Undertaking U-1:

To provide information that demonstrates what the Equifax tool does.

Response U-1:

Please refer to Attachment 1 for a description of the Equifax Service that is used at NS Power.

EQUIFAX

Date: Aug 25, 2026

Subject: Equifax iDecision Service Configuration & Privacy Protections

To whom it may concern,

This letter provides an overview of Equifax's iDecision service and outlines how it is configured at Nova Scotia Power (NSP) for their operations. Crucially, the underlying processes are structured as an automated, objective system specifically designed to protect consumer privacy and ensure that highly sensitive personal financial data is completely shielded from direct exposure to NSP frontline employees.

What is the Equifax iDecision Service?

Equifax's iDecision platform is a secure, automated credit-decisioning engine that integrates real-time credit bureau queries with NSP's proprietary business rules. Instead of requiring manual retrieval and interpretation of raw credit files by employees, iDecision acts as a secure "black box" intermediary. It automatically processes customer data against predefined credit scores, knockout parameters, and risk-evaluation matrices to deliver immediate, standardized, and objective outcomes required for service setup or financing approvals.

How Nova Scotia Power Configures and Uses iDecision

Nova Scotia Power utilizes three distinct strategy configurations tailored to specific customer groups and programs:

- **Consumer Strategy 01 (Res On-Bill Finance):** This strategy manages credit checks for residential customers applying for on-bill financing programs (such as energy-efficiency or heating upgrade loans from $1 up to a maximum of $50,000). The system securely retrieves and synthesizes multiple Equifax risk scores — including the Bankruptcy Navigator Index 3 (BNI3), Equifax Credit Behaviour Segmentation (ECBS), and Equifax Risk Score 2 (ERS2) — alongside SafeScan (SAFE) fraud alerts. The system applies these models to NSP's pre-configured matrices to approve credit limits ranging from $5,000 up to $50,000, or to flag applications for required administrative reviews.

- **Consumer Strategy 02 (Res Credit Check):** Activated during standard residential customer onboarding, this strategy determines if a utility security deposit is required and establishes the specific category (e.g., No Deposit, Standard Deposit, or a 3-Month Security Deposit). It is driven primarily by the Equifax Risk Score 2 (ERS2) and critical knockout attributes (such as active bankruptcies, foreclosure notices, satisfied or unsatisfied judgments, high-risk collections, and serious delinquencies).
- **Commercial Strategy 01 (Com On-Bill Finance):** Designed for business accounts, this strategy evaluates commercial creditworthiness by querying the Business Failure Risk Score(BFRS2.1) and the Commercial Delinquency Score (CDS2.1) to approve commercial financing tiers up to and over $30,000, while executing automated knockouts on commercial bankruptcies, NSF activity, or collection history.

Strict Protections for Consumer Privacy and Personal Information

A foundational benefit of NSP's iDecision integration is its rigorous, system-enforced protection of customer data. The platform completely eliminates manual oversight and subjective bias, protecting customer privacy through several programmatic guardrails:

- **1. Direct Credit Report and Score Masking:** NSP frontline employees never see or have access to a customer's detailed Equifax credit report, transaction histories, outstanding balances, or specific trade line activities. In fact, even the numerical credit scores themselves (such as the ERS2 or BNI3 scores) are fully masked. The scores are computed and evaluated entirely within Equifax's secure servers and are never transmitted to utility customer representatives.

- **2. High-Level, Actionable Output Flags Only:** The iDecision engine returns only high-level operational codes, known as Special Output Elements. For standard credit checks, the employee only sees the resulting service action, such as 'Class Code: ACPT' (Accept with No Security Deposit Required) or a standardized deposit directive (e.g., 'Standard Deposit Required' or '3 Months Security Deposit Required'). Because employee screens display only these high-level instructions, customers are spared from having to discuss the details of past bankruptcies, judgments, or collections with utility personnel.

- **3. Standardized Identity and Fraud Safeguards:** Integrated fraud checks like SafeScan (SAFE) automatically detect active warnings or identity red flags (such as deceased indicators or under-age applicants). If a warning is triggered, the system displays a neutral, standard administrative code (such as 'H1' or 'N2' indicating manual review is required) to protect the applicant's identity while preventing frontline employees from viewing sensitive fraud files or holding subjective biases.

