 to adopt the recommendations stemming from that review as part of its ongoing compliance
21 commitments to the OPC.
22

23 As set out in Section 5 of the Incident Report,⁹ at the time of the Attack, NS Power had formally
24 documented its approach to privacy compliance through an established suite of written privacy
25 policies, procedures, and related documentation. That framework was designed to align with the
26 Company's obligations under the federal PIPEDA which governs NS Power's collection, use, and
27 disclosure of customer information, as well as evolving regulatory expectations and industry
28 standards relating to the processing of personal information.

⁹ M12600, Exhibit N-3, Incident Report (Exhibit N-3 from M12273).

**Cybersecurity Accountability
REDACTED**

1 NS Power's Customer Privacy Policy available online¹⁰ lists the types of information the Company
2 collects and maintains:

- 3
- 4 • Name
 - 5 • Premise Address and Mailing Address
 - 6 • Email address
 - 7 • Telephone number
 - 8 • Identifying information such as your date of birth and information from government issued
9 identification, such as your driver's license number
 - 10 • Banking information and/or credit card information if you pay by credit card
 - 11 • Credit history
 - 12 • Transaction history, which includes a history of your power consumption and service
13 requests
 - 14 • Demographic and household information, such as the number of individuals per household
15 and your household heat source
 - 16 • Participation in Nova Scotia Power programs
- 17

18 NS Power identifies that the purposes for collection, use and disclosure are limited to purposes
19 that a reasonable person would consider appropriate in the circumstances. As noted in the
20 Customer Privacy Policy, some of these purposes are:

- 21
- 22 • To provide products and services to our customers;
 - 23 • To manage our business and operations;
 - 24 • To create and maintain effective business relationships with our customers;
 - 25 • To facilitate account, billing, credit, collections, and customer services;
 - 26 • To contact customers and respond to their inquiries and requests and/or to monitor and
27 assess quality of service, which may include recording telephone calls with customer care
28 agents for quality assurance and training purposes;

¹⁰ <https://www.nspower.ca/privacy-statement>

**Cybersecurity Accountability
REDACTED**

-
- To establish customer identity;
 - To assess credit history to determine if a security deposit is required from a customer or to assess an application to receive certain products and services or participate in certain programs, which includes periodically exchanging information with credit bureaus in order to maintain the integrity of the credit reporting system;
 - To collect and process past due accounts;
 - To avoid and investigate fraud and/or identity theft;
 - To address and respond to issues related to the usage of critical power dependent medical equipment during an outage;
 - To offer personalized energy management and enhanced customer energy consumption feedback, enabled through the collection of hourly consumption data;
 - To reduce energy and revenue theft which may include the collection of outage, voltage, load profile and consumption information;
 - To further develop, enhance and market products and services we offer, which may include contacting our customers to offer them participation in pilots, rebates or other programs;
 - To understand customer needs and preferences, which may include contacting our customers to ask them to participate in surveys regarding our products and services; and
 - To meet legal and regulatory requirements.

NS Power's Customer Privacy Policy notes that the length of time NS Power keeps customer information necessarily varies depending on the product or service in question and the nature of the information. The Customer Privacy Policy indicates that as a result of those customer service, legal, and regulatory needs, it may be necessary for the Company to keep some of a customer's information on record even after the end of the customer relationship with NS Power.

NS Power further notes that a customer may choose to refuse or withdraw consent to the collection, use, or disclosure of certain personal information at any time¹¹ and explains the caveat that the withdrawal of consent in some circumstances may prevent the Company from providing a

¹¹ <https://www.nspower.ca/privacy-statement#:~:text=Subject%20to%20certain,respect%20your%20choices>.

Cybersecurity Accountability
REDACTED

customer with certain products or services for which personal information is necessary. NS Power confirms that it will explain all options and any consequences of refusing or withdrawing consent and that the Company will record and respect a customer's choices.

Taken altogether, the contents of NS Power's Privacy Governance Program are aligned with expected industry standards and as suggested by the regulators in their guidance as confirmed in the INQ Evidence.¹²

NS Power is closely monitoring the Government of Canada's Bill C-36, the Protecting Privacy and Consumer Data Act, introduced June 15, 2026. While the legislation remains under consideration and its final form is not yet known, the Company is staying apprised of developments and assessing potential implications for its privacy, data governance, retention, and customer communication practices. Should this legislation be enacted, NS Power will review its policies and procedures against applicable requirements and emerging best practices and will implement changes, as appropriate, to support ongoing compliance and the protection of customer information.

Recommendation 3: InterGroup recommends NS Power 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.

In leading to this recommendation, InterGroup noted that

...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 has engaged another third-party expert to verify no additional customers SINs remain in the legacy system environment.¹³

¹² M12600, Exhibit N-14, Evidence – Tricia Ralph INQ Law/Consulting, June 23, 2026, paragraph 19.

¹³ M12600, Exhibit N-13, Evidence – InterGroup on behalf of CA, June 23, 2026, p 13.

**Cybersecurity Accountability
REDACTED**

1 This assessment would benefit from additional context, such as that provided below.

2
3 As part of the OPC's investigation being carried out under PIPEDA, NS Power committed that,
4 by March 31, 2026, it would provide the OPC with confirmation that the Company had deleted all
5 instances of customer social insurance numbers from its systems, subject to legal requirements to
6 retain such information (e.g., pursuant to a legal hold, or tax reporting obligations) and
7 implemented segregation of that data to ensure that it is not used for any other purpose. NS Power
8 obtained this certification from KPMG, which had been retained to conduct a confirmatory scan
9 and verify deletion before the March 31, 2026 deadline. After that date, NS Power became aware
10 that customer SINs remained in certain select change logs. These records were not identified
11 during KPMG's initial scan due to technical limitations in the scanning tool. Once those limitations
12 were addressed, NS Power engaged KPMG to perform a follow-up scan to verify that all remaining
13 customer SINs had been deleted. KPMG subsequently provided a follow-up certification to the
14 OPC.

15
16 Out of an abundance of caution, NS Power has also retained IBM to develop a scanning tool
17 specific to searching legacy systems, such as the CIS. The tool was designed to conduct a
18 comprehensive review of all data fields and repositories within CIS, including change logs, to
19 ensure that any remaining customer SINs are identified and deleted. This work is anticipated to be
20 completed in September.

21
22 Regarding the recommendation specifically, NS Power is not opposed to retaining a third-party to
23 conduct a compliance audit at least every three years, focusing on privacy policy related
24 compliance. As of now however, NS Power voluntarily committed to the OPC to undergo a
25 confidential security assessment with an independent third party, "LevelBlue", which
26 encompasses consideration of whether relevant privacy policies and procedures are operating
27 effectively in practice. To the extent InterGroup proposes an external recurring audit regime, NS
28 Power views such a requirement as duplicative of the commitments already established with the
29 OPC and risks creating overlapping oversight mechanisms governing substantially the same
30 privacy and security activities. NS Power believes it is appropriate to consider the implementation

Cybersecurity Accountability
REDACTED

1 of an audit regime considering the OPC compliance process audit and to ensure any regime is
2 consistent with the outcome of that process.

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

7
8 NS Power does not support Recommendation 4. Such an approach is neither required by privacy
9 law nor consistent with sound, risk-based decision-making. Both PIPEDA and OPC guidance
10 prescribe an approach that focuses on notifying individuals who are in fact affected by a breach,
11 rather than issuing broad notifications to unaffected customers as a matter of routine.¹⁴ PIPEDA's
12 breach notification regime is triggered where a breach creates a "real risk of significant harm" to
13 individuals. In those circumstances, organizations must notify the OPC and the affected
14 individuals. To be clear, the legislation does not require blanket notification to all customers
15 regardless of whether their information was involved.

16
17 Further, privacy breach notifications are serious communications. Sending breach notices to
18 customers who were not impacted can unnecessarily alarm them, create confusion regarding
19 whether their own information was compromised, and dilute the significance of future
20 notifications. This is contrary to the underlying rationale of the notification regime, which is to
21 communicate meaningful risk, not merely demonstrate that communications were sent. NS Power
22 followed the OPC framework which is based on assessing actual risk and responding
23 proportionately. Moreover, NS Power was conscious of causing "notification fatigue". If
24 customers repeatedly receive breach notices about events that do not affect them, they may become
25 desensitized and less likely to take action to protect themselves when a future notification concerns
26 their own personal information.

27

¹⁴ PIPEDA, s 10.1(3).

Cybersecurity Accountability
REDACTED

Regarding a prescriptive number of notifications, there is no evidentiary support for a one-size-fits-all communication rule for future privacy incidents as the appropriateness of notification depends on the facts of the particular breach. It is NS Power's understanding that every privacy incident differs in terms of the nature and sensitivity of the information involved, the number of individuals affected, the likelihood of misuse, and the resulting risk of harm. The OPC specifically requires organizations to assess these circumstances when determining their notification obligations.

Recommendation 5: InterGroup recommends NS Power 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.

Commercial and industrial customers are generally corporations, businesses, or other organizations, and therefore do not have "personal information" within the meaning of applicable privacy legislation. As a result, a review of the specific nature of personal information for those customer classes is not applicable. Moreover, a further review will not provide any greater or further protection to customers that have not been covered off already by offering credit monitoring.

InterGroup expresses its view that it is reasonable for customers to ask NS Power to specify the information that was potentially accessed. NS Power agrees. For residential customers, NS Power has identified the categories of information it collects that were potentially accessed and included those details in its direct notifications. The OPC's breach guidance states that individual notifications must include enough information to allow affected individuals to understand the significance of the breach and take steps to reduce or mitigate harm, and that the notice should describe the personal information involved "to the extent that the information is known".¹⁵ NS

¹⁵ See https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/#:~:text=a%20description%20of%20the%20personal%20information%20that%20is%20the%20subject%20of%20the%20breach%20to%20the%20extent%20that%20the%20information%20is%20known%3B

Cybersecurity Accountability
REDACTED

1 Power's Privacy Office responded to all requests from customers to identify what specific personal
2 information NS Power had on file for that customer, however, NS Power has no way to know what
3 the threat actor successfully accessed due to the nature of the Attack.

4
5 The Attack involved unauthorized access to data stored on NS Power's NAS and within its Azure
6 Data Lake environment, which contained tens of thousands of files. Due to the volume of files
7 involved and the manner in which the data was exfiltrated, NS Power has been unable to determine
8 with precision which specific personal information relating to each affected individual was
9 accessed or obtained. NS Power has been able to identify the data repositories that the threat actor
10 attempted to access and the categories of personal information contained within those repositories.
11 However, it cannot determine, on an individual-by-individual basis, which specific data elements
12 relating to a particular customer were viewed, accessed, or obtained. Accordingly, NS Power
13 assessed the Attack on the basis that the threat actor may have obtained the full contents of any
14 files for which there is evidence of unauthorized access. Regardless, the protective measures
15 identified in NS Power's customer notifications would be the same irrespective of the particular
16 type of information that may have been accessed.

17
18 **Recommendation 6: InterGroup recommends NS Power be directed to review options to**
19 **reach former customers who may have relocated outside the province.**

20
21 NS Power is amenable to reviewing options to reach former customers who have relocated outside
22 the province. That said, in this instance, the evidence does not establish that additional direct
23 notification mechanisms to reach former customers were available, operationally feasible, or likely
24 to have achieved materially better outcomes than the extensive notification efforts already
25 undertaken.

26
27 Nova Scotia has a somewhat transient population due, in part, to the concentration of post-
28 secondary institutions that attract students from across Canada and internationally. A significant
29 portion of former NS Power customers are individuals who resided in the province temporarily
30 while attending university or college and subsequently relocated to other provinces or countries.

**Cybersecurity Accountability
REDACTED**

1 After closing an account, many former customers no longer maintain a relationship with NS
2 Power, and the company has no ongoing means to verify or update their contact information.

3
4 When distributing direct notifications, NS Power utilized Canada Post's mail forwarding tools to
5 confirm the addresses of affected customers, however, Canada does not maintain a comprehensive
6 national address registry that private organizations can access to locate former customers through
7 address look-up tools. Once a customer has moved and ceased their relationship with the utility,
8 there are limited mechanisms available to obtain updated contact information. In these
9 circumstances, NS Power's use of direct notification to individuals for whom valid contact
10 information was available, combined with broad public notifications, media outreach, website
11 updates, paid advertising, national paid search optimization, and customer support channels,
12 represented a reasonable and proportionate approach to maximizing awareness among both current
13 and former customers.

14
15 Direct email notification to former customers who were affected and may have had an email
16 address on file was considered; however, NS Power determined that warning customers to remain
17 vigilant and cautious about any unsolicited communications (such as emails, text messages, social
18 posts or phone calls, including messages that appear to be from NS Power, asking you to provide
19 your personal information) was in the best interest of customers to reduce the risk of harm that
20 could potentially result. For this reason, NS Power determined that mitigating that risk was
21 paramount and was concerned that following up with an email from NS Power with a link to sign
22 up for TransUnion may be counterintuitive to the warnings provided and may cause customer
23 confusion.

24
25 As noted above, through the ongoing investigation at the time, NS Power determined that the
26 personal information of former customers was also accessed by the threat actor. Out of an
27 abundance of caution, and in the interest of assisting customers to further mitigate the potential
28 harm from the Attack, on June 25, 2025, all current customers not previously directly notified and
29 former customers, were indirectly notified of the details of the Attack and were provided with an
30 offer to sign up for five years of credit monitoring with TransUnion.

**Cybersecurity Accountability
REDACTED**

Recommendation 7: InterGroup recommends NS Power be directed to monitor customer uptake of the credit monitoring service and explore options to improve uptake. NS Power should report annually to the Board on uptake and methods implemented to improve uptake for at least the next three years.

NS Power has limited ability to monitor further uptake of the myTrueIdentity service. The credit monitoring service model requires the purchase of unique redemption codes that have an expiration date. The codes purchased by NS Power following the Attack have all expired. The codes issued on October 31, 2025, expired as of December 31, 2025. NS Power has purchased a select number of additional codes for customers who contact the customer care centre wishing to enroll. While NS Power cannot track uptake of the expired codes, it can report on enrollment through these additional codes; approximately 100 customers have signed up since January 2026.

As of December 31, 2025, there were 87,223 myTrueIdentity redemptions using a code provided by NS Power to its customers. Approximately 22% of eligible individuals enrolled during the initial notification wave on May 13, 2025. For context, it is NS Power's understanding that enrollment after an initial notification wave is on average, 16%. It is NS Power's understanding that a decline in enrollment across later notification efforts is consistent with many breach response programs, where most registrations occur shortly after the initial notification is issued. Further, it is NS Power's understanding that these enrollment figures do not capture utilization through the lookup tool which accounted for a significant number of additional access code redemptions.

Any enrollment codes not used through the mailing process were provided to NS Power's customer care team for further distribution and support purposes. Accordingly, there may have been additional enrollment not tracked by TransUnion.

Complaint records received by NS Power through this process note that some customers received similar coverage through a prior breach experienced by other parties, their banks, or credit card providers providing rational reason why an affected customer may opt not to sign up with myTrueIdentity.

Cybersecurity Accountability
REDACTED

1 All told, NS Power met or exceeded industry standard in the roll out of credit monitoring service,
2 extended the offer beyond industry norms and used multi-channel functions to encourage
3 enrollment through website updates, press releases, social media posts, and media interviews
4 encouraging enrollment. Additionally, NS Power updated its website with tips addressing common
5 sign-up problems, which were echoed on social media and in media interviews, and encouraged
6 employees, municipal councilors, and community partners to spread the word to families and
7 neighbours. Additionally, NS Power hosted more than 30 community support sessions province-
8 wide and deployed employees for hands-on registration help.
9

10 **Recommendation 8: InterGroup recommends NS Power be directed to offer cost**
11 **reimbursement mechanisms up to the value of the service offered by NS Power for customers**
12 **who already had subscriptions in place or for customers who choose alternative accredited**
13 **monitoring services upon provision of an invoice.**
14

15 While NS Power recognizes that some customers may already have credit monitoring
16 subscriptions in place or may prefer another provider, offering reimbursement for alternative
17 services would not be a reasonable or proportionate measure given that equivalent monitoring and
18 identity protection services are already being offered by NS Power at no cost to affected customers
19 for a term of five years. Further, the cost is not likely like-for-like. NS Power was able to secure
20 bulk pricing for redemption codes through TransUnion that would be lower than the retail cost that
21 individual customers would incur when independently purchasing comparable services.
22

23 InterGroup further states as part of this recommendation:
24

25 In InterGroup's view, the provision of credit monitoring services does not fully
26 resolve potential future liability damages which could occur after the expiry of the
27 credit monitoring period. In information response M12273 Exhibit N-5, NSEB IR-
28 3(j), NS Power acknowledges that the risk of malicious attacks in the future arising
29 from the data breach cannot be ruled out post credit monitoring.¹⁶
30

¹⁶ M12600, Exhibit N-13, Evidence – InterGroup on behalf of CA, June 23, 2026, p 19.

**Cybersecurity Accountability
REDACTED**

1 However, InterGroup has not provided evidence of any utility, regulated entity, or private-sector
2 organization that has responded to a privacy breach by offering credit monitoring services for a
3 period exceeding five years or by assuming ongoing responsibility for speculative future losses
4 arising after the expiry of the monitoring period.

5
6 This was confirmed by Ms. Valdetero in her evidence, where she stated,

7
8 I am unaware of any regulatory settlement, consent order, or adjudicative decision
9 — in Canada, the United States, the United Kingdom, or Australia — that has
10 required an organization to offer or explore credit monitoring beyond five ears as a
11 condition of resolving a breach notification regulatory proceeding.¹⁷
12

13 INQ identified one instance out of Saskatchewan, involving Innomar Strategies Inc., where the
14 Information and Privacy Commissioner recommended that credit monitoring be provided for a
15 minimum of ten years in response to a privacy breach,¹⁸ however, the breach compromised
16 personal health information such as names, addresses, dates of birth, height, weight, telephone
17 number, email addresses, dates, location of services, health diagnosis/condition,
18 medications/prescriptions, medical record number, patient numbers, health insurance/subscriber
19 number, signature, lab results and medical history were a part of the information that had been
20 exfiltrated from its systems. This is distinguishable from the case at hand. Further, NS Power has
21 no information, nor has Ms. Ralph provided any, on whether Innomar Strategies Inc. was able to
22 fulfill this recommendation.
23

24 By their nature, privacy incidents may carry the potential for residual risk. The fact that a potential
25 future misuse of information cannot be categorically ruled out does not establish that an
26 organization should be required to provide indefinite monitoring services or open-ended
27 compensation for hypothetical potential future harms. Rather, the appropriate question is whether
28 the mitigation measures being offered are reasonable, proportionate, and consistent with industry
29 practice.

¹⁷ Attachment 1, Valdetero Evidence, p 21.

¹⁸ M12600, Exhibit N-15. INQ responses to CA IR-3, filed July 29, 2026.

Cybersecurity Accountability
REDACTED

1 NS Power submits that the five-year credit monitoring and identity protection package being
2 provided is a significant and robust mitigation measure. In the absence of evidence demonstrating
3 that organizations facing comparable privacy incidents have provided monitoring for longer
4 periods or accepted continuing liability beyond the monitoring term, there is no basis to conclude
5 that additional obligations are warranted in this case.

6
7 **Recommendation 9: InterGroup recommends NS Power be directed to examine longer-term**
8 **options for credit monitoring and provide a report with options to the Board.**

9
10 It is NS Power's understanding that only 6% percent of breach response incidents supported by
11 TransUnion include five years of credit monitoring, making NS Power's offering a longer-than-
12 average coverage period.

13
14 According to statistics provided to NS Power from TransUnion, only six percent of
15 companies who were victims of a cyber security incident in 2025 and utilized
16 TransUnion for their credit card monitoring services offered five years of credit
17 monitoring following a breach. As such, a two-year offer aligns with standard
18 industry practice across Canada for organizations across industries (financial
19 services, healthcare, retail, telecommunications, education, etc.) when they suffer a
20 ransomware or other data breach involving sensitive personal information.¹⁹

21
22 Furthermore, as confirmed by INQ, the offer of five years of credit monitoring was reasonable.²⁰

23
24 **Recommendation 10: InterGroup recommends that the Board direct NS Power to prioritize**
25 **accelerated implementation of photo meter reads should an incident of this nature reoccur**
26 **in the future.**

27
28 InterGroup further notes that an earlier introduction of the photo meter reading system could have
29 mitigated some of the billing issues or reduced the number of estimated bills.

30

¹⁹ Attachment 1, Valdetero Evidence, p 20.

²⁰ M12600, Exhibit N-14, Evidence – Tricia Ralph INQ Law/Consulting, June 23, 2026, paragraph 105.

Cybersecurity Accountability
REDACTED

1 NS Power agrees that customer-submitted photo meter reads are a valuable tool in supporting
2 billing accuracy when regular meter reading processes are disrupted. However, the Company
3 wishes to clarify that earlier implementation of photo meter reads during this event was
4 constrained. In the months following the Attack, photo meter reads required manual ingestion into
5 the Customer Information System (CIS), and the volume of customer accounts affected by the
6 Attack made large-scale manual processing impracticable. Photo meter reads became available
7 again on November 21, 2025 as soon as operational processes were established to support their
8 use. Approximately 775 customers submitted photo meter readings by the end of 2025, and
9 approximately 80 percent of photo meter reads were successfully used to adjust estimated bills.²¹

10
11 That said, NS Power acknowledges the benefits of facilitating photo meter reads more quickly
12 during significant billing disruptions and is evaluating opportunities to improve this capability. As
13 part of the ongoing CIS replacement project, NS Power will assess the feasibility of automated
14 photo-read ingestion and related technologies that could reduce manual processing requirements
15 and enable a more efficient use of customer-submitted meter reads in the future.

16 The Company submits that the specific timing and design of future system enhancements should
17 remain subject to the technical evaluation, operational requirements, and prudent investment
18 considerations evaluated as part of the broader CIS replacement project that is underway. The
19 Board has directed NS Power to report on the status of this project in NS Power's next Annual
20 Capital Expenditure proceeding.

21
22 **Recommendation 11: InterGroup recommends the Board direct NS Power to implement a**
23 **more robust contingency method for estimating customer bills in the event of a similar future**
24 **incident.**

25
26 InterGroup notes:

27
28 In response to CA-IR 10, NSP notes the CIS estimation logic used for billing
29 customers is mainly a back-up system used for opt-out customers and business

²¹ M12600, Exhibit N-4, NSPI (NSEB) IR-14(f) (Exhibit N-4 in M12273).

**Cybersecurity Accountability
REDACTED**

1 continuity purposes. Given customer complaints about overestimated bills and
2 inaccurate billings, it appears NSP's back up billing estimate methods should be
3 further reviewed. We understand the CIS platform is due for replacement, and more
4 robust contingency billing estimation methods should be incorporated into NSP's
5 new systems.²²
6

7 NS Power's view is that any consideration of contingency methods for estimating customers' bills
8 is in the scope of the CIS Replacement Project which is targeted for mid-2029. The new system
9 architecture will include improved estimation logic, will eliminate manual/out-of-system
10 calculations, and support modern billing methods. In the interim, NS Power has restored the more
11 robust estimation capabilities available from the AMI platform (which had been in place since
12 AMI was implemented in 2019) which is now cloud-based (as opposed to an on-premise AMI
13 platform). The cloud-hosted AMI platform is architected with redundancies that are not reliant on
14 the on-premises corporate network and therefore not subject to the compromise as occurred on
15 April 25, 2025. This means that actual meter reads or AMI-generated estimates keep flowing to
16 billing even during an on-premises cyber event, mitigating the need to use the legacy CIS
17 estimation, other than for opt-out customers.
18

19 It is important to note that NS Power's existing contingency was layered and consistent with the
20 redundancy principle. NS Power's primary estimation method, and first contingency, is statistical
21 imputation within the AMI/smart meter data model. When the Attack severed communication with
22 the AMI network, estimation reverted to the CIS seasonal subroutine as the designed fallback. NS
23 Power was aware of limitations associated with its secondary contingency like shoulder-season
24 tuning (April–May, October–November transitions) which were bounded and being actively
25 managed by the Company's billing team (e.g., NS Power reverted November 1, 2025 bills back to
26 warm billing on November 21, 2025 after analysis showed the shoulder season results). All told,
27 the CIS seasonal subroutine functioned as designed, however, it was overwhelmed by the
28 unprecedented volume and duration of the billing disruption. If NS Power does revert to CIS
29 estimated billing again, the Company has tracked lessons learned, has more detail regarding how
30 to adjust seasonal logic further for accuracy, and will consider all reasonable efforts to become

²² M12600, Exhibit N-13, Evidence - InterGroup on behalf of CA, June 23, 2026, page 22.

**Cybersecurity Accountability
REDACTED**

1 better equipped to handle volume and duration if the seasonal subroutine remains a secondary
2 contingency.

3
4 As a final point, InterGroup seems to validate complaints about overestimated bills and inaccurate
5 billing without performing any analysis on the accuracy of estimated billings in relation to actual
6 bills as part of this recommendation. InterGroup notes:

7
8 This estimation approach resulted in inaccurate billings with customers
9 complaining of overbilling. NSP acknowledged that some customer bills did appear
10 larger than anticipated, attributing this to a variety of reasons; payments had not
11 been received and processed in some cases; some customers received bills closer
12 together as NS Power caught up on billing; and estimated bills mean that changes
13 customers have made at the premises may not be reflected.²³

14
15 InterGroup's Evidence replicates Table 8-1 provided by NS Power to show the monthly totals of
16 estimated bills from May 2025 to April 2026. InterGroup then links this Table 8-2, a replication
17 of a Table provided by NS Power to suggest that the large number of customer billing-related calls
18 related to inaccurate billings with customers complaining of overbilling. The existence of customer
19 complaints and increased call volumes does not, on its own, demonstrate that estimated bills were
20 wholly inaccurate or that customers experienced widespread overbilling.

21
22 Table 8-1 establishes the prevalence of estimated bills, while Table 8-2 establishes heightened
23 customer call activity related to billing. However, the evidence does not assess estimation
24 accuracy, quantify any systematic over- or under-billing, identify the drivers of customer calls
25 related to billing, or compare the performance of NS Power's estimation methodology against
26 alternative approaches.

27
28 On the contrary, the available evidence suggests that instances where reconciliation of estimated
29 and actual consumption resulted in a customer credit, represented a relatively small proportion of

²³ M12600, Exhibit N-13, Evidence – InterGroup, on behalf of CA, June 23, 2026, p 20.

Cybersecurity Accountability
REDACTED

total bills issued during the recovery period.²⁴ In addition, refund requests declined over the course of the response to the Attack. NS Power's experience was that billing escalations increased as actual meter reads were restored, suggesting that customer concerns were not limited to overestimation and, in many cases, related to the reconciliation process itself following the return to actual billing.²⁵ These results are consistent with the challenges inherent in any large-scale transition from estimated to actual billing and do not necessarily demonstrate a systemic flaw in the contingency estimation approach.

None of this is to suggest that the customer experience was unaffected by the incident. Clearly, the use of estimated bills during the recovery period created uncertainty and frustration for some customers. However, InterGroup's recommendation for a more robust contingency billing methodology is ultimately presented without an assessment of estimation accuracy, error rates, or comparison to alternative methodologies. As such, the recommendation is more properly characterized as a continuous improvement suggestion for future events rather than a finding that NS Power's contingency billing approach resulted in widespread inaccurate billing or unreasonable customer impacts.

Recommendation 12: InterGroup recommends NS Power 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. Intervenor in the current proceeding should be provided the opportunity to comment on the report.

Given the Company's existing disclosures and clear commitment that restoration costs will not be passed on to customers, NS Power does not believe any additional direction from the Board is necessary in relation to Recommendation 12. Furthermore, the reporting of same is not required given the fact that rates in effect in 2025 were determined in 2022 and those in effect for 2026 and

²⁴ M12600, Exhibit N-10, NSPI (NSEB) IR-23. Overbilling or overpayment scenarios represent less than 1% of bills post-recovery. There were 23,989 residential bills that had a "true up bill" which amounted in a credit balance. The average credit amount for residential customers of the 23,989 true up bills was \$169.

²⁵ M12600, Exhibit N-10, NSPI (NSEB) IR-23.

Cybersecurity Accountability
REDACTED

1 that will be in effect for 2027 have already been confirmed to have been developed prior to the
2 Attack and therefore do not include any related costs.

3
4 As NS Power noted throughout M12451, the 2026/2027 General Rate Application proceeding, the
5 revenue requirement forecast was developed prior to the Attack and therefore does not include
6 costs related to the restoration effort. In addition, the restoration program is expected to be
7 substantially complete by the end of the current GRA period. Accordingly, these costs are not
8 included in rates, and NS Power has already confirmed it does not intend to seek recovery of these
9 costs from customers through rates.

10
11 NS Power has been tracking and reporting costs associated with the cyber security restoration
12 effort. A substantial portion of these costs is covered through the Company's insurance policies,
13 with any remainder being expensed by NS Power. Again, none of these restoration costs are being
14 recovered from customers. This is a matter that has already been before the Board in M12451.

15
16 **Recommendation 13: InterGroup recommends that NS Power be directed to isolate any**
17 **future increases in premiums related to the incident, to the extent feasible, and not pass on**
18 **such higher premiums to customers through rates.**

19
20 Carrying appropriate insurance coverage is a fundamental and prudent utility practice. Further,
21 insurance is purchased to protect against losses and their financial impacts regardless of fault.
22 Insurance premiums are typically established based on an insurer's assessment of the utility's
23 overall risk profile, claims history, market conditions, and numerous other factors which can
24 change year over year.

25
26 Under the regulatory compact, the mechanism for excluding a cost from rates is a finding that the
27 cost was imprudently incurred – which is determined by the Board through evidence, generally, at
28 the time of a rate application. InterGroup's recommendation 13 instead, directs a blanket future
29 exclusion now, without waiting for the causal/prudence record to be put forward regarding why
30 premiums might rise. This substitutes an anticipatory directive for the regulatory compact's

**Cybersecurity Accountability
REDACTED**

1 evidentiary process which, to the extent necessary, is appropriately dealt with in the Company's
2 next rate application.
3

Cybersecurity Accountability
REDACTED

5.0 EVIDENCE OF INQ LAW

NS Power acknowledges that the INQ Evidence may assist the Board in understanding privacy concepts and generally accepted privacy practices. However, care must be taken in assessing Ms. Ralph's conclusions regarding "unreasonableness". The Board has already determined that the issue before it is not whether NS Power complied with privacy law. Rather, the Board's task is to assess the reasonableness of NS Power's actions as a regulated utility. The existence of alternative approaches, evolving best practices, or opportunities for improvement does not, without more, establish that NS Power acted unreasonably. As the Board recognized, broader questions of privacy compliance and interpretation fall within the specialized expertise of the OPC, and such compliance is not determinative of the question before it under the PUA.²⁶

Each of Ms. Ralph's eight findings of unreasonableness as summarized at paragraph 106 of the INQ Evidence will be addressed in turn.

The reasonableness of NS Power's actions regarding use of a PI inventory.

INQ notes:

An adequate PI inventory as a privacy program control is a critically important building block. In their guidance, the regulators explain that organizations need to be able to determine what PI it holds and where, why it is collecting, using or disclosing PI, and the sensitivity of the PI it holds. In its confidential response to NSEB IR-9, NSPI provided its records management policies, within which NSPI directed that there be a PI inventory. A copy of the PI inventory was not provided and therefore it is not possible for me to give an opinion on it. However, because NSPI said that it does not know and will never know what data points for each individual impacted customer were exposed through the Incident, this raises concerns about the fulsomeness of NSPI's PI inventory practices.²⁷

²⁶ M12600, Doc. 101377, Board Letter re Final Issues List, March 25, 2026.

²⁷ M12600, Exhibit N-14, INQ Evidence, page 6, paragraph 13.

**Cybersecurity Accountability
REDACTED**

1 NS Power has had a Personal Information Inventory in place since 2018. As noted above, it has
2 been attached hereto as Confidential Attachment 3.

3 In INQ's response to CA IR-1, INQ added, when asked how a "well-structured PI inventory"
4 could have enabled Nova Scotia Power to determine what data points were affected by the cyber
5 incident", INQ noted:

6
7 A well-built inventory maps personal information (PI) at the field level to the
8 systems and repositories where it resides, not just at the system level. A well-
9 structured PI Inventory would not just indicate what systems were compromised
10 but also what specific data points were exposed. Had NSPI sufficiently mapped and
11 inventoried both system level and more granularly, field level, this should have
12 allowed NSPI to determine which exact data points were exposed, as opposed to
13 types of PI that may have been compromised.²⁸

14
15 The opinion appears to conflate the purpose of a personal information inventory with the objectives
16 of a forensic investigation. A privacy inventory may identify the categories and fields of personal
17 information that reside within a system, even at the field level, but it does not establish which
18 specific records or data elements were accessed, viewed, or exfiltrated by a threat actor during a
19 cyber incident. That determination is typically dependent on forensic evidence such as system logs,
20 access records, and exfiltration analysis. Consequently, even a highly mature field-level inventory
21 would not have enabled NS Power to determine with certainty which exact data elements relating
22 to individual customers were compromised. At most, such an inventory would identify the types
23 of personal information capable of being stored within the affected systems. NS Power knew this
24 information and provided specifics in both its direct and indirect notification to customers.

25
26 Further, NS Power was able to identify customers that had their SINS compromised and sent out a
27 different version of the May 10, 2025 direct notification letter indicating so.

28

²⁸ M12600, Exhibit N-15, INQ response to CA IR-1b, July 29, 2026.

Cybersecurity Accountability
REDACTED

1 **The reasonableness of the timeframe to notify former customers.**

2
3 Ms. Ralph concludes that NS Power's customer notification approach was unreasonable. However,
4 the evidence shows that NS Power engaged experienced privacy, cybersecurity, and incident-
5 response advisors throughout the incident and that those advisors supported the Company's
6 approach.

7
8 As noted above and in NS Power's response to M12273 NSEB IR-1, the timing of notification
9 was driven by the need to understand the nature and scope of the incident, identify affected
10 individuals, and provide meaningful information to customers.

11
12 The evidence also demonstrates that NS Power's notification occurred comparatively quickly,
13 relative to many large-scale cybersecurity incidents, and was undertaken while forensic
14 investigations were ongoing.

15
16 As noted in the Valdetero Evidence, it is necessary to appreciate the entire timeline for the context
17 regarding the Incident and NS Power's communication to customers, media and others about the
18 Attack, its potential impact and the protections being offered by NS Power through TransUnion.²⁹
19 The timeline is set out below.

- 20
21 • **April 25, 2025:** NS Power discovered the Incident when employees reported certain
22 applications were not functional. NS Power immediately activated its incident response
23 and business continuity protocols and engaged Osler and, through Osler, Mandiant's
24 cybersecurity and incident response team.
25
26 • **April 27, 2025:** NS Power notified the Canadian Centre for Cybersecurity (CCCS), the
27 RCMP, CSIS, and the FBI.
28

²⁹ Attachment 1, Valdetero Evidence, section 5.0, p 6.

**Cybersecurity Accountability
REDACTED**

-
- 1 • **April 28, 2025:** NS Power informed customers on its website that it was actively
2 responding to a cybersecurity incident.
3
 - 4 • **May 1, 2025:** NS Power determined that customer personal information had been
5 impacted, provided an update on its website that it had “identified that certain customer
6 personal information was accessed and taken by an unauthorized third party and notified
7 the OPC.” NS Power also initiated the process of notifying affected individuals and
8 retained third-party service providers to assist.
9
 - 10 • **May 13, 2025:** NS Power sent direct notices to approximately 277,000 current customers
11 whose personal information it could determine had been impacted and offered two years
12 of credit monitoring and identity theft protection services through TransUnion. NS Power
13 sent two versions of the letter: (1) a version identifying that customer SINS may have been
14 affected; (2) a version to individuals where SINS were not collected and therefore could
15 not have been impacted by the Incident.
16
 - 17 • **May 14, 2025:** NS Power issued a press release and provided a detailed update on its
18 website and social media pages, receiving widespread local and national media coverage.
19
 - 20 • **May 22, 2025:** NS Power became aware that the threat actor had published data on the
21 dark web
22
 - 23 • **May 23, 2025:** NS Power posts update on website and prior channels.
24
 - 25 • **May 28, 2025:** The OPC initiated a formal investigation into the Incident.
26
 - 27 • **June 4, 2025:** NS Power leadership appeared before the Nova Scotia Public Accounts
28 Committee, confirmed that customer data had been exfiltrated, and encouraged existing
29 account holders to sign up for free credit monitoring.
30

Cybersecurity Accountability
REDACTED

-
- 1 • **June 25, 2025:** Via substitute notice on its website, in the media, on social media,
2 stakeholders, paid advertising, national paid search optimization, NS Power notified the
3 public that former customer information had also been impacted. NS Power simultaneously
4 extended its credit monitoring offer from two years to five years for all current and former
5 customers. Affected customers who had already enrolled in the two-year product offer were
6 automatically extended to five years.
7
 - 8 • **June 30, 2025:** NS Power sends proactive notices to Cape Breton media outlets.
9
 - 10 • **July 3, 2025:** NS Power sends proactive notices to Springhill media outlets.
11
 - 12 • **July 8, 2025:** NS Power sends proactive notices to Yarmouth media outlets.
13
 - 14 • **July 9, 2025:** NS Power sends proactive notices to Bridgewater media outlets.
15
 - 16 • **July 10, 2025:** NS Power sends proactive notices to Millbrook media outlets.
17
 - 18 • **September 19, 2025:** NS Power posted information on its website explaining how all
19 customers can sign up for free credit monitoring for five years, providing a link to same,
20 and reminding customers that the sign-up period for this credit monitoring would end on
21 September 30, 2025.
22
 - 23 • **October 31, 2025:** NS Power sent direct notices to approximately 97,000 additional
24 customers identified as impacted.
25
 - 26 • **November 3, 2025:** NS Power again posted information on its website explaining how
27 those customers who had now received a letter could sign up for free credit monitoring for
28 five years, providing a link to additional information on signing up for this offer.
29

Cybersecurity Accountability
REDACTED

-
- **December 31, 2025:** Enrollment period for TransUnion closes for all customers; however, NS Power continues to offer free credit monitoring upon request.

Ms. Valdetero disagrees with the findings in the Ralph Report regarding the reasonableness of notice to former customers. In doing so, Ms. Valdetero states:

While I agree that it is important to take steps to identify whether sensitive personal data was affected in an incident and act quickly to notify as soon as feasible, a finding of unreasonableness is not sustained by the evidentiary record when the full factual context is considered. Any assessment of reasonableness is contextual and should distinguish between the timing of NS Power's determination that former customer information may have been implicated and the operational feasibility of reaching that population with meaningful, accurate, and usable notice. Where reliable contact information was not available, indirect notice was not a failure of notice; it was a recognized notification mechanism expressly permitted by Canadian law, provided it was reasonably designed to reach affected individuals.³⁰

The most immediate issue to be addressed following a major security incident is the threat of ongoing threat actor access and incursion and potential disruption of operations. NS Power's top priority was ensuring continuity of services to customers. It is also important to identify what information was taken by the threat actor. As stated by Ms. Valdetero:

In the course of responding to a cybersecurity incident as extensive and severe as the Incident, a company can typically begin to look for current contact information for those affected only after the following: restoration of the affected systems, extraction of copies of documents from the file tree, engagement of a third-party e-discovery service provider to review said files, and then compilation of a list of individuals identified in the files. Then, the company typically must retain a vendor, like TransUnion, to assist with providing credit monitoring and identity theft services, mailing notices to the affected population, and establishing a call center to assist with customer inquiries about the Incident. The record establishes that NS Power took these very steps, but in the context of considerable operational disruption caused by the threat actor.³¹

³⁰ Attachment 1, Valdetero Evidence, p 8-9

³¹ Attachment 1, Valdetero Evidence, p 10

**Cybersecurity Accountability
REDACTED**

1 The amount of information exfiltrated was approximately 13 Terabytes (Tb) of data, there were
2 3.1 million files on the threat actor's file tree, and the ransomware encrypted files and systems in
3 both on-premises and cloud storage systems. This was not a routine privacy breach; it was a large-
4 scale ransomware event. Despite this, NS Power mailed 277,000 letters to current customers on
5 May 13, 2025, less than three weeks after it discovered the Incident. Ms. Valdetero notes that this
6 was an impressive response in the circumstances:
7

8 NS Power's understanding of the file enabled it to engage TransUnion and take
9 steps to mail letters to current customers, which NS Power did incredibly quickly
10 to mail 277,000 letters on May 13, 2025. In my experience, it is unusual for any
11 company experiencing a ransomware event of this scale to notify affected
12 individuals less than two weeks after determining that customer personal
13 information had been impacted. In my experience, direct notice to approximately
14 277,000 current customers within this timeframe was unusually fast for a
15 ransomware incident of this scale, particularly where the organization was
16 simultaneously managing containment, restoration, customer support, and
17 regulatory communications.³²
18

19 Not surprisingly, there are different challenges associated with obtaining contact information for
20 former customers, which is acknowledged by Ms. Valdetero:
21

22 My understanding is that NS Power did not have confidence that it had current
23 addresses for former customers. As customers of a local utility often discontinue
24 services because they relocate, this fact is not unusual and is consistent with my
25 experience advising a large U.S.-based utility company for the past five years. The
26 transient nature of NS Power's customer base is compounded by the existence of
27 six universities in Nova Scotia, all of which are serviced by NS Power. NS Power
28 worked with the assistance of third-party experts highly experienced in responding
29 to large scale cyber security incidents to determine whether it was possible to
30 identify current addresses for former customers, ultimately determining it could not
31 do so with any degree of confidence.³³
32

33 To assist with notification to former customers, NS Power worked with TransUnion and Sogica to
34 develop a website where customers could obtain a credit monitoring code. NS Power also had to

³² Attachment 1, Valdetero Evidence, p 10.

³³ Attachment 1, Valdetero Evidence, p 11.

Cybersecurity Accountability
REDACTED

coordinate broad notification to customers by website, media, social media, stakeholder communication, advertising, community outreach and search engine optimization. As noted in its response to CA IR-11, 85 percent of respondents in a July 2025 consumer pulse survey indicated they were aware of the incident. This communication strategy took time to arrange and deploy, and it is necessary to consider the totality of this approach, while continuing to provide electricity service to customers, in determining what was reasonable in the circumstances.

The reasonableness of the timeframe for additional customer notification.

As noted above in the timeline, 97,000 additional customers were notified of the Incident on October 31, 2025. This represents a targeted individual outreach approach following continued analysis to determine the customers affected. Again, consideration of the relevant context and circumstances are essential to assessing the reasonableness of any of the decisions made or actions taken by NS Power. Ms. Valdetero finds that the timing of notification to additional customers was wholly appropriate under the circumstances:

The elapsed time between the May 13 notification and the October 31 notification requires contextual analysis that Ms. Ralph's approach does not fully or otherwise sufficiently provide. The October 31 direct mailing should be understood as a later, more individualized outreach step made possible by continued forensic and data analysis, not as the first point at which NS Power communicated about the Incident to potentially affected individuals. In my view, based on my experience, the timing of NS Power's additional customer notification was wholly appropriate and reasonable under the circumstances.³⁴

The reasonableness and sufficiency of information included in customer notices

INQ opines that it is best practice that an organization structures its systems so it can make determinations as to identify which data points were in fact breached as specifically as possible in notification letters. INQ states:

³⁴ Attachment 1, Valdetero Evidence, p 13.

Cybersecurity Accountability
REDACTED

1 In addition, as set out above, NSPI stated that factors affecting its ability to
2 determine specificity were the nature of the impacted records and the structure of
3 the data available. While I do not have enough information to determine exactly
4 what is meant by this, and although it is not within my scope to assess the technical
5 aspects of why this specificity could not be determined, it is best practice that an
6 organization structure its systems so it can make these determinations. In my
7 opinion, the contents of customer notices were insufficient and unclear and
8 therefore unreasonable.³⁵

9
10 Ms. Valdetero disagreed with the conclusion in the Ralph Report that the contents of the customer
11 notices were insufficient and unreasonable, recognizing, as INQ did, that it is not always possible
12 to parse out the data points that were in fact breached for such a large number of customers in
13 circumstances involving exfiltration of different types of customer data. Ms. Valdetero noted:

14
15 Customers were sent two different types of notifications: those where SINS were
16 collected and therefore could have been affected in the Incident and those whose
17 SINS were not collected and therefore not affected. The remaining data elements
18 identified as potentially exposed are those that either were collected of most if not
19 all customers (e.g., contact information and date of birth) or those where a customer
20 would reasonably be aware if they provided that information to NS Power (e.g.,
21 banking information for those enrolled in autopay). PIPEDA expressly
22 contemplates that a notifying organization may not know every data element with
23 customer-specific precision at the time notice is provided.

24 In my view, the remaining contents of the letter provided clear guidance fully
25 consistent with accepted industry standards. The use of a TransUnion call center is
26 a common industry practice to ensure rapid response to callers, and any difficulties
27 with credit monitoring were addressed through community outreach and the
28 dedicated TransUnion call center. In my opinion, NS Power acted reasonably and
29 met or exceeded industry standards in its notification strategy.³⁶

30
31 It would not have been possible to identify all the different data impacted in the breach while
32 notifying customers in a three-week timeline. In its investigation, NS Power did differentiate
33 between customers whose SINS may have been impacted and those whose SINS were not taken.
34 Further, NS Power was compliant with PIPEDA in terms of the contents of its notification to

³⁵ Exhibit N-14, INQ Evidence, para 57.

³⁶ Attachment 1, Valdetero Evidence, p 15-16.

**Cybersecurity Accountability
REDACTED**

1 customers. The decision to advise customers of the potential categories of information was both
2 defensible and reasonable in the circumstances.³⁷

3
4 **Collection of SINS**

5
6 INQ opines that the collection of SINS, aside from where necessary for legal or tax reporting
7 purposes, was unreasonable.³⁸

8
9 To be clear, other than as required by law, NS Power has not collected customer SINS for nearly a
10 decade. Based on informal discussions with other major utilities in Canada, it is NS Power's
11 understanding that the collection of SINS to confirm the identification of a customer was a common
12 practice during the relevant period; however, as privacy practices and standards evolved and
13 changed over time, NS Power made the decision in 2018 to cease the practice and, since 2018, NS
14 Power has not collected customer SINS other than as required by law, including for tax reporting
15 requirements.

16
17 **Not identifying that SINS were collected in NS Power's public-facing Customer Privacy**
18 **Policy was unreasonable.**

19
20 NS Power only collects customer SINS in a very limited set of circumstances where they are
21 required for income tax reporting purposes related to customer deposits. Under Section 237 of the
22 Income Tax Act, Canadian institutions are legally required to make a "reasonable effort" to collect
23 the SIN from any customer opening or holding an interest-bearing account. This directive ensures
24 that banks can accurately report earned interest and dividends to the Canada Revenue Agency
25 using T5 tax information slips. The collection, use, and disclosure of customer SINS is restricted
26 to this specific purpose and is not part of NS Power's routine customer information collection
27 practices.

28

³⁷ Attachment 1, Valdetero Evidence, Finding 3(b), p.17

³⁸ Exhibit N-14, p 26, para 106.

**Cybersecurity Accountability
REDACTED**

1 NS Power's Customer Privacy Policy advises customers that personal information may be
2 collected, used, and disclosed to satisfy legal and regulatory requirements which would include
3 tax reporting. Given the narrow and infrequent circumstances in which SINs are collected from
4 customers, NS Power also relies on a specific point-of-collection process to provide customers
5 with detailed information about the purpose of the collection.

6
7 To elaborate, the specific point-of-collection process is as follows: when tax reporting
8 requirements arise, a Customer Care Representative discusses the requirement directly with the
9 customer and explains why the SIN is being requested, how it will be used, and the related tax
10 reporting obligations. Customers are then given the opportunity to voluntarily provide or decline
11 to provide their SIN. Where a customer agrees to provide their SIN, NS Power obtains express
12 verbal consent and is provided with the SIN verbally. This approach ensures that customers receive
13 clear and meaningful notice at the time the information is collected, when the information is most
14 relevant to them. The point-of-collection notice and express consent process provides customers
15 with specific information regarding the collection and use of their SIN for T5 reporting purposes,
16 supplementing the general privacy disclosures contained in NS Power's Customer Privacy Policy.
17 Accordingly, customers are well apprised of the purposes of collection in a manner that
18 communicates more directly than in the Company's Privacy Policy.

19
20 Further, NS Power has surveyed the public-facing Customer Privacy policies of several Canadian
21 utilities, including Newfoundland and Labrador Hydro, NFLD Power, Maritime Electric, NB
22 Power, Hydro Quebec, Hydro One, Manitoba Hydro, SaskPower, ATCO, BC Hydro, Yukon
23 Energy, and Northwest Territories Power Corp. Of those utilities, only Hydro Quebec mentions
24 SINs in its public-facing Privacy Policy.

25
26 **Keeping record of records destruction activities.**

27
28 While the company maintains retention and destruction policies, it does not maintain detailed
29 records sufficient to verify the destruction of each individual record or file. Automated records
30 destruction activities that are programmed, such as the deletion of SINs, are managed through the

**Cybersecurity Accountability
REDACTED**

1 IT Change Management process which captures the description, activity date, and approvals for
2 the activity.

3
4 **Reasonableness of retaining customer data beyond the time frames set out in its internal**
5 **record retention standards.**

6
7 As previously discussed, what is reasonable is contextual and this applies equally to what may be
8 a reasonable or necessary timeframe as it relates to PIPEDA. While NS Power retained customer
9 data beyond the timeframes set out in its record retention schedule, the retention schedule had been
10 developed with specific technical functionalities in mind and strict adherence to it was not possible
11 until those functionalities were in place. The technological evolution of how information is stored,
12 transferred, and used within businesses is part of the relevant context that must be considered when
13 entities are developing, operationalizing, and implementing privacy frameworks. PIPEDA, as well
14 as NS Power's Records Management and Privacy policies and procedures recognize and account
15 for this reality.

16
17 More specifically, there were three systems where personal information was retained for longer
18 than the timeframe set out in the retention schedule and which resulted in the exposure of customer
19 information as a result of the Attack.

20
21 The first is NS Power's Customer Information System (CIS). To be clear, CIS itself was not
22 impacted by the Attack; however, a copy of data containing customer personal information from
23 CIS made in July 2021 to support the MyEnergy Insights project existed in a staging area of the
24 Azure Data Lake and was accessed by the threat actor.

25
26 This data existed in CIS in the first instance as the CIS is a legacy system of a vintage where
27 automated removal of data is not an option. NS Power had identified the need to remove SINS
28 from CIS and began to manually do so in 2018 before carrying out a more robust approach in 2024
29 to remove all SINS from the main customer database within CIS. This involved developing an
30 approach to identify nine-digit numbers within the database and remove them by "zeroing-out"

**Cybersecurity Accountability
REDACTED**

each number. This was done to mitigate the risk of adverse impacts within CIS as the removal of the data / line-item could have broader implications within the system and result in catastrophic impacts. These processes were resource-intensive and dependent on individual review and execution, resulting in progress that was slower and less comprehensive than anticipated.

Similarly, this risk also exists with other forms of personal information within CIS and the manual removal of such a large amount of data was deemed to present a significant risk to the system. Considering the risks to a system that is integral to the delivery of customer services, NS Power elected to remove all SINS by replacing them with zeros. This decision reflected both the sensitive nature of SINS and their consistent format within the system (i.e., universally represented as nine-digit numbers), while helping to ensure that all other personal information could be effectively removed during the implementation of a new CIS. In a more modern CIS, there would be a function that monitors age of customer data, and that would allow for such information to be automatically removed. This function will be developed as part of NS Power's CIS modernization project.

It is these limitations within CIS coupled with the timing of the copy from CIS to the Data Lake staging area in 2021 that resulted in past customer information and SINS being present in the Azure Data Lake staging area.

A data lake is a centralized repository that ingests, stores, and allows for processing of large volumes of data in its original form. Data within the Azure Data Lake was encrypted in transition and at rest. Work streams within the Azure Data Lake, including in the staging area, were automated to cycle through the age of information every 14 and 90 days and automatically remove the data on those timelines. This automatic setting must be manually engaged and, while it was in place and functioning for other workstreams within the Azure Data Lake, it was not in place to capture the data that the threat actor was able to access from the staging area. Since the Attack, the Azure Data Lake has been on legal hold, isolated from NS Power's systems, and locked down with limited access privileges. Once it can be removed from legal hold, NS Power intends to destroy it and is in the process of rebuilding a new data lake.

**Cybersecurity Accountability
REDACTED**

1 In addition to the CIS and Azure Data Lake, personal information was also retained in NS Power's
2 Network Attached Storage (NAS). The NAS was a dedicated storage device that enables multiple
3 users to store and share files from a central location. The NAS contained millions of files
4 supporting various aspects of NS Power's operations and business, including some employee and
5 customer information.

6
7 Similar to CIS, there was no ability to automate the removal of files from the NAS and in order to
8 address the challenge this presented to ensuring retention timelines were met, prior to the Attack,
9 the Company had a plan in place to provide business units with a defined deadline to convert files
10 from the NAS to SharePoint Online, which would allow for appropriate security classifications to
11 be utilized and corresponding retention schedules to be automated, following which all records
12 contained in the NAS would be destroyed.

13
14 As part of that conversion effort, individual employees migrating data from the NAS to SharePoint
15 Online would identify personal information and that data would be cleansed from data migrating
16 to SharePoint Online. While this work was scheduled to occur, the Attack preceded the work being
17 undertaken. As a result, personal information (retained longer than the timeframe set out in the
18 retention schedule) existed in the NAS at the time of the Attack and some of the drives containing
19 this information were accessed by the threat actor. Since the Attack, the NAS has been on legal
20 hold, isolated from NS Power's systems, and locked down with limited access privileges. Once it
21 can be removed from legal hold, NS Power intends to destroy it and has no intention of rebuilding
22 it as the Company has now migrated systems to Sharepoint Online.

23
24 While NS Power acknowledges it had personal information on its systems beyond the timeframes
25 set out in its retention schedule, the information was present within CIS and NAS due to technical
26 limitations that, prior to the Attack, had been identified with plans in place to address and ensure
27 that NS Power would be able to fully implement its retention schedule as intended.

**Cybersecurity Accountability
REDACTED**

Reasonableness of credit monitoring offer

NS Power wishes to also address INQ's finding that the initial offer of two years of credit monitoring was not reasonable, while the subsequent offer of five years was reasonable.³⁹

It should be noted at the outset that in Canada there is no prescribed or regulated minimum credit reporting period for data breaches, including under PIPEDA. Duration of complimentary credit monitoring depends on the extent and nature of the compromised data as well as the risk profile of the incident. Ms. Valdetero notes that in the US there are only a few jurisdictions requiring credit monitoring, and the duration is between one and two years. Ms. Valdetero only knows of three instances where more than two years of credit monitoring was offered. As stated by Ms. Valdetero, NS Power's initial offer of two years of credit monitoring was reasonable:

According to statistics provided to NS Power from TransUnion, only six percent of companies who were victims of a cyber security incident in 2025 and utilized TransUnion for their credit card monitoring services offered five years of credit monitoring following a breach. As such, a two-year offer aligns with standard industry practice across Canada for organizations across industries (financial services, healthcare, retail, telecommunications, education, etc.) when they suffer a ransomware or other data breach involving sensitive personal information. Regardless, Ms. Ralph herself acknowledges that the extension to five years was reasonable.⁴⁰

The criticism of NS Power's initial offer of two years of credit monitoring should be viewed in the context of the absence of any legal, regulatory, or established industry standard requiring a longer period. As acknowledged by INQ, there are no legal or regulatory standards prescribing the duration of credit monitoring following a privacy breach, and historically Canadian organizations have commonly offered two years of monitoring in response to similar incidents.⁴¹ NS Power announced its initial two-year credit monitoring offering in its direct notification letter, dated May 10, 2025, consistent with prevailing industry practice at the time and indirectly in an online update

³⁹ M12600, Exhibit N-14, Evidence – Tricia Ralph INQ Law/Consulting, June 23, 2026, p 21, para 89.

⁴⁰ Attachment 1, Valdetero Evidence, p 20.

⁴¹ M12600, Exhibit N-15, INQ response to CA IR-3, July 29, 2026.

**Cybersecurity Accountability
REDACTED**

1 posted on May 14, 2025. As additional information became available and evolving expectations
2 regarding longer-term protections emerged, the Company proactively expanded the offering to
3 five years on June 25, 2025.

4
5 Importantly, there is no evidence that any affected individual was denied access to credit
6 monitoring, suffered harm as a result of the initial two-year offer, or was disadvantaged by the
7 period between the initial and enhanced offerings. Once the offering was expanded, customers
8 received the benefit of the more extensive protection.

9
10 The relevant question is therefore not whether five years is preferable in hindsight, but whether
11 the Company's initial decision to offer two years was unreasonable when made. Given the absence
12 of any legal requirement, the historical practice of offering two years of monitoring following
13 comparable breaches, and the Company's subsequent decision to increase the benefit to five years,
14 it is difficult to conclude that the initial response fell outside the range of reasonable responses
15 available at the time.

16
17 By extending coverage from two to five years, NS Power provided protection well beyond
18 prevailing industry norms and demonstrated a proactive commitment to mitigating potential harm.
19 Further, the offer of credit monitoring services is a protective measure and not an opportunity for
20 reimbursement to customers.

**Cybersecurity Accountability
REDACTED**

6.0 PIPEDA AND THE ROLE OF THE OFFICE OF THE PRIVACY COMMISSIONER

The Personal Information Protection and Electronic Documents Act (PIPEDA) is federal privacy legislation that governs how private-sector organizations collect, use, retain, disclose, safeguard, and dispose of personal information. When there is no provincial private-sector privacy legislation that has been deemed "substantially similar" to PIPEDA, the federal PIPEDA applies to the organization's collection, use, and disclosure of personal information in the course of commercial activities, and the Office of the Privacy Commissioner of Canada (OPC) is the regulator with jurisdiction.

NS Power reported the Incident to the OPC on May 1, 2025, with an update on May 14, 2025. The OPC initiated an investigation into the Incident on May 28, 2025, and the Company actively and fully cooperated with the OPC to support that investigation. On March 18, 2026, NS Power signed a Compliance Letter with the OPC (publicly available online) outlining its commitments and confirmation of the actions the Company has taken and will continue to take to further safeguard personal information since the privacy breach.⁴² NS Power has committed to confirm the deletion of customer SINs from its systems subject to legal requirements to retain such information and to implement the segregation of that data to ensure its not used for any other purpose. Further, NS Power committed to an independent third-party information security assessment with LevelBlue which will assess:

- a description of the safeguard enhancements implemented since the breach;
- an assessment of the effectiveness of Nova Scotia Power's information security safeguards to protect personal information, and to prevent, detect, and respond to potential breaches;
- an assessment of the effectiveness of Nova Scotia Power's employee training and awareness program with respect to privacy and security;

⁴² <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2026/2026-ns-power-ca/>

**Cybersecurity Accountability
REDACTED**

-
- an assessment of the effectiveness of Nova Scotia Power's processes for notifying affected individuals as soon as feasible following a breach;
 - the identification of any remaining gaps in assessed security safeguards and notification processes; and
 - recommended solutions to address those gaps.

NS Power is to inform the OPC in writing whether LevelBlue has made recommendations, which recommendations it accepted, and the reasons why any recommendations were not accepted.

NS Power raises this process, as the issue of duplication and jurisdictional overlap previously raised by the Company remains and is highlighted by the following InterGroup's recommendations:

- Recommendation 2 would require NS Power to redesign its privacy policy, retention framework, storage requirements, and destruction standards.
- Recommendation 3 would require the establishment of a recurring privacy compliance audit regime.
- Recommendation 4 would require amendments to breach communication protocols.
- Recommendation 6 would require development of new processes for locating and contacting former customers.

These items are either wholly or partially duplicative of matters already being addressed through the OPC-directed review process.

**Cybersecurity Accountability
REDACTED**

7.0 NS POWER'S ENHANCED PRIVACY GOVERNANCE PROGRAM

Beyond the circumstances of this Attack and the response to it, the Company recognizes that the privacy, cybersecurity, and related regulatory landscape is ever evolving with significant and often rapid shifts occurring in recent months. In particular, the introduction of Bill C-36, which proposes substantial reforms to Canada's private-sector privacy framework, together with the increasing adoption and proliferation of artificial intelligence and other technologies across business operations, presents an appropriate opportunity to review and strengthen the Company's privacy governance program. As part of its commitment to continuous improvement, NS Power is assessing enhancements to its privacy framework, policies, controls, and oversight mechanisms to ensure they remain effective, current, and responsive to emerging legal, technological, and operational risks.

In this regard, NS Power has implemented a number of initiatives to further advance its existing privacy program and strengthen organizational safeguards since April 25, 2025. These enhancements are intended to reinforce governance, deepen accountability, and support the consistent implementation of privacy requirements across all levels of the organization, while building on the privacy practices NS Power already has in place.

- NS Power has long maintained a Privacy Officer function which was traditionally held by a solicitor with a broad range of responsibility; however, the role is currently being enhanced and formalized as a dedicated full-time position with authority to implement changes, review, revise, and establish as necessary, privacy policies and procedures, and monitor organizational compliance. The internal reporting structure for the Privacy Officer will be determined based on seniority level of the successful candidate but is anticipated to ultimately report up to the Executive Vice President Finance and Commercial (EVP).

**Cybersecurity Accountability
REDACTED**

-
- 1 • NS Power's Corporate Secretary and Director Legal has substantial privacy expertise and
2 currently acts as Privacy Officer. The Corporate Secretary and Director Legal reports into
3 the Vice President Legal and Regulatory.
4
 - 5 • The Vice President Legal and Regulatory reports into the Executive Vice President (EVP)
6 Finance and Commercial, who reports to the Executive Leadership Team (ELT) on privacy
7 related matters. The EVP Finance and Commercial also briefs the Nova Scotia Power
8 Board of Directors on matters of privacy. The EVP Finance and Commercial will brief the
9 NS Power Board of Directors on privacy related matters as a standing agenda item on a
10 quarterly basis.
11
 - 12 • NS Power has elevated and expanded its Privacy Committee to include personnel that are
13 Director-level and above, with ability to direct business units and influence the culture to
14 ensure a top-down approach to the implementation and operationalization of policies and
15 procedures across the various business units.
16
 - 17 • NS Power has refreshed all internal privacy policies and procedures with the support of
18 third-party expert, Gartner. These refreshed and revised policies have been provided to
19 LevelBlue for review during the OPC-directed audit referenced above. That audit is to be
20 completed by the end of October 2026.
21
 - 22 • In the interim, NS Power has certified compliance with applicable privacy laws and
23 obligations tracked in Optro by the Company's internal compliance team. Optro (formerly
24 known as AuditBoard) is an AI-powered cloud platform for Governance, Risk, and
25 Compliance. It is designed to help organizations manage internal audits, SOX compliance,
26 cybersecurity risk, and regulatory frameworks in a single centralized system.
27
 - 28 • NS Power has implemented technology that identifies and continuously scans for personal
29 information including SINS in the Microsoft 365 environment. Those scans are currently

**Cybersecurity Accountability
REDACTED**

1 focusing on customer SINs. The scans produce a report that is reviewed by NS Power's
2 Privacy Officer who will then authorize deletion, unless the customer SIN is required for
3 tax reporting purposes. This scanning process will be expanded to include other personal
4 information data.
5

- 6 • Customer SINs collected and retained for tax reporting purposes will be maintained in a
7 secure SharePoint site in a password protected file. There are dedicated site owners, and
8 those site owners are the only roles with access to the site and the password protected file.
9 Access to this secure SharePoint site will be monitored and audited using DLP Monitoring
10 (Purview). Personal information data from this site will be shared with the CIS IT team in
11 order to generate and print T5s for CRA to submit securely to CRA and to mail to
12 customers so that they can claim the additional income.
13

- 14 • Regarding customer SIN collection for tax reporting on interest bearing accounts, NS
15 Power is corresponding with the Canada Revenue Agency to discuss alternatives to
16 collecting customer SINs in order to issue a T5 which record interest earned on deposit
17 accounts for tax reporting purposes.
18

- 19 • The Company is continuing to develop and implement opportunities to automate the
20 deletion or anonymization of personal information once applicable retention periods have
21 expired. This includes developing approaches for SharePoint repositories, email records,
22 and other systems that may contain personal information external to CIS. Such
23 opportunities include:
24

- 25 • Adoption of Microsoft Purview as the enterprise platform for Email Records
26 Management. Purview enables the automation of consistent classification,
27 retention, protection, and disposal of email content aligned to regulatory, legal, and
28 business requirements; and

**Cybersecurity Accountability
REDACTED**

-
- 1 • Data Loss Prevention (DLP) policies that work together with data sensitivity
2 labelling to protect sensitive and personal information from unauthorized access,
3 reduce the risk of accidental data sharing, support regulatory and privacy
4 compliance obligations, and reinforce a culture of data responsibility across the
5 organization. Employees experience notifications explaining that an action could
6 expose sensitive data with guidance on how to proceed securely, and in some cases,
7 actions like sending an email externally or sharing a document may be blocked if
8 highly sensitive information is detected.
9
 - 10 • The Company is also continuing to evaluate how future system modernization initiatives,
11 including the planned CIS replacement in 2029, will support enhanced records disposition
12 capabilities, recognizing that the removal of historic data must be balanced against
13 operational and system functionality requirements at this time.
14
 - 15 • NS Power is strengthening its Privacy Impact Assessment (PIA) program by expanding the
16 circumstances in which PIAs are mandatory. Prior to the incident, PIAs were generally
17 conducted on a project-specific basis. Going forward, a PIA will be required for any
18 initiative involving the collection, use, storage, access, disclosure, or movement of personal
19 information, including the creation of SharePoint sites, Microsoft Teams channels, and
20 other information repositories containing customer or employee information. To support
21 this enhanced governance framework, NS Power is investing in the ServiceNow Privacy
22 Module, which will automate key components of the privacy management program,
23 including PIA workflows, privacy breach reporting, policy and procedure management,
24 and program documentation. This investment is intended to improve oversight,
25 consistency, accountability, and readiness for evolving privacy regulatory requirements.
26
 - 27 • Under the enhanced process, all PIAs are reviewed by the Privacy Officer, who is
28 responsible for assessing privacy risks and identifying required mitigation
29 measures. Where cybersecurity risks are identified, the Privacy Officer works in

**Cybersecurity Accountability
REDACTED**

1 collaboration with the cybersecurity team to evaluate and address those risks. The
2 business area initiating the action/work receives documented recommendations and
3 required actions arising from the assessment and is responsible for implementing
4 the identified controls. Initiatives cannot proceed until the Privacy Officer is
5 satisfied that applicable privacy risks have been appropriately mitigated and
6 required controls have been incorporated. Compliance with mitigation measures
7 and associated action items will be tracked and monitored through Optro.

- 8
- 9 • All NS Power business leaders have completed a Business Area Inventory listing the
10 personal information each unit collects, uses, and stores including location(s). The Privacy
11 Officer collects and retains the information as part of the Privacy Program.
12
 - 13 • All employees who interact with personal information have received either role specific
14 privacy training or general privacy training that is mandatory. Initial training begins at
15 onboarding and occurs annually thereafter. This is in addition to the Company's
16 cybersecurity training and awareness program referenced above which includes mandatory
17 quarterly cybersecurity training and monthly phishing simulation testing exercises for all
18 employees.
19

20 Further, as listed at section 8.1 of the Company's Incident Report, NS Power is pursuing key
21 additional remediation and restoration efforts related to strengthening the Company's
22 cybersecurity systems.

23

24 Taken together, these measures constitute a comprehensive remediation plan developed with the
25 assistance of leading cybersecurity experts and informed by lessons learned from the incident. The
26 breadth and depth of the initiatives encompass infrastructure, identity management, access
27 controls, monitoring, threat detection, network segmentation, encryption, endpoint protection, and
28 governance enhancements.
29

**Cybersecurity Accountability
REDACTED**

8.0 CONCLUSION

Over the past 16 months, the team at NS Power has worked around the clock to restore and strengthen all systems and to support its customers. NS Power acknowledges the significant impact the Attack and consequent privacy breach had on its customers, and does not understate the disruption, frustration, and concern experienced by those whose personal information was affected and whose billing was interrupted during the Company's recovery. The Company respects the diligence that the Board and intervenors have brought to this proceeding, and for the opportunity the record has provided to examine, transparently and in detail, the reasonableness of NS Power's response.

The evidentiary record in M12600, including the forthcoming testimony of NS Power leadership, demonstrates that NS Power's response to an unprecedented and sophisticated attack was substantively guided by a commitment to transparency, customer support, and continuous improvement. The Company respectfully submits that this record, taken as a whole, does not describe a utility resistant to accountability, but one that met an extraordinary event with customer-centered measures that continued to evolve to meet the needs of customers - many of which exceeded industry norms. NS Power has been forthcoming, through its own filings and cooperation with the Board's inquiry into the areas warranting further attention and has made commitments to restoring and enhancing its systems. With that said, the Company expects that the Board's findings and any resulting directives be calibrated to that record: preserving the ordinary regulatory processes by which cost recovery, investments in the system, and service standards are properly tested, while recognizing the action plans and commitments the Company has made and remains committed to making.

NS Power reaffirms its commitment to rebuilding and maintaining the trust of the customers it serves, and to working with the Board, its customers, and all intervenors as its remediation and enhancement efforts continue.

Nova Scotia Energy Board

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

M12600

Inquiry into Nova Scotia Power Incorporated's Cybersecurity Incident

Evidence of Jena Valdetero, Co-Chair US Data
Privacy and Cybersecurity at Greenberg Traurig
LLP

Prepared for NS Power Inc.

August 10, 2026

NON-CONFIDENTIAL

Inquiry into NS Power’s Cybersecurity Incident – Evidence of Jena Valdetero
NON-CONFIDENTIAL

TABLE OF CONTENTS

1.0 Scope and Mandate 3

2.0 Qualifications 3

3.0 Information Considered 4

4.0 Summary of Opinions 5

5.0 Key Chronological Facts Identified in the Record 6

6.0 PART ONE: Rebuttal of Ralph Report (INQ) Findings..... 8

7.0 PART TWO: Rebuttal of Mollard (InterGroup) Recommendations 22

Appendix A 29

1.0 SCOPE AND MANDATE

I have been retained by Nova Scotia Power Incorporated (“NS Power” or “Company”) in connection with the recent cybersecurity incident (the “Incident”) impacting the Company to provide expert rebuttal opinion in response to certain findings and recommendations contained in the expert reports of:

- Tricia Ralph of INQ Law/Consulting (the “Ralph Report”), dated June 23, 2026, submitted as the Opinion of Board Counsel Consultant in Matter M12600; and
- Ed Mollard of InterGroup, dated June 23, 2026 (the “Mollard Report”).

2.0 QUALIFICATIONS

I am Co-Chair of Greenberg Traurig’s U.S. Data Privacy and Cybersecurity Practice. Since 2012, I have advised clients on more than a thousand data security incidents, including ransomware, extortion, business email compromise, inadvertent disclosure, and payment-card matters. My work regularly includes coordinating forensic investigations, document review, breach notification analysis, credit monitoring and identity-protection offerings, call-center and notification vendors, and regulatory response. I have also advised on international breach-notification obligations, including Canadian requirements, in coordination with Canadian counsel. My Curriculum Vitae is included as Appendix A.

Where I disagree with a finding or recommendation in the Ralph Report or Mollard Report, I explain my rationale and identify factual considerations that appear to have been overlooked or insufficiently weighted.

I note at the outset that Ms. Ralph’s mandate, as she describes it, was to opine “on the reasonableness of NSPI’s actions in delivering services to its customers relating to the privacy related issues addressed in [her] report” arising from or in relation to the Company’s response to the Incident. She expressly refers to the Personal Information Protection and Electronic Documents Act (“PIPEDA”) as the applicable legislative framework but that she expresses “no opinion on

questions of legal interpretation or statutory compliance, which fall outside [her] role.” [Ralph Report p. 5.]

I have been retained to provide an opinion as to whether NS Power acted reasonably under the circumstances. In forming my opinions, I have relied on my experience managing more than 1,000 data security incidents and advising organizations on the interpretation and application of privacy laws and regulatory expectations following cybersecurity incidents. I have reviewed PIPEDA and similar Canadian privacy legislation, am familiar with their requirements, and have advised clients regarding compliance with those requirements in numerous prior matters. The underlying privacy principles are substantially similar to those found in U.S. and international privacy laws, with which I have extensive professional experience.

3.0 INFORMATION CONSIDERED

In preparing this Report, I have considered:

- The Ralph Report (M12600, Exhibit N-14, Evidence of Tricia Ralph INQ Law/Consulting, June 23, 2026);
- The Mollard Report (M12600, Exhibit N-13, Evidence of Ed Mollard, InterGroup Consultants Ltd., June 23, 2026);
- NS Power's responses to NSEB Information Requests 1 through 12, filed September 5, 2025 in Matter M12273, including all attachment (M12600, Exhibit N-2, NSPI (NSEB) RIR 1-12, February 6, 2026);
- NS Power's customer notification letters (M12600, Exhibit N-2, NSPI (NSEB) RIR 1-12, NSEB IR-1 Attachments 1 and 2, February 6, 2026);
- NS Power's customer fact sheet and community support materials (M12600, Exhibit N-2, NSPI (NSEB) RIR 1-12, NSEB IR-1 Attachment 3, February 6, 2026);
- NS Power's website cyber incident updates through September 5, 2025 (M12600, Exhibit N-2, NSPI (NSEB) RIR 1-12, NSEB IR-1 Attachment 4, February 6, 2026);

-
- 1 • The 2025 Nova Scotia Power Cybersecurity Incident Report (the “Incident Report”) dated
 - 2 December 22, 2025, as referenced in the Ralph Report (M12600, Exhibit N-3, Incident
 - 3 Report, February 2, 2026);
 - 4 • Applicable regulatory guidance, including guidance from the Office of the Privacy
 - 5 Commissioner of Canada (“OPC”), and equivalent provincial regulators;
 - 6 • Industry standards documentation, including guidance published by the Identity Theft
 - 7 Resource Center (“ITRC”), the International Association of Privacy Professionals
 - 8 (“IAPP”), NIST Special Publication 800-61, and comparable breach response
 - 9 frameworks;
 - 10 • Publicly available breach response benchmarking data and settled regulatory decisions;
 - 11 • Information obtained from representatives of TransUnion, NS Power, Osler, and Emera.

12 **4.0 SUMMARY OF OPINIONS**

13 In my opinion, NS Power's response to the Incident should be assessed in the context of a large-
14 scale ransomware event involving extensive data exfiltration, severe operational disruption
15 experienced by the Company, forensic uncertainty common for large-scale ransomware incidents,
16 and the need for NS Power to coordinate customer support at province-wide scale. While
17 reasonable practitioners may differ on certain communications judgments, in my view the record
18 reflects an appropriate, substantial, and evolving response of NS Power to the Incident that
19 included early public notice, direct notice to current customers, indirect notice to former
20 customers, expanded credit monitoring, extensive community support, and continued direct
21 outreach as additional affected individuals were identified. In my experience over the past 14 years
22 handling more than a thousand data security incidents, the timing of the response for both direct
23 and indirect notice is in the top three percent of companies addressing similarly significant
24 incidents. I therefore disagree with the conclusions in the Ralph Report and Mollard Report that
25 the timing and content of the notice to NS Power customers, and the Company's remedial measures
26 were unreasonable.

5.0 KEY CHRONOLOGICAL FACTS IDENTIFIED IN THE RECORD

Before turning to the specific findings and recommendations in the Ralph Report and Mollard Report, I set out the key chronological facts established by the evidentiary record, as these facts are essential context for the opinions that follow:

- **April 25, 2025:** NS Power discovered the Incident when employees reported certain applications were not functional. NS Power immediately activated its incident response and business continuity protocols and engaged Osler and, through Osler, Mandiant's cybersecurity and incident response team.
- **April 27, 2025:** NS Power notified the Canadian Centre for Cybersecurity (CCCS), the RCMP, CSIS, and the FBI.
- **April 28, 2025:** NS Power informed customers on its website that it was actively responding to a cybersecurity incident.
- **May 1, 2025:** NS Power determined that customer personal information had been impacted, provided an update on its website that it had "identified that certain customer personal information was accessed and taken by an unauthorized third party and notified the OPC." NS Power also initiated the process of notifying affected individuals and retained third-party service providers to assist.
- **May 13, 2025:** NS Power sent direct notices to approximately 277,000 current customers whose personal information it could determine had been impacted and offered two years of credit monitoring and identity theft protection services through TransUnion. NS Power sent two versions of the letter: (1) a version identifying that social insurance numbers (SINs) may have been affected; (2) a version to individuals where SINs were not collected and therefore could not have been impacted by the Incident.
- **May 14, 2025:** NS Power issued a press release and provided a detailed update on its website and social media pages, receiving widespread local and national media coverage.

-
- 1 • **May 22, 2025:** NS Power became aware that the threat actor had published data on the
2 Dark Web.
 - 3 • **May 23, 2025:** NS Power posted an update on website and prior channels.
 - 4 • **May 28, 2025:** The OPC initiated a formal investigation into the Incident.
 - 5 • **June 4, 2025:** NS Power leadership appeared before the Nova Scotia Public Accounts
6 Committee, confirmed that customer data had been exfiltrated, and encouraged existing
7 customers to sign up for free credit monitoring.
 - 8 • **June 25, 2025:** Via substitute notice on its website, in the media, on social media,
9 stakeholders, paid advertising, national paid search optimization, NS Power notified the
10 public that former customer information had also been impacted. NS Power simultaneously
11 extended its credit monitoring offer from two years to five years for all current and former
12 customers. Affected customers who had already enrolled in the two-year product offer were
13 automatically extended to five years.
 - 14 • **June 30, 2025:** NS Power sent proactive notices to Cape Breton media outlets.
 - 15 • **July 3, 2025:** NS Power sent proactive notices to Springhill media outlets.
 - 16 • **July 8, 2025:** NS Power sent proactive notices to Yarmouth media outlets.
 - 17 • **July 9, 2025:** NS Power sent proactive notices to Bridgewater media outlets.
 - 18 • **July 10, 2025:** NS Power sent proactive notices to Millbrook media outlets.
 - 19 • **September 19, 2025:** NS Power posted information on its website reiterating and
20 reinforcing that all customers could sign up for free credit monitoring for five years,
21 providing a link to same, and reminding customers that the sign-up period for this credit
22 monitoring would end on September 30, 2025.
 - 23 • **October 31, 2025:** NS Power sent direct notices to approximately 97,000 additional
24 customers identified as impacted.

-
- 1 • **November 3, 2025:** NS Power again posted information on its website explaining how the
 - 2 additional customers who had now received a letter could sign up for free credit monitoring
 - 3 for five years, providing a link to additional information on signing up for this offer.
 - 4 • **December 31, 2025:** Enrollment period for TransUnion closed for all customers; however,
 - 5 NS Power continued to offer free credit monitoring upon request.

6 **6.0 PART ONE: REBUTTAL OF RALPH REPORT (INQ) FINDINGS**

7 **Finding 1: That the Timeframe for Notification to Former Customers Was Unreasonable**

8 **Summary of Ms. Ralph's Finding**

9 At paragraph 46 of the Ralph Report, Ms. Ralph concludes that the approximately two-month
10 delay between the discovery of the Incident on April 25, 2025, and the public notification to
11 former customers on June 25, 2025, was unreasonable.¹ Ms. Ralph states that NS Power “would
12 or should have been aware that it had data of former customers in its record systems and this should
13 have triggered assessment of whether former customer data was also impacted in or around the
14 same time as that of current customers.”² Ms. Ralph further states that best practice requires
15 notification within days rather than months, absent extenuating circumstances such as a police
16 investigation, and that no such extenuating circumstance was identified by NS Power.

17 **Expert Opinion**

18 I disagree with this finding. While I agree that it is important to take steps to identify whether
19 sensitive personal data was affected in an incident and act quickly to notify as soon as feasible, a
20 finding of unreasonableness is not sustained by the evidentiary record when the full factual context
21 is considered. Any assessment of reasonableness is contextual and should distinguish between the
22 timing of NS Power's determination that former customer information may have been implicated
23 and the operational feasibility of reaching that population with meaningful, accurate, and usable
24 notice. Where reliable contact information was not available, indirect notice was not a failure of

¹ Exhibit N-14, PDF pg 12/29, para 46.

² Exhibit N-14, PDF pg 12/29, para 46.

1 notice; it was a recognized notification mechanism expressly permitted by Canadian law, provided
2 it was reasonably designed to reach affected individuals.

3 **Rationale**

4 **(a) The Incident Was a Complex, Large-Scale Ransomware Event, Not a Routine Breach**

5 The record establishes that this was not a routine data breach. This was a sophisticated and
6 coordinated cyberattack in which a threat actor gained unauthorized access, exfiltrated
7 approximately 13 terabytes of data, and deployed ransomware that encrypted numerous files and
8 systems across multiple interconnected IT environments, including both on-premises and cloud
9 storage systems.

10 Ms. Ralph's statement that notification to former customers should have occurred within days is
11 not consistent with my experience handling hundreds of similarly complex matters such as this
12 one. While in principle I agree that faster is usually better, Ms. Ralph's opinion does not take into
13 consideration the level of complexity involved in this Incident. Nor does she acknowledge the risks
14 of moving too quickly and notifying hundreds of thousands of people before a victim company
15 has the resources in place to meaningfully assist concerned customers.

16 It helps to provide context for what a company experiences after identifying that it is the victim of
17 a major security incident. In general, a company must engage its internal incident response team
18 to address the most immediate issue: the threat of ongoing threat actor access and potential
19 operational disruption caused by encryption of key servers. As a public utility providing essential
20 services, NS Power's top priority should be to ensure continuity of services.

21 A victim company often engages external legal counsel experienced in cybersecurity incidents,
22 which NS Power did when it engaged the Osler firm. Osler, in turn, retained a forensic investigator,
23 Mandiant, to assist with eliminating unauthorized access and determining threat actor activity.

24 In tandem, many companies engage in discussions with the threat actor. One key reason to do so
25 is to obtain a list of documents the threat actor claims to have stolen, known as a file tree. In
26 ransomware situations where there is widescale encryption rendering servers and forensic evidence

1 unavailable, as well as operational disruption, the fastest way to identify a list of potentially stolen
2 files is to request it from the threat actor.

3 Even having such a list, as NS Power did on May 1, 2025, does not guarantee that a company is
4 aware that sensitive personal data may have been obtained by the threat actor, let alone which
5 individuals are affected and what data may have been stolen. In the course of responding to a
6 cybersecurity incident as extensive and severe as the Incident, a company can typically begin to
7 look for current contact information for those affected only after the following: restoration of the
8 affected systems, extraction of copies of documents from the file tree, engagement of a third-party
9 e-discovery service provider to review said files, and then compilation of a list of individuals
10 identified in the files. Then, the company typically must retain a vendor, like TransUnion, to assist
11 with providing credit monitoring and identity theft services, mailing notices to the affected
12 population, and establishing a call center to assist with customer inquiries about the Incident. The
13 record establishes that NS Power took these very steps, but also that it did so in the context of
14 considerable operational disruption caused by the threat actor.

15 **(b) Current Customer Notification Speed Does Not Establish What Was Feasible for**
16 **Former Customers**

17 Based on the information in the record and information obtained from individuals directly involved
18 in the Incident response, NS Power obtained a file tree from the threat actor and worked quickly
19 to review it. Despite the file tree containing the names of over 3.1 million files, NS Power quickly
20 identified a historic billing file dated July 21, 2021. NS Power's understanding of the file enabled
21 it to engage TransUnion and take steps to mail letters to current customers, which NS Power did
22 incredibly quickly to mail 277,000 letters on May 13, 2025. In my experience, it is unusual for any
23 company experiencing a ransomware event of this scale to notify affected individuals less than
24 two weeks after determining that customer personal information had been impacted. In my
25 experience, direct notice to approximately 277,000 current customers within this timeframe was
26 unusually fast for a ransomware incident of this scale, particularly where the organization was
27 simultaneously managing containment, restoration, customer support, and regulatory
28 communications.

1 NS Power was able to do so because it had valid addresses for current customers in its existing
2 customer database, which was not affected by the ransomware incident. Exporting those names
3 and addresses and providing them to TransUnion made the speed of its current customer
4 notification possible.

5 Former customer information presented a different challenge. My understanding is that NS Power
6 did not have confidence that it had current addresses for former customers. As customers of a local
7 utility often discontinue services because they relocate, this fact is not unusual and is consistent
8 with my experience advising a large U.S.-based utility company for the past five years. The
9 transient nature of NS Power's customer base is compounded by the existence of a significant
10 number of universities in Nova Scotia that are serviced by NS Power. NS Power worked with the
11 assistance of third-party experts highly experienced in responding to large scale cyber security
12 incidents to determine whether it was possible to identify current addresses for former customers,
13 ultimately determining it could not do so with any degree of confidence.

14 **(c) Former Customer Notice Required Additional Operational Readiness**

15 Tasked with notifying former customers indirectly, NS Power sought assistance from TransUnion,
16 who in turn connected NS Power with Sogica, an IT services company with extensive experience
17 in incident notifications to ensure that NS Power was prepared for thousands of people to seek
18 more information about the Incident on its website and obtain credit monitoring services. NS
19 Power worked with Sogica to develop and launch a website devoted specifically to the Incident
20 where customers could enter their name and year of birth to confirm they were a customer and
21 obtain a free credit monitoring code. When communicating with individuals about a data security
22 incident, it is incredibly important to ensure seamless and error-free communication to the extent
23 possible. Individuals often are skeptical about providing additional information to take advantage
24 of services provided by the victim company; this concern was present during the Incident response
25 because to get a TransUnion code, NS Power customers had to enter their name and year of birth.
26 It was therefore imperative that NS Power and Sogica test the website to ensure it worked properly
27 and would not lead to additional confusion.

1 At the same time, NS Power was receiving feedback from certain customers and third parties that
2 the offer of two years of credit monitoring fell below expectations (see discussion below). NS
3 Power ultimately worked closely with TransUnion to contract for a five-year product and obtain a
4 substantial number of credit monitoring codes. NS Power also arranged for TransUnion to extend
5 the two-year product offered in the May 13 letters to five years without requiring recipients to take
6 any action.

7 Once NS Power felt that it was prepared to “go live” with the website and offer five-year codes to
8 all affected individuals, it also had to coordinate how it would ensure the greatest number of people
9 would be notified of the Incident. This included posting notice on its website, in the media, on
10 social media, stakeholder communication, community outreach, paid advertising, and through
11 national paid search optimization. NS Power’s efforts were extremely effective: in a July 2025
12 consumer pulse survey, 85% of respondents reported that they were aware of the Incident.³

13 **(d) Multi-Channel Public Notice Was a Relevant Mitigating Factor**

14 Ms. Ralph acknowledges at paragraph 45 of the Ralph Report that NS Power “actively shared this
15 information with media, on social media, with stakeholders, through paid advertising, as well as
16 national paid search optimization, to reach as many current and former customers as possible.”⁴
17 This public notification activity is a relevant mitigating factor that Ms. Ralph’s analysis does not
18 fully credit in assessing the overall reasonableness of the notification program, nor does she
19 acknowledge the time it takes to become operationally ready to deploy such a robust
20 communication strategy.
21

³ Exhibit N-6, NS Power’s Response to CA IR-11, filed May 6, 2026

⁴ Exhibit N-14, PDF p 11/29.

**Finding 2: That the Timeframe for Additional Customer Notification Was Unreasonable
(Ralph Report, para 48)**

Summary of Ms. Ralph's Finding

At paragraph 48 of the Ralph Report, Ms. Ralph concludes that the delay in notifying approximately 97,000 additional customers — who were not included in the initial May 13, 2025 notification of 277,000 current customers and who received direct notices on October 31, 2025 — was unreasonable, for the same reasons articulated with respect to former customers at paragraph 46.

Expert Opinion

I disagree with this finding. The elapsed time between the May 13 notification and the October 31 notification requires contextual analysis that Ms. Ralph's approach does not fully or otherwise sufficiently provide. The October 31 direct mailing should be understood as a later, more individualized outreach step made possible by continued forensic and data analysis, not as the first point at which NS Power communicated about the Incident to potentially affected individuals. In my view, based on my experience, the timing of NS Power's additional customer notification was wholly appropriate and reasonable under the circumstances.

Rationale

Further Identification Required Continued Forensic and Data Analysis and Ms. Ralph's Analysis Does Not Fully Credit Substitute Notice and Ongoing Public Communications

As noted above, NS Power's multi-channel public communication strategy provided broad awareness of the Incident to all current and former customers from April 28, 2025. NS Power provided indirect public notice directed to former customers beginning June 25, 2025, through multiple channels. I understand that NS Power relied on indirect notice because it lacked reliable current contact information for former customers.

1 Even so, NS Power continued to conduct a data analysis of impacted files with third-party vendor
2 assistance to review terabytes of stolen data. The process of identifying the approximately 97,000
3 additional customers required continuation of the forensic analysis across multiple data systems,
4 including environments that had been subject to ransomware encryption and that required detailed
5 data recovery before the scope of their contents could be assessed.

6 NS Power retained KPMG to conduct a forensic analysis of a relevant subset data that would have
7 potentially contained customer personal information to identify any sensitive personal data that
8 may have been present in a dataset affected by the breach. KPMG also was retained to identify
9 sensitive personal data as part of NS Power's efforts to engage in a data deletion exercise for data
10 minimization purposes. Deloitte was retained to analyze an additional subset of the data that would
11 have potentially contained personal information to address the following primary objectives:
12 identify individuals (i.e., natural persons rather than businesses or organizations) who are both
13 current customers and may have had personal data within affected files, and assess, for each
14 individual, the extent of PII exposure (i.e., what information was potentially exposed for each
15 individual). This effort was undertaken to identify any current customers in this dataset who may
16 not have been notified directly in the initial notification effort. The result of these efforts was to
17 identify and mail 97,000 letters to additional confirmed affected individuals.

18 Ms. Ralph's opinion ignores the reality of the efforts required to identify with any degree of
19 confidence personal data contained in such a large data set. She also does not credit NS Power for
20 having previously notified former customers via substitute notice months earlier or the extent to
21 which the ongoing public communications program provided additional constructive awareness of
22 the Incident and the availability of credit monitoring during the period prior to direct notification.
23

Finding 3: That the Contents of the Customer Notices Were Insufficient, Unclear, and Therefore Unreasonable

Summary of Ms. Ralph's Finding

At paragraph 57 of the Ralph Report, Ms. Ralph concludes that the contents of NS Power's customer notices were insufficient and unclear and therefore unreasonable.⁵ Ms. Ralph's primary criticism is that the notices did not provide customers with specific information about which of their data elements were affected; she suggests customers should have been told to assume all of their data elements were impacted. Ms. Ralph also references customer complaints about lack of guidance on whether to replace SINs or open new bank accounts, difficulties with the credit monitoring activation process, and the experience of being directed to TransUnion when calling the dedicated number.

Expert Opinion

I disagree with this finding. Customers were sent two different types of notifications: those where SINs were collected and therefore could have been affected in the Incident and those whose SINs were not collected and therefore not affected. The remaining data elements identified as potentially exposed are those that either were collected of most if not all customers (e.g., contact information and date of birth) or those where a customer would reasonably be aware if they provided that information to NS Power (e.g., banking information for those enrolled in autopay). PIPEDA expressly contemplates that a notifying organization may not know every data element with customer-specific precision at the time notice is provided.⁶

In my view, the remaining contents of the letter provided clear guidance fully consistent with accepted industry standards. The use of a TransUnion call center is a common industry practice to ensure rapid response to callers, and any difficulties with credit monitoring were addressed through

⁵ Exhibit N-14, PDF p 14/29.

⁶ *Breach of Security Safeguards Regulations*, SOR/2018-64, s. 3(c), enacted under PIPEDA.

1 community outreach and the dedicated TransUnion call center. In my opinion, NS Power acted
2 reasonably and met or exceeded industry standards in its notification strategy.

3 **Rationale**

4 **Individualized Data Element Identification Was Not Reasonably Feasible on the Notification**
5 **Timeline**

6 The record establishes clearly that the absence of customer-specific data element information in
7 the notices was not a matter of organizational choice or insufficient effort — it reflected a genuine
8 forensic impossibility when viewed in the context of providing notices to affected individuals as
9 soon as possible.

10 In my experience, when an incident involves exfiltration of a substantial amount of data – here, 13
11 terabytes – and when a victim company has confirmed the presence of sensitive personal
12 information in the data set belonging to most of its customers, it is quite common and appropriate
13 for companies to take a “one size” approach when identifying affected data elements in a breach
14 notification letter. This is particularly the case when a victim company weighs issuing notifications
15 quickly against the need for precision. Given Ms. Ralph’s criticism of NS Power’s speed of issuing
16 post May 13 notifications, I find her criticism contradictory that the information about what data
17 elements were affected should have been more precise. It simply ignores the reality of how breach
18 investigations and notifications happen.

19 Notably, NS Power did provide certainty about whether a customer’s SIN could have been
20 impacted when it sent two different letter versions to customers; one to those where NS Power
21 possessed their SIN and one where NS Power did not. As a SIN is one of the most sensitive data
22 elements a Canadian resident has, this decision was highly appropriate.

23 **(a) PIPEDA Does Not Require Certainty About Every Affected Data Element**

24 PIPEDA itself does not require certainty in communicating what personal information was
25 affected in a breach. PIPEDA requires notices to affected individuals to include “a description of
26 the personal information that is the subject of the breach to the extent that the information is

known.”⁷ Thus, even the governing privacy law expressly contemplates that such information may not be known.

(b) Telling Customers to Assume All Data Was Accessed Would Have Created Its Own Risks

Ms. Ralph suggests at paragraph 55 that a more cautious approach would have been to advise customers to assume that all data points had been accessed rather than state that some or more of the elements could have been accessed. This approach carries risks. It may cause unnecessary alarm among customers whose data was not, in fact, meaningfully compromised. It could lead customers to take unnecessary and costly protective actions, and it may create an inaccurate impression of the scope of the breach. Reasonable practitioners can and do disagree about the appropriate balance between precautionary communication and accurate communication. However, NS Power's approach — advising customers of the largest scope of categories of information that may have been affected while acknowledging that the scope varied by customer — is both an accurate statement and a defensible choice, as it certainly was within the range of decisions a victim of a large-scale cyber security incident would have reasonably made in the circumstances.

(c) Customer Confusion Does Not, By Itself, Establish Inadequate Notice

In my experience advising on numerous large scale cyber security incidents, when communicating information to a large population of individuals of varying education levels and backgrounds, it is impossible to communicate without receiving at least some negative feedback. Even accepting Ms. Ralph's characterization of customer confusion with respect to certain aspects of the notices, the applicable standard is not whether the notices were perfectly drafted from the personal perspective of each individual but whether they were adequate to inform affected individuals of the nature of the Incident and the steps available to protect themselves. Customer confusion, while regrettable,

⁷ *Breach of Security Safeguards Regulations*, SOR/2018-64, s 3(c).

1 does not by itself establish that the notice was inadequate — particularly where, as here, NS Power
2 deployed extensive supplemental support infrastructure to address individual inquiries.

3 **(d) NS Power Deployed Unusually Robust Supplemental Support**

4 The record establishes that NS Power deployed a comprehensive support infrastructure alongside
5 the community outreach, which materially addressed any informational limitations inherent in the
6 notices themselves and any difficulties signing up for the TransUnion offer. This infrastructure
7 included:

- 8 • A dedicated call center staffed by TransUnion employees with prepared responses, with
9 escalation protocols to NS Power customer care for complex queries;
- 10 • NS Power customer call center staff support;
- 11 • A dedicated cyber update landing page on NS Power's website providing regular updates,
12 FAQs, and guidance;
- 13 • A comprehensive fact sheet (Exhibit N-2, NSEB IR-1, Attachment 3) with step-by-step
14 credit monitoring enrollment guidance and additional protective measures;
- 15 • A paid media strategy across online, television, print, and radio platforms;
- 16 • Proactive outreach to local radio stations across the province, with contacts documented in
17 NS Power's response to Exhibit N-2, NSEB IR-1;
- 18 • Thousands of paper copies of the fact sheet distributed at NS Power depots, through
19 community sessions, and via MLAs and local councilors.

20 In addition, NS Power took the incredibly unusual step of setting up more than 30 in-person
21 community support sessions where affected customers could meet in person with NS Power
22 representatives who could assist them by answering questions about the Incident or signing up for
23 credit monitoring. In my experience responding to more than a thousand incidents, in-person

1 community support sessions of this scope are largely unheard of in breach response. I personally
2 have never seen a company make such extensive efforts to provide in-person support.

3 This multi-channel support infrastructure represents a level of customer support that substantially
4 exceeds what is typically deployed in comparable breach response programs and must be
5 considered in assessing the overall adequacy of NS Power's customer communication program.

6 **(e) Use of TransUnion for Call Center Support Was Operationally Appropriate**

7 Ms. Ralph notes at paragraph 52 of the Ralph Report that customers who called the dedicated
8 number were directed to TransUnion rather than NS Power.⁸ This design was deliberate and
9 operationally appropriate, as NS Power's Exhibit 2, NSEB IR-6 response explains. TransUnion
10 staffed the call center with experienced breach response customer service representatives to handle
11 the initial high volume of calls (which at points exceeded 1,000 calls in a day) and to facilitate
12 credit monitoring enrollment. NS Power customer care staff handled escalated queries on a call-
13 back basis. In addition, NS Power's own customer service center was equipped with FAQs to assist
14 those who opted to call the company directly. This arrangement is standard in incidents of this
15 nature and is consistent with the breach response practice of engaging specialized vendors to
16 manage high-volume customer support functions.

17 **Finding 4: That the Initial Offer of Two Years of Credit Monitoring Was Not Reasonable,**
18 **While the Subsequent Offer of Five Years Was Reasonable (Ralph Report, para 89)**

19 **Summary of Ms. Ralph's Finding**

20 At paragraph 89 of the Ralph Report, Ms. Ralph concludes that NS Power's initial offer of two
21 years of credit monitoring was insufficient because SINS, which are static identifiers that cannot
22 readily be changed, present a persistent and indefinite risk of misuse. Ms. Ralph concludes that the
23 extension to five years brought the remedial offering to a reasonable level given the nature of the
24 information compromised.⁹

⁸ Exhibit N-14, PDF p 13/29.

⁹ Exhibit N-14, PDF p 21/29.

Expert Opinion

I disagree with the conclusion that a two-year offer was not reasonable as a matter of standard breach response practice. Based on TransUnion breach-response data and my experience, five-year monitoring offers were uncommon in 2025, and offers longer than five years were rarer still. This supports treating NS Power's five-year extension as an enhancement beyond standard practice, rather than evidence that the initial two-year offer was deficient.

(a) No Canadian Rule Prescribes a Minimum Credit Monitoring Period

There is no universally prescribed minimum duration for credit monitoring offers in data breach response. I am unaware of any Canadian federal or provincial law or regulation, including under PIPEDA, prescribing a minimum credit monitoring duration. Duration is typically determined by reference to the nature of the compromised information, the applicable regulatory and jurisdictional guidance, and the temporal risk profile of the Incident.

(b) Two Years Is Consistent with Standard Breach Response Practice

In the United States, a handful of states require credit monitoring where the U.S. equivalent of SINs – Social Security Numbers (SSNs) are affected in an incident. The durations range from one year (e.g., California) to two years (e.g., Connecticut), but no state requires more than two years. In my experience, most companies offer no more than two years of credit monitoring, even where SINs or the equivalent were affected. I have only been involved in three breaches where more than two years of monitoring was offered.

According to statistics provided to NS Power from TransUnion, only six percent of companies who were victims of a cyber security incident in 2025 and utilized TransUnion for their credit card monitoring services offered five years of credit monitoring following a breach. As such, a two-year offer aligns with standard industry practice across Canada for organizations across industries (financial services, healthcare, retail, telecommunications, education, etc.) when they suffer a ransomware or other data breach involving sensitive personal information. Regardless, Ms. Ralph herself acknowledges that the extension to five years was reasonable.

(c) Five Years Was an Enhancement, Not Evidence of an Initial Deficiency

The two-year offer was not unreasonable, and the extension to five years represents an enhancement beyond the standard rather than a correction of a deficiency.

In my experience, it is not standard practice in breach responses to offer credit monitoring beyond five years, nor is it standard practice to actively explore extension options beyond five years as a matter of course during the incident response effort. The major credit monitoring service providers — including TransUnion, Equifax, Experian (in the US only), and specialized identity protection vendors — do not generally offer standardized multi-year monitoring products exceeding five years for organizational breach response engagements.

I am unaware of any regulatory settlement, consent order, or adjudicative decision — in Canada, the United States, the United Kingdom, or Australia — that has required an organization to offer or explore credit monitoring beyond five years as a condition of resolving a breach notification regulatory proceeding. I note that in response to Information Requests from the Consumer Advocate, Ms. Ralph included one instance where the privacy commissioner in Saskatchewan issued a decision on November 25, 2024, in a matter involving a data breach at Innomar Strategies Inc., recommending a credit monitoring offer of ten years. However, that incident involved substantial exposure of detailed health information, and there is no evidence that I could identify that Innomar Strategies implemented the recommendation.

(d) Credit Monitoring Is a Protective Measure, Not a Cash Reimbursement Program

NS Power has been clear that TransUnion's services were not intended to be a financial reimbursement to customers. This position is consistent with the characterization of credit monitoring as a forward-looking protective measure rather than compensation for harm. It is not standard for victim companies who are otherwise providing a market-comparable credit monitoring product to reimburse affected individuals who chose to purchase competing products.

I am not aware of a Canadian regulatory settlement or enforcement decision that has required or recommended reimbursement for independently purchased credit monitoring services as a

condition. of resolution. In my experience, reimbursement is only offered as part of a negotiated settlement in data breach class actions, for good reason. A reimbursement program requires a defined claims period, a process for receiving and reviewing claims, a mechanism for verifying invoices and confirming service eligibility, a dispute resolution mechanism, and a budget allocation process. These are not trivial requirements for a utility that is simultaneously managing a complex systems recovery. The record confirms that NS Power was, during the relevant period, focused on extensive concurrent workstreams including containment, remediation, customer billing restoration, and regulatory cooperation — contexts in which the administrative burden of a reimbursement program would be a materially significant additional obligation.

7.0 PART TWO: REBUTTAL OF MOLLARD (INTERGROUP) RECOMMENDATIONS

Recommendation 4: That the Board Direct NS Power to Update Its Communications Policy to Require a Minimum of Two to Three Direct Notifications to All Customers — and Not Only Those Potentially Affected — in the Event of Future Privacy Breaches (Exhibit N-13, Mollard Report, p. 16)

Expert Opinion

I disagree with this recommendation. It is inconsistent with accepted incident response practice in both its prescriptive notification count and in its requirement that notification be directed to all customers regardless of whether their information was involved. It is also not operationally workable as formulated and could lead to confusion as individuals may not understand if their information was exposed in one incident or in multiple incidents.

Rationale

(a) The Recommendation Conflicts with Risk-Based Notification Principles

The foundational principle of data breach notification — reflected in PIPEDA and in analogous provincial frameworks — is that notification obligations are risk-proportionate and targeted. They arise where an individual is, or may reasonably be, affected by the breach. Notifying all customers

1 — including those whose information was not involved — is not required by any US or other
2 regulatory framework or guidance document of which I am aware and serves no meaningful
3 privacy protection purpose.

4 **(b) A Fixed Minimum Number of Notices Is Not Standard Practice**

5 I am aware of no incident response framework or guidance — including those published by NIST,
6 the IAPP, and Canadian privacy regulators — that sets a minimum notification count. In my
7 experience, no company sends multiple notices about a single incident to the same individuals
8 absent unusual circumstances, like the identification of additional personal data elements
9 subsequently identified about a person who was previously sent a notice. Sending multiple direct
10 notifications to affected individuals advising of the same breach would only increase breach
11 fatigue, leading recipients to be less likely to take action in response to being notified of an
12 incident. At the same time, it could lead to confusion and anxiety, as individuals may be unsure if
13 they are being told multiple times about the same incident or whether their information has been
14 breached in multiple incidents.

15 To the extent there is a concern by Mr. Mollard that individuals may not receive or read one letter
16 in the mail, this risk was mitigated by the extensive public communications program deployed
17 from April 28, 2025 onward, encompassing website updates, social media, press releases, paid
18 media across television, radio, print, and digital platforms, proactive media outreach to
19 approximately 140 media contacts across the province, direct notifications to 277,000 current
20 customers and subsequently to former customers and an additional 97,000 customers, more than
21 30 in-person community support sessions, and a dedicated call center. These efforts resulted in
22 85% of Nova Scotians expressing awareness of the incident as early as July 2025. This was, by
23 any reasonable measure, a multi-channel and multi-notification response designed to ensure
24 awareness without creating confusion or uncertainty.

25 **(c) Over-Notification May Cause Confusion and Unnecessary Alarm**

26 Sending notices to customers to tell them they have not been affected by an incident sharply
27 departs from industry practice. In my experience, where an organization has determined that an

1 individual's information was not involved, there is generally no reason or expectation to send a
2 separate communication confirming that negative determination.

3 **Recommendation 6: That the Board Direct NS Power to Review Options to Reach Former**
4 **Customers Who May Have Relocated Outside the Province (Exhibit N-13, p. 17)**

5 **Expert Opinion**

6 I disagree with this recommendation. NS Power did, in fact, review options to reach former
7 customers. I further disagree with the recommendation to the extent that it requires NS Power to
8 take steps that are simply not feasible.

9 **Rationale**

10 **(a) The Record Shows NS Power Took Meaningful, Effective Steps to Reach Former**
11 **Customers**

12 The obligation to make reasonable efforts to notify affected individuals applies to former
13 customers as well as current ones. The record confirms that NS Power recognized this challenge
14 and took meaningful steps to address it: NS Power's June 25, 2025 public notification specifically
15 addressed former customers, was distributed through media, social media, paid advertising, and
16 national paid search optimization, and included an invitation to former customers to use a
17 Customer Verification Form to obtain a unique credit monitoring activation code. These efforts
18 demonstrate genuine engagement with the challenge of reaching customers across diverse
19 geographies and demographics, including potentially those who had relocated outside the
20 province.

21 **(b) The Board Should Recognize Practical Limits on Locating Relocated Former**
22 **Customers**

23 There are inherent practical limits on what can reasonably be achieved in reaching former
24 customers who have relocated outside Nova Scotia. NS Power has no access to real-time national
25 address databases. My understanding is that Canada does not have a readily maintained database

1 that can be easily used to search for an individual's current address in the manner suggested by
2 Mr. Mollard.

3 While Canada Post does maintain a National Change of Address ("NCOA") database, this database
4 is subject to certain limitations that lead to it not being a feasible option for the purposes of
5 notification on a large scale to NS Power's former customers, due to its unreliability for a number
6 of factors. Based on information provided by TransUnion and the record materials I reviewed,
7 Canada Post's NCOA data would not have provided a reliable large-scale solution for locating
8 former NS Power customers. The limitations included the limited lookback period (six years from
9 2025, i.e., only reflecting address changes going back to 2019), the fact that NCOA depends on
10 consumers proactively filing mail-forwarding or address-change information, and the likelihood
11 that certain former customers, including students or temporary residents, may not have filed such
12 updates. Given the scale of former customer records and the nature of the data – the likelihood of
13 receiving incorrect results (i.e., out of date addresses), would have been too high on the scale of
14 the data to render this a practicably feasible option or otherwise followed in standard practice.

15 I understand that TransUnion offers a service in Canada that permits certain of its customers to
16 validate the accuracy of an individual's address by viewing that individual's credit profile. Any
17 such lookup, however, would result in a "soft hit" being recorded on the individual's credit profile,
18 meaning that NS Power's name would appear on the individual's credit report as having accessed
19 it. In addition, this service is only available to customers who have completed TransUnion's
20 onboarding and credentialing process to securely receive, handle, and protect consumer data
21 obtained from TransUnion. For new customers, the onboarding and credentialing process can take
22 several months to complete. Given the time-sensitive nature of the notifications, this timeline did
23 not align with the immediate need for address validation and enhancement services. As a result,
24 this solution was not considered a viable option for NS Power, as it would not have provided the
25 necessary support within the required implementation timeframe.

26 However, even if this look up service was available to NS Power (which it was not), the practical
27 consequence is that individuals see NS Power's name appear on their credit file, with no
28 accompanying explanation of why. That is precisely the kind of signal that generates inbound

1 complaints and inquiries from affected individuals and would compound — rather than mitigate
2 — the confusion and concern arising from the incident itself.

3 Any direction the Board issues on this point should acknowledge these structural constraints and
4 frame the obligation as one of reasonable and documented effort rather than comprehensive reach.

5 A requirement to actually achieve comprehensive reach to all relocated former customers would
6 not be operationally workable and should not be the standard against which NS Power's efforts is
7 assessed.

8 I understand that the type of paid SIN-based address lookup sometimes available in the United
9 States is not available in Canada for this purpose, and I would not regard such a method as a
10 standard or appropriate breach-notification practice in Canada absent specific legal authority and
11 privacy review.

12 **Recommendation 8: That the Board Direct NS Power to Offer Cost Reimbursement, Up to**
13 **the Value of the Service Offered by NS Power, to Customers Who Already Had Subscriptions**
14 **in Place or Who Elect an Alternative Accredited Monitoring Service, Upon Provision of an**
15 **Invoice (Exhibit N-13, p. 19)**

16 **Expert Opinion**

17 I disagree with this recommendation as a matter of established breach response practice and have
18 significant reservations about its operational workability. As discussed above, reimbursement for
19 independently purchased credit monitoring is not an established requirement in Canadian
20 regulatory breach response proceedings or elsewhere, and I have not seen this done other than as
21 part of a negotiated class action settlement.

22 **(a) Mr. Mollard Does Not Challenge the Adequacy of the TransUnion Product**

23 Importantly, Mr. Mollard does not offer criticism of the product offered by NS Power through
24 TransUnion, essentially conceding that it is a reasonable offer by a recognized company. His
25 criticism appears to be focused on the failure to offer customers the chance to choose their own

1 monitoring “accredited” service in lieu of signing up for the free services offered through
2 TransUnion.

3 **(b) The Recommendation Fails to Define an “Accredited” Monitoring Service**

4 There is no recognized accreditation body for credit monitoring services in Canada. If NS Power
5 were required to reimburse customers for alternative services, it would need to establish a process
6 for determining which services qualify, which would be contentious, resource-intensive, and
7 subject to dispute in individual cases.

8 **(c) Customer-Selected Alternatives Would Create Unnecessary and Uncertain Costs**

9 The value of the TransUnion myTrueIdentity service offered through NS Power’s mass-enrollment
10 breach response engagement may differ from the retail market price of equivalent services.
11 Customers who elect premium alternative services may incur costs exceeding any reasonable cap,
12 and the recommendation does not address how partial reimbursement would be calculated or how
13 disputes would be resolved. The five-year myTrueIdentity service includes daily credit report
14 access, credit score monitoring, dark web monitoring, identity restoration support, and up to
15 \$1,000,000 in expense reimbursement insurance — a comprehensive package whose commercial
16 equivalent value may not be straightforward to establish.

17 **(d) Administering a Reimbursement Program Would Create Significant Operational**
18 **Burdens**

19 A reimbursement program requires a defined claims period, a claims administration process,
20 invoice verification, dispute resolution, and budget management. These are not trivial
21 requirements for a utility that was simultaneously managing a major systems recovery program
22 involving the rebuilding of core business applications across finance, human resources,
23 procurement, and customer billing systems.

(e) Reimbursement Would Recast Credit Monitoring as Compensation Rather Than Protection

The equity argument for reimbursement assumes that the credit monitoring offer is a form of compensation for harm rather than a forward-looking protective measure. Reframing the offer as compensation may have unintended legal and regulatory implications and may set a precedent that encourages customers to forgo the offered service in favor of claiming reimbursement, which would reduce the overall protective benefit achieved by the program. To the extent customers already had purchased credit monitoring services before the Incident, those costs clearly had been incurred regardless of the Incident. Permitting reimbursement is not standard in the industry, as discussed above.

Recommendation 9: That the Board Direct NS Power to Examine Longer-Term Credit Monitoring Options and Provide a Report on Those Options to the Board (Exhibit N-13, p. 19)

Expert Opinion

I disagree with this recommendation and note significant limitations on what such an examination can be expected to yield, and I caution against the recommendation being interpreted as a finding that NS Power's existing five-year offer is inadequate.

(a) The Five-Year Offer Was Already Beyond Standard Practice

The record establishes that NS Power's five-year offer was itself a voluntary extension beyond the two-year industry standard. Any direction to examine longer-term options should be accompanied by a clear Board statement that NS Power's current five-year offer is not itself found to be inadequate, and that the examination is a forward-looking governance measure rather than a finding of deficiency. As noted above, TransUnion's breach response data confirms that in 2025 only six percent of Canadian companies offered even five years of credit monitoring. Only three percent of companies offered more than five years. For example, the Government of Nova Scotia

1 offered five years to individuals whose personal information was impacted by the breach of
2 Progress Software's MOVEit platform.

3 **(b) Affected Individuals Retain Access to Credit Information After the Monitoring**
4 **Period**

5 NS Power's response to Exhibit N-2, NSEB IR-4 notes that "beyond five years, customers will
6 also continue to have free access to their own credit information directly through TransUnion
7 and/or other providers." This is a relevant consideration in assessing whether a longer monitoring
8 period is necessary, as it confirms that affected individuals retain meaningful tools for self-
9 protection beyond the expiry of the monitoring subscription.

10

**Inquiry into NS Power's Cybersecurity Incident – Evidence of Jena Valdetero
NON-CONFIDENTIAL**

Appendix A

Curriculum Vitae

I serve as Co-Chair of the firm's U.S. Data Privacy and Cybersecurity Practice at Greenberg Traurig, LLP, where I reside in the Chicago office. I graduated from Georgetown University Law Center with a juris doctor (law degree), cum laude, in 2005. I have continuously practiced law in the United States for the past 21 years. I began advising clients on data security incidents in 2012.

Since 2012, I have had a high-volume practice advising hundreds of clients on more than a thousand data breach investigations, including a significant number of ransomware and/or extortion attacks. My role includes leading an incident investigation, retaining vendors like the ones NS Power retained here: forensic investigators, document review vendors, and notification services. I advise on obligations under various data breach notification laws, including U.S. state and federal breach notification laws. Many of the matters I have handled require analysis of international breach notification laws, including Canadian laws like PIPEDA and similar provincial laws. In those matters, I frequently engage with a local Canadian law firm, but I am familiar with the notification obligations and standards of Canadian data privacy and security laws. I regularly publish articles and speak publicly about data security issues.

My concentrations include:

- Assessing cyber security risks and advising on cybersecurity programs
- Leading investigations into data security incidents
- Defending companies in privacy and security class action litigation
- Drafting policies, procedures, and training materials related to data privacy and security compliance
- Analyzing privacy and security liabilities and risks of target companies in mergers and acquisitions
- Conducting bespoke executive leadership data breach tabletops
- Advised clients on more than a thousand data breaches, including those caused by ransomware, business email compromises, inadvertent disclosure of personal data, and PCI breaches.
- Represented clients in regulatory investigations related to data security and privacy issues.

Inquiry into NS Power's Cybersecurity Incident – Evidence of Jena Valdetero

NON-CONFIDENTIAL

-
- 1 • Assisted hundreds of clients with becoming “data breach ready,” including reviewing cyber
 - 2 insurance policies, drafting incident response plans and written information security
 - 3 policies and procedures, and leading tabletop exercises.
 - 4 • Prepared clients with operationalizing requirements imposed by emerging data privacy
 - 5 laws, including the GDPR and CCPA, including development of policies, procedures, and
 - 6 training materials, and conducting data inventories.
 - 7 • Evaluated risks associated with data privacy and security issues in M&A transactions.
 - 8 • Represented clients in litigation before multiple state Supreme Courts and state and federal
 - 9 appellate courts, including in data privacy and security litigation, and obtaining rulings in
 - 10 high risk litigation, including dozens of class actions, often obtaining dismissal via motion
 - 11 to dismiss.

12 **Awards & Accolades**

- 13 • Listed, *Crain's Chicago Business*, “Notable Women in Law,” 2026
- 14 • Listed, *Chambers Global*, Privacy & Data Security: Cybersecurity, 2026
- 15 • Listed, *Chambers USA Guide*, Privacy & Data Security: Cybersecurity, 2025-2026
- 16 • Listed, *The Legal 500 United States*, Media, Technology and Telecoms Cyber law
- 17 (including data privacy and data protection), 2024-2026
- 18 • Listed, *Lawdragon*, “500 Global Leaders in Crisis Management,” 2025-2026
- 19 • Selected, *Delinian Legal Media Group*, “2024 Privacy & Data Protection Lawyer of the
- 20 Year,” 2024
- 21 • Listed, *Leading Lawyers*, 2024, 2026
- 22 • Shortlisted, *Euromoney*, Americas Women in Business Law Awards, “Best in Privacy &
- 23 Data Protection,” 2023-2024
- 24 • Named, Client Service All Star, *BTI Client Service All-Stars Report*, 2022
- 25 • Listed, *Thomson Reuters*, “Stand-Out Lawyers,” 2023-2025
- 26 • Listed, *Super Lawyers* magazine, *Illinois Super Lawyers*, 2023-2026
- 27 • “Rising Stars,” 2013-2020
- 28 • Listed, *Cybersecurity Docket* “Incident Response 40,” 2021

29 **Professional & Community Involvement**

- 30 • Founding Board Member, Chicago Compassion Project
- 31 • Member, Women in Law Empowerment Forum (WILEF), 2015-Present
- 32 • Co-Chair, Chicago Chapter, 2017-2020

- 1 • Member, Global Advisory Board, 2019-2020
- 2 • Member, International Association of Privacy Professionals, 2013-Present
- 3 • Co-Chair, KnowledgeNet (Chicago), 2015-2017

4 **Education**

- 5 • J.D., *cum laude*, Georgetown University Law Center, 2005
- 6 • B.A., *summa cum laude*, The George Washington University, 2001

**Cybersecurity Accountability Rebuttal
Attachment 2 - Retention Disposition Schedule
has been filed electronically.**

**Cybersecurity Accountability Rebuttal Confidential
Attachment 3 - Personal Information Inventory has
been removed due to confidentiality.**

**Cybersecurity Accountability Rebuttal Confidential
Attachment 4 - NSP Data Lake Information
Protection Audit Report has been removed due to
confidentiality.**