Request IR-1:

Please provide a timeline of this cybersecurity incident, including:

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

Response IR-1:

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

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

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

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

Under the direction of Osler, Mandiant assisted the Company and other cybersecurity experts with containment, investigation, and remediation efforts, and took immediate actions to contain and remediate the unauthorized activity, [redacted] Teams within NS Power also began working diligently with cyber security experts [redacted] The Company has no evidence the threat actor accessed any operational technology and energy delivery systems.

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

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

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

The OPC initiated an investigation into the Incident on May 28, 2025, and the Company is actively and fully cooperating with the OPC to support the OPC's investigative efforts. The Company has also provided updates to the Nova Scotia Energy Board, as well as other relevant government officials throughout the Incident and investigation.

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

Transparency and Steps Taken to Reduce Risk of Harm

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

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

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

The Company also employed a multi-platform advertising strategy that includes online media, as well as TV, print and radio to reach a wide variety of customer demographics. In addition, NS Power activated a paid search strategy throughout the Incident to ensure that the NS Power website and information appeared as the top search result when customers used search engines (i.e. Google) to find information about the Incident. Social media accounts have been regularly monitored, and where appropriate, the Company has provided answers to related customer questions online. The Customer Care Centre remained fully operational and available during the Incident and customers were also able to speak directly with NS Power customer care representatives on the phone for any questions or concerns.

Customer Notification Timeline

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

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

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

The following morning (May 14, 2025), the Company also issued a press release, and provided a detailed update on its website and social media pages, all of which received widespread coverage in the local and national media. Senior Company personnel participated in multiple media interviews to ensure that the public remained informed about the Incident.

The process to identify what data was impacted has been extremely complex and remains ongoing. As set out in the notices sent to impacted customers, the impacted data would have varied by customer, and depended, in part, on the information a customer would have

provided NS Power (i.e. not all personal information elements would have been impacted for all notified customers).

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

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

The credit monitoring service offered to customers is provided by TransUnion and 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 the individual's 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 an individual's 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.

- 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.

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

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.

Former Customers

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

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

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.

Customer Support and Dedicated Call Centres

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

As is standard in incidents of this nature, to ensure that the call centre had sufficient capacity to handle the volume of calls and allow NS Power’s customer service team to focus on a subset of escalated queries, this call centre was staffed by TransUnion employees who had been provided with prepared responses from NS Power, and instructed to escalate any queries that could not be addressed to the Company so that customers could

receive a call-back from the NS Power customer service team. This also allowed customers to connect directly with TransUnion for assistance in signing up for credit monitoring (and a dedicated phone line for questions about the credit monitoring process was included with the instructions provided to customers in their letter).

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

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

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

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

In addition, the Company deployed dozens of employees to communities across the province to provide hands-on support for customers who prefer assistance in person, recognizing that not all customers may be comfortable registering online, and to ensure that customer needs are being met and access to services being granted. More than 30 of

these community sessions have been held to date, and have assisted hundreds of customers in signing up for the service. The NS Power website also has been updated with additional tips and tools to help customers navigate support services.

Existing Safeguards

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

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

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

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

Incident Response and Remediation:

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

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

[redacted]

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

To coordinate work streams on business restoration and information security strengthening efforts, a business restoration process office has been established within NS Power. Restoration efforts are continuing, [redacted]

[redacted]

[redacted]

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

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

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

- Monday, April 28, 2025
- Thursday, May 1, 2025
- Wednesday, May 14, 2025
- Friday, May 23, 2025
- Wednesday, June 4, 2025
- Wednesday, June 25, 2025

Customers can access these public/media updates via a banner on the NS Power homepage labeled "Cyber Incident Updates", which directs viewers to a dedicated subpage where the updates are listed in chronological order. Please refer to Attachment 4.

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

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

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

Cape Breton – Monday, June 30, 2025

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

Springhill, Cumberland County – Thursday, July 3, 2025

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

Yarmouth - Tuesday, July 8

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

Bridgewater – Wednesday, July 9

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

Millbrook – Thursday, July 10

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

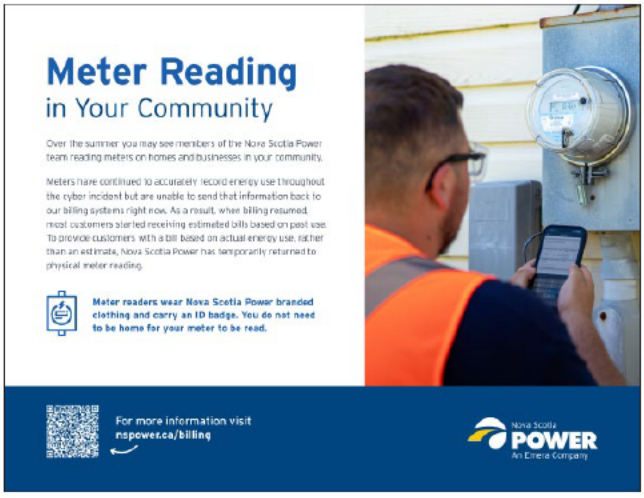
From July 8-11, 2025, NS Power responded to several media inquiries about customer bills and meter readers being hired to manually read meters at homes and businesses across the province. This media response included NS Power's Director of Customer Care, Chris Lanteigne participating in interviews with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

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

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

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

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



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

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

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

Nova Scotia POWER
An Emera Company

PO Box 910 Halifax,
Nova Scotia B3J 2W5

00766-ADFSON L001 AUTO *000001

MT2SAS001
000001

[redacted]

Re: Important Notice About Your Personal Information

Dear Valued Customer:

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

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

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

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

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

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

00766-ADFSON-187641-L001 AUTO_000001-000001-000-1/2

MT1SEAS001

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

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

Sincerely,

Peter Gregg

President & CEO

Nova Scotia Power

Services Description

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

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

https://www.mytrueidentity.ca

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

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

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

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

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

00766-ADPSGN-187641-L001 AUTO_000001-000003-000-2/2

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

MT2SSASB01

Additional Guidance

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

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

Obtain a Copy of Your Credit Report

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

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

Place a Fraud Alert on Your Credit Report

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

Nova Scotia POWER
An Emera Company

PO Box 910 Halifax,
Nova Scotia B3J 2W5

May 10, 2025

00766-ADFSON L001 AUTO *000002

[redacted]

Re: Important Notice About Your Personal Information

Dear Valued Customer:

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

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

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

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

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

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

00766-ADFSON-187641-L001 AUTO_000002-000005-000-1/2

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

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

Sincerely,

Peter Gregg

President & CEO

Nova Scotia Power

Services Description

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

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

https://www.mytrueidentity.ca

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

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

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

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

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

00766-ADPSGN-187641-L001 AUTO_000002-000007-000-2/2

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

MT25SA5001

Additional Guidance

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

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

Obtain a Copy of Your Credit Report

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

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

Place a Fraud Alert on Your Credit Report

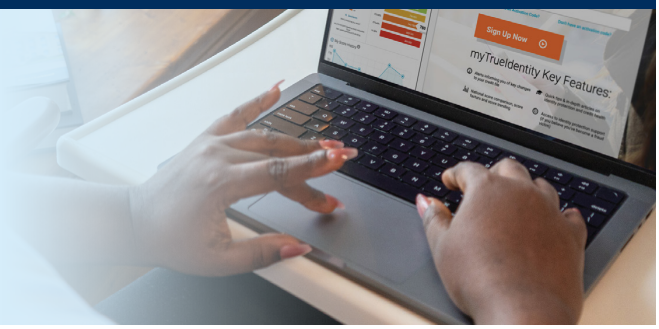
You can also place a fraud alert on your credit report. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact TransUnion Canada and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

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

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

Signing up for TransUnion's Credit Monitoring, myTrueIdentity®

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



What you need to know

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

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

Examples of security questions:

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

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

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

What is the dark web?

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

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

Nova Scotia POWER
An Emera Company

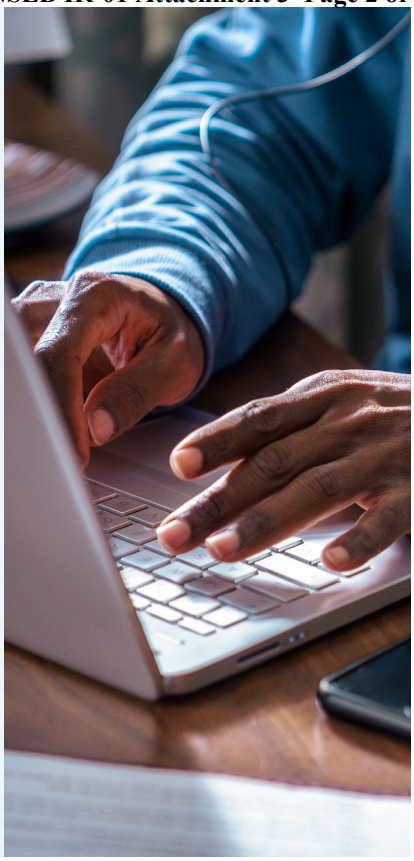
Further Protection

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

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

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

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



We're Here to Help

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

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

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

Find a location
nearest you
nspower.ca/cyberhelp

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

For more information,
please visit **nspower.ca/cyber**

Nova Scotia POWER
An Emera Company

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

CYBER INCIDENT UPDATES

NEWS

July 8, 2025

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

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

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

Learn more about our adjusted billing process **here >**

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

Wednesday, June 25, 2025 Update

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Wednesday, June 4, 2025 Update

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

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

Opening remarks by Peter Gregg, President & CEO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Thank you. We look forward to the discussion.

Peter Gregg, President & CEO, Nova Scotia Power

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

Friday, May 23, 2025 Update

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

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

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

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

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

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

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

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

Wednesday, May 14, 2025 Update

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

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

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

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

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

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

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

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

Thursday, May 1, 2025 Update

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

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

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

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

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

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

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

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

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

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

Monday, April 28, 2025 Update

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

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

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

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

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

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

LATEST UPDATES

July 8, 2025

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

Wednesday, June 25, 2025

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

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

Wednesday, June 5, 2025

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

Friday, May 23, 2025

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

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

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

Wednesday, May 14, 2025

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

Thursday, May 1, 2025

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

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

Monday, April 28, 2025

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

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

FAQS

What happened?

Last updated: Tuesday, June 24, 2025

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

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

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

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

Last updated: Tuesday, June 24, 2025

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

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

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

Was customer information or confidential business information accessed?

Last updated: Tuesday, June 24, 2025

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

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

Was my data impacted?

Last updated: Wednesday, June 25, 2025

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

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

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

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

Last updated: Wednesday, June 25, 2025

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

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

Last updated: Wednesday, June 25, 2025

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

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

Last updated: Wednesday, June 25, 2025

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

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

Last updated: Wednesday, June 25, 2025

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

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

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

Last updated: Wednesday, June 25, 2025

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

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

Last updated: Wednesday, June 25, 2025

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

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

What services have been affected?

Last updated: Tuesday, June 24, 2025

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

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

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

Request IR-2:

NS Power's Thursday, May 1, 2025, cybersecurity update letter stated:
While our investigation is ongoing, we have identified that certain customer personal information was accessed and taken by an unauthorized third party.

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

[Cyber| Nova Scotia Power: Thursday, May 1, 2025 Update]

(a) Please confirm the number of NS Power customers that are affected by this cybersecurity incident.

(b) Has this cybersecurity breach impacted former customers of NS Power?

(i) If yes, please provide the number of former customers impacted, along with the percentage of these who have not been NS Power customers for more than 2 years, 5 years, 10 years, 15 years, 20 years.

(ii) If not, please explain.

(c) Please confirm whether the number of former customers impacted is included in the numbers provided by the utility in subsections a) – c) of this Information Request.

Response IR-2

(a) The Company has been actively investigating the cyber attack with the assistance of leading third-party data analysis experts to determine the precise number of impacted customers. This investigation is ongoing and has been complex given the severe nature of

the cyber attack. It remains possible that all of the Company's customers may have been impacted by the cyber attack. On June 25, 2025, the Company offered five years of free credit monitoring to all customers of Nova Scotia Power—past and present. (See IR-01, Attachment 4). On May 1, 2025, NS Power determined that the personal information of approximately 277,000 current active customers had been impacted, and sent letters about the incident to those customers. The Company will send letters about the incident to other active customers it identifies as being impacted.

(b) Given the impact of the Incident on the Company's systems, the information available to the Company is limited. Due to the nature of the impacted records, it will not be possible to determine with certainty when these individuals ceased to be customers of NS Power.

(c) Please refer to IR-2(a).

Request IR-3:

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

> **Beginning today, we will be offering five years of free credit monitoring to all customers of Nova Scotia Power—past and present—regardless of whether you received a letter from us about the incident. Customers will not pay for any costs incurred by Nova Scotia Power for credit monitoring resulting from this incident**
>
> **[Cyber| Nova Scotia Power: Wednesday, May 14, 2025 Update]**

(a) How did the utility determine that there was no evidence of misuse of personal information for all the customers?

(b) When did the utility start sending out the notice letters?

(c) How can the utility ensure that all impacted customers or former customers have received the notice letters or any form of communication?

(d) If applicable, please explain the delay between identifying the data breach and sending out the notices.

(e) Did different customers receive different notice letters?

- **(i) If yes, how many different letters were sent out, and provide samples of each different version sent out to customers.**
- **(ii) How did the utility determine which letter customers would receive?**

(f) Why did the utility select TransUnion myTrueIdentity® services?

- **(i) Please list the components of this service and provide comment of their appropriateness.**
- **(ii) What is the cost of two-year and five-year service to the utility?**

(g) How did the utility determine that two years of credit monitoring was sufficient?

(h) Please provide the reasons for changing the credit monitoring period from two to five years.

(i) During the five-year credit monitoring period, if there is unauthorized activity, how is the customer protected? Please explain.

(j) After the five-year credit monitoring expires, how can the utility determine that this breach will not lead to unauthorized activity beyond that period?

Response IR-3

[redacted]

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

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

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

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

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

As the company continued its investigation of the impacted data, NS Power determined that personal information relating to former customers had also been impacted by the Incident. On June 25, 2025, NS Power notified the public that information of former customers had also been impacted in the Incident.

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

With respect to direct notifications, the Company sent two versions of letters to impacted current customers, samples of which are attached as Attachments 1 and 2 to IR-1. The notices are identical, except that one of the notices indicates that based on the investigation, the customer's social insurance number may have been impacted in the incident.

(f) TransUnion's myTrueIdentity® service offering is a highly regarded credit monitoring and identity protection service, and TransUnion has extensive experience providing customer

notification and call centre services to companies which have been the victim of security incidents The credit monitoring service offered to customers is provided by TransUnion and 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 the individual's 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 an individual's 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.

- 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.

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

[redacted]

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

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

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

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

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

- Unlimited online access to their TransUnion CreditVision® Risk credit score, updated daily.

- Credit monitoring, which provides individuals with email notifications to key changes on an individual's 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.

- 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.

Request IR-4:

(a) Please provide the utility's comments to complaints received by the Board and filed as Letters of Comment that request at least 10 years of credit monitoring Identity theft.

(b) Please provide the utility's comments to complaints received by the Board and filed as Letters of Comment that state, "many Canadians already receive similar coverage at no cost through their banks or credit card providers".

Response IR-4:

(a) As noted above, NS Power extended the offer of credit monitoring by three additional years beyond the two-year industry standard, providing additional protection for delayed impacts of the breach and made the credit monitoring available to all current and former customers. Throughout this timeframe, current and former customers who subscribe to the service will benefit from tools such as daily credit report and credit score updates, credit monitoring alerts, dark web monitoring and access to identity restoration support.

Beyond five years, customers will also continue to have free access to their own credit information directly through TransUnion and/or other providers, and we encourage customers to monitor their credit information regularly.

(b) NS Power is not able to comment on the similarity and availability of coverage customers might receive through their individual banks or credit card providers. NS Power chose to offer five years of free credit monitoring services through myTrueIdentity to ensure all customers, regardless of their existing coverage, can receive a consistent and comprehensive solution.

Request IR-5:

Please provide the utility's comments to complaints received by the Board and filed as Letters of Comment that request a credit equal to the cost of the two-year credit monitoring service if a customer chooses not to take the credit monitoring service

Response IR-5:

These services were not intended to be a financial reimbursement to customers, and so no equivalent monetary credit was offered. As stated in the June 25 release, the cost of credit monitoring service will not be paid by customers regardless of whether they subscribe to the credit monitoring service or not.

Request IR-6:

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

> **The types of impacted personal information varied by individual customer and depended, in part, on the information provided by each customer. This may have included one or more of the following: name, phone number, email address, mailing and service addresses, Nova Scotia Power program participation information, date of birth, and customer account history (such as power consumption, service requests, customer payment, billing, and credit history, and customer correspondence), driver's license number, and Social Insurance Number. For some of our customers, bank account numbers (for pre-authorized payment) may also have been impacted, if this information was provided by these customers.**
>
> **[Cyber| Nova Scotia Power: Wednesday, May 14, 2025 Update]**

(a) If a customer requests it, could the utility provide details about the compromised information relating specifically to that customer?

(i) If yes, please explain the process.

(ii) If not, please explain.

(b) Please specifically explain why the utility could not send a letter to the customer, detailing exactly what personnel information of that customer was compromised.

(c) The letter noted a dedicated phone number for customers with questions. Please provide the current wait times, drop-off times, the number of dedicated personnel supporting it, and whether a callback option is available to a customer.

(d) Complaints received by the Board and filed as Letters of Comment have noted that the dedicated number (1-844-818-0376) connects users to TransUnion instead of NS Power representatives:

(i) Please confirm whether the dedicated number belongs to NS Power's support team or TransUnion.

(ii) If TransUnion, please explain why it is operated by a third-party and comment on its appropriateness.

Response IR-6:

(a) The Company's investigations remain ongoing. At this time, it is not possible to determine precisely what specific personal customer information, if any, was affected by this incident. Due to the nature of the breach and the complexity of the systems involved, and despite the Company's comprehensive investigative efforts, the data accessed or exfiltrated cannot be definitively identified on an individual basis.

(b) Please refer to IR-6 (a) above.

(c) The phone number stated in the letter belongs to TransUnion, which provides the myTrueIdentity service. Current call volumes are minimal (between 1-10 customers a day), and the number of support staff is adjusted as needed to ensure efficient service. A callback option is available, allowing consumers to avoid long wait times and receive support at a time more convenient for them.

(d) NS Power established a dedicated call centre for the Incident where individuals may receive more information about the Incident, and support for credit monitoring sign-ups, whose number was included in the notice letters, and made available to customers.

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

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

Request IR-7:

NS Power's Thursday, May 23, 2025, cybersecurity update letter stated:

> **Notifications have been mailed to impacted account holders, which include detailed information about resources and support.**
>
> **[Cyber| Nova Scotia Power: Wednesday, May 23, 2025 Update]**

(a) Please list all the resources and support provided to an impacted account.

(b) Did the utility provide any guidance on steps customers could take to protect themselves from potential identity theft or fraud resulting from this breach?

(i) If yes, please share.

(ii) If not, why not.

Response IR-7:

(a) Resources and support include the following:

Customer Support

Please refer to IR-6(d).

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

To assist current and former customers with the sign-up process, guidance on registering for credit monitoring has been posted online on the company's website and promoted through social media and has made available in locations throughout the province. This

guidance includes information on additional measures customers can take to protect themselves against identity theft, as well as details on other available services.

A fact sheet was also created with information about the service and tips for signing up. Thousands of paper copies were distributed and available to customers across the province through customer support sessions at community locations. In addition, the fact sheet was available at NS Power local depots and provided to MLAs and local councillors. NS Power has also actively encouraged customers, as well as its employees, to reach out to their families and neighbours to encourage them to sign up for the credit monitoring service.

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

Credit Monitoring

NS Power's notice to impacted customers included guidance for steps they could take to reduce any risk of harm resulting from the incident (including steps to protect themselves from fraud or potential identity theft), as well as an offer for two years of complimentary credit monitoring and identity monitoring services for impacted individuals. As described below, the Company subsequently extended the offer of complimentary credit monitoring to five years.

The credit monitoring service provided to customers and offered by TransUnion 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 the individual's financial history and is one of the primary tools leveraged for determining credit-related identity theft or fraud.

- Unlimited online access to their TransUnion CreditVision® Risk credit score, updated daily.

- Credit monitoring, which provides individuals with email notifications to key changes on an individual's 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.

- Up to $1,000,000 of expense reimbursement insurance for identity restoration in case of 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.

Thereafter, NS Power continued to keep customers updated regarding the ongoing incident and investigation. See response to IR-1 for additional details on NS Power's customer communication efforts.

(b) As noted above in response to IR-1 and IR-7(a), NS Power provided additional guidance on steps customers could take to protect themselves from potential identity theft or fraud resulting from this breach, which was included with the letters mailed to impacted customers. Please refer to IR-1 Attachments 1 and 2.

NS Power has also made this information available via its website.

Request IR-8:

Is the utility aware of any instances where the credit monitoring activation code is not working?

(a) If yes, please explain the mechanism in place to address these issues.
(b) If not, please provide a mechanism to resolve these issues.
(c) Are there any dedicated resources supporting these kinds of queries? Please explain.

Response IR-8:

(a-c) The vast majority of individuals were able to complete the online enrollment process within a few minutes using their activation code.

Notices to impacted customers also included a dedicated phone number for anyone having technical issues to speak with the team at TransUnion for help to enroll in the comprehensive credit monitoring service at no cost to them. NS Power has been working closely with TransUnion throughout this incident to resolve issues as they arise.

However, the Company is aware that some customers have had difficulty registering online. To help customers who were experiencing challenges with sign up, NS Power updated its website to include tips on some of the common issues customers have had in signing up. These tips have also been included on social media and shared during media interviews, as well as being made physically available in locations throughout the province.

NS Power has also held more than 30 in-person sessions in communities across the province to provide support for customers who need assistance in person in signing up for the credit monitoring service. The community partners or stakeholders who have reached out to the Company worked to share that information with the people and groups they heard from.

While signing up online remains the best path for most customers, this in-person support was intended to help those who are less comfortable with the online process or have questions.

Request IR-9:

Does the utility currently have a communication policy in place in case of a cybersecurity breach?

(a) If yes, please share the policy document.

(b) If not, why not.

Response IR-9:

(a) Yes, NS Power currently maintains a "Cyber Incident Communication Playbook" that outlines steps and approaches for NS Power's communications response in the event of a cyber incident at the Company. A copy of this playbook is included as Board Confidential Attachment 1.

Cybersecurity Incident NSEB IR-9 Attachment 1 has been removed due to confidentiality.

Request IR-10:

(a) Please list the customer services, such as pole relocation and new connection service requests, that have been impacted by this breach due to the shifting of resources away from these activities to support NS Power's cybersecurity response. In addition, provide a status update on the estimated time for full restoration of these services.

(b) Please provide a list of actions taken, along with corresponding dates, to inform NS Power's customers about the impact of the cybersecurity breach on customer services and response times.

Response IR-10:

(a-b) NS Power has clearly and frequently communicated with customers throughout the incident that there has been no disruption to NS Power's generation, transmission and distribution facilities and no impact to the Company's ability to safely and reliably serve customers.

Customers are still able to report an outage or emergency through the 24/7 outage line at 1-877-428-6004. The outage line has not experienced a disruption during or since the incident.

Unfortunately, while the Company initially worked to bring systems back, only calls about power outages and emergency situations were able to reach Customer Care in the initial stages of the response. NS Power resolved this issue by May 5, 2025.

NS Power acknowledges that the incident unavoidably presented challenges for customers trying to reach the Company during a limited timeframe. The team worked quickly to address this and implemented a workaround for customers requiring service hook-ups, service closures, or moves.

This was communicated via the NS Power website on April 30th, and the Company continued to provide services for thousands of customers every day.

Additionally, NS Power has expanded its Customer Care capacity to address questions related to the cyber incident:

- On Wednesday, April 30, the Company established online workarounds for the most common requests, including requests to start, stop or move electrical service.

- On Thursday, May 1, the Company established an incident response line to handle inquiries related to the breach and general customer concerns. This line was opened as soon as NS Power communicated to the public that certain customer data had been impacted.

- On Monday, May 5, NS Power expanded its Customer Care services to ensure that all regular service calls are answered. The Wiring Permit Centre has remained operational. While there were delays with certain services, the Company continued to assist customers throughout the incident. NS Power continued to book and complete wiring inspections as normal.

Excerpts of the communications and relevant dates can be found set out at www.nspower.ca/cyber. Please refer to IR-1 Attachment 4.

Request IR-11:

Please confirm whether NS Power customers can still pay their bill at a Canada Post location, if needed.

Response IR-11:

All previous payment options, including the ability to pay bills via Canada Post locations, remain available to customers. The only exception was the ability to use My Account between April 25 and June 4.

Request IR-12:

Board staff understands the billing of many customers was affected by the breach, and the customers received bills beyond their billing cycle. Further, as a result, their bills were higher than expected.

(a) Does the utility concur with the Board staff's understanding as expressed in the above preamble?

(b) Please confirm whether billing issues have been resolved.

(c) Please confirm if a customer can now access their online account, including billing history, usage details, and payment management.

(d) Please confirm that customers were not charged any penalty due to this delay.

(e) Please confirm the utility offered payment options to the impacted customers with no additional charges.

(f) Please confirm whether any negative credit impacts will apply during this disruption period.

Response IR-12:

(a) NS Power continues to work to restore all regular services to customers. This includes fully restoring the internal billing systems and delivering accurate bills to customers based on actual usage date. For this reason, the sending of bills to customers was temporarily paused.

To help avoid large and potentially unmanageable bills for customers in the future, in early June, NS Power began to issue estimated customer bills, which is a previously established process within the Company. Estimated bills are based on an average of the previous energy used at a customer's property during a similar timeframe in the previous year.

Some customer bills did appear larger than anticipated, and there were a variety of reasons for this. In some cases, payments had not yet been received and processed; some customers

received bills closer together as NS Power caught up on billing after the pause from April 25-June 4; and estimated bills mean that changes customers have made at the premises may not be reflected. NS Power is focused on maintaining a normal billing schedule as much as possible to help mitigate some of these customer concerns.

Customers will never pay for power they do not use. Any under- or over-payment will be addressed and accurately reflected on a future bill. Also, the Company has not applied late charges, or penalties on any outstanding balances since the incident. NS Power will communicate directly with customers before reintroducing late fees on outstanding amounts.

As of July 7, 2025, NS Power hired and deployed meter readers who are gathering energy use data from residential and business meters across the province. The data gathered will be used to provide bills to customers based on their actual energy use, and such bills will include adjustments as appropriate to reflect actual energy usage. Recovering from a ransomware attack is a complex and lengthy process. NS Power has teams of employees supported by third-party experts focused on making sure the business is continuing to operate, while other teams are focused on restoring and rebuilding the systems for these business processes.

As noted above, NS Power is working to fully restore its internal billing systems and automatically produce bills that reflect the actual energy used per the customer's meter. This is a complex process that must be undertaken carefully to ensure that the meters are safely reconnected with the system. The Company continues to work diligently to resolve this as soon as possible. The use of manual meter reading is a temporary measure that was implemented to produce bills from actual reads until the automated process is restored. Please also refer to part (a) above.

(b) Access to MyAccount was restored the evening of June 3, 2025. While customers can view their billing history and payment management on MyAccount, usage details are still unavailable as noted above. While meters are still accurately recording power use, the Company cannot automatically retrieve the information from meters and apply it to bills; therefore, usage details are not currently available through MyEnergyInsights.

(c) In the immediate response to the incident, NS Power committed and confirmed that customers would not be charged late fees or have their service disrupted as a result of this incident.

(d) NS Power has continued to assure customers that there will be no late charges or penalties on any outstanding bill balances until further notice, and has communicated this through its website, media releases, Customer Care Centre, social media channels, media interviews, stakeholders and other available channels.

(e) NS Power continues to work with customers to offer payment options. The Company encourages any customers who have concerns to call the Customer Care Centre, and NS Power can offer interest-free payment plans up to 24 months to help manage outstanding balances. More details are available to customers here: Ways to Pay| NS Power.

(f) Negative credit impacts related to payments do not apply during this disruption period. Customers are not being charged late fees, and NS Power is not disconnecting customers who are unable to pay their bills. The Company will communicate directly with customers to advise when late fees will be charged, and will work with all customers who need support with outstanding balances at that time.