- **4. Systematic Compliance with Credit Locks:** In compliance with consumer protection legislation, such as the Credit Assessment Agents Act (CAAA), customers who have locked their credit files are fully accommodated. If a consumer's credit file is locked, iDecision automatically blocks the query and returns a standardized, neutral reject code 'B7' with the description 'REPORT UNAVAILABLE - CREDIT FILE LOCKED'. Frontline employees handle this standard notice without making negative credit assumptions or gaining unauthorized access to the customer's financial history.

Conclusion

By configuring Equifax's iDecision service as an automated gateway, Nova Scotia Power protects customer data in the course of Nova Scotia Power's operations. Sensitive financial profiles are handled strictly in the background by Equifax's secure infrastructure. Frontline staff are provided only with the minimal, high-level operational outputs required to establish service. This robust technical boundary ensures absolute compliance with credit-reporting laws, prevents personal data leakage, and fosters a high-trust onboarding experience for all Nova Scotia Power customers.

Sincerely,

Dillon McGuire
Director, Solutions - Public Sector
Equifax Canada Co.

EQUIFAX

Undertaking U-2:

To provide the volume of data held in the information technology systems by Nova Scotia Power at the time of the cyberattack

Response U-2:

NS Power's information technology systems held approximately 3,000TB of data at the time of the cyberattack.

Undertaking U-3:

To enquire how many Social Insurance Numbers may have been resident in the Data Lake at the time of the cyberattack, and provide that number if available, and how many were expunged in 2024.

Response U-3:

Following a review of available records, NS Power has determined that the Company does not possess information sufficient to establish the number of Social Insurance Numbers that may have been resident in the Data Lake at the time of the cyberattack. Please refer to U-11.

Undertaking U-4:

To provide the verification process for confirming the identity of small business customers and the representative who is speaking on behalf of the small business when they contact NSP.

Response U-4:

The following is the verification process for any commercial / business account:

Is the caller the account holder or listed on the account?

IF YES [redacted]

IF NO [redacted]

REDACTED

[redacted]

Undertaking U-5:

To provide an updated phishing failure rate for the period of April 2025 to date.

Response U-5:

Updated phishing failure rates to the end of July 2026 are as follows:

	Jan	**Feb**	**Mar**	**Apr**	**May**	**Jun**	**Jul**	**Aug**	**Sep**	**Oct**	**Nov**	**Dec**
2023				2.8%	1.3%	2.3%	1.1%	4.3%	4.9%	2.3%	1.7%	11.0%
2024	0.4%	17.7%	1.7%	3.7%	1.1%	2.5%	4.7%	0.2%	0.5%	0.7%	14.3%	0.7%
2025	6.4%	3.3%	0.5%	0.2%	N/A	N/A	4.8%	1.9%	9.6%	0.5%	2.9%	1.6%
2026	1.7%	2.2%	2.8%	2.2%	3.7%	1.3%	0.7%					

Undertaking U-6:

To confirm that CA IR-1(e) will be addressed in Proceeding M12273.

Response U-6:

CA-IR-1(e) reads as follows:

> Cyber Security Program Effectiveness
>
> Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 18, ll 1-4
>
> > Quote: NS Power maintains a cybersecurity training and awareness program and conducts mandatory quarterly cyber training and monthly phishing simulation testing exercises with all employees to educate employees about NS Power's information security policies and common risks, and to help them understand their information security responsibilities
>
> (e) Please provide a summary of the number and types of cyber incidents NSPI recorded in the last 5 years? What improvements have been made to systems and practices as a result of these events.

While NS Power had indicated an intention to address this question in M12273, the Company can now confirm that there were no cyber incidents recorded in the last five years. NS Power commits to answering any follow up questions throughout the course of the M12273 proceeding.

REDACTED

Undertaking U-7:

To provide the actuals from 2025 for the costs associated with the cybersecurity incident, including cost categories, as well as an updated forecast for 2026.

Response U-7:

	2025 Actual	2026 Forecast	Total
[redacted]			

[redacted]

Undertaking U-8:

To provide a more granular breakdown of the table in Attachment 1, CA IR-6.

Response U-8:

Please refer to Confidential Attachment 1.

Minister of Energy - Accountability for Nova Scotia Power U-08 Confidential Attachment 1 has been removed due to confidentiality.

Undertaking U-9:

To confirm if carrying costs on accounts received are tracked separately, and if they are, what that amount is for 2025-2026 until it is forecasted to get back to normal.

Response U-9:

Carrying costs on accounts receivable are not tracked separately by NS Power.

As stated in the response to NSEB IR-5, NS Power has not prepared an analysis on how much of the increase in the accounts receivable balance is due to the Company's decision to suspend collection activities, including the application of interest on late payments, after discovery of the cyber incident.

NS Power believes that it is not possible to precisely determine how much suspension of collection activities increased the accounts receivable balance as opposed to such items as growth in active customer accounts, higher billed revenues or other external impacts.

NS Power estimates that the average monthly accounts receivable balance increased by approximately $65 million in 2025 due to changes in the collection policy, driving increased interest expense of approximately $1 million in 2025. The forecast increase in the average monthly accounts receivable balance for 2026 is approximately $101 million which would forecast an increase in carrying costs of approximately $3 million.

Increased costs due to the cyber attack were not included in NS Power's 2025 or 2026 rates. NS Power would not have earned above the top of the Company's approved earnings band in 2025 had these additional financing expenses not been incurred. NS Power anticipates that accounts receivable balances will return to normal in 2027, after the reinstatement of collections activities and interest charges on late payments in October 2026.

Undertaking U-10:

To search for, and produce if found, directions in 2018 to customer service representatives regarding the deletion of Social Insurance Numbers

Response U-10:

NS Power has conducted a search for this information and has not been able to locate the 2018 instructions that were provided to Customer Service Associates.

Undertaking U-11:

To provide the 2024 SIN elimination program; to advise how many SIN numbers were purged from NS Power's system.

Response U-11:

NS Power has searched for documentation confirming the amount of Social Insurance Numbers that were removed from the Customer Information System (CIS) in 2024. This information was part of data that was lost during the cyber attack. As a result, the Company cannot confirm the total number that were removed; however, as indicated in testimony at the hearing, NS Power sent letters to approximately 228,000 customers whose SINs were on record as of July 2021 (see transcript page 152) and which would have been removed from the CIS before or during the 2024 work to remove SINs.

Undertaking U-12:

To provide the script given to Nova Scotia Power staff to answer questions about the cyber incident.

Response U-12:

Please refer to Attachment 1 for the Customer Service Associate (CSA) scripting relating to the cyber incident.

Updates

*****June 25th update as per public announcement*****

Beginning June 25th, we will be offering 5 years of free credit monitoring to ALL customers, past and present, regardless of whether they received a letter about the incident. For any customers who already signed up, they will automatically be extended to 5 years. Customers will not pay for any costs incurred by Nova Scotia Power for credit monitoring resulting from this incident.

General Guidance

- As always, we can demonstrate that we care for our customers by showing empathy and support at this time.
- Our website **nspower.ca** is the best single source for cyber incident updates and customer support.
- **We encourage customers (current and former) to take full advantage of the free 5-year credit monitoring service provided by TransUnion (myTrueIdentity®)**. *Redeem your activation code before 9/30/2025 to take advantage of the service.
    - **If a customer received a notification letter, they should use the code included to sign up for credit monitoring**
    - **Current or former customers may obtain an activation code for credit monitoring by using the customer verification tool on our website.**
- Tips on registering for credit monitoring and info on additional steps to take to protect against identity theft are available at **nspower.ca/cyberhelp.**

TransUnion Contact Information:

Arrangements have been made with TransUnion to provide customers with a free, five-year subscription to a comprehensive credit monitoring service called myTrueIdentity. We encourage customers (current and former) to take advantage of this free service.

- **To sign up for the credit monitoring service, customers go directly to the TransUnion website https://www.mytrueidentity.ca and enter their code.**
    - For technical support with setup/troubleshooting myTrueIdentity®, call 1-877-884-3441.
    - **IMPORTANT:** A customer must complete the online registration for myTrueIdentity during the session. If they stop or pause for too long, they will be locked out and will need to call 1-877-884-3441 for technical assistance.
- For questions about the notice, call 1-844-818-0376. This is a dedicated line for Nova Scotia Power customers. (*If a customer calls any other TransUnion phone number, they will not be offered specific info on Nova Scotia Power's cyber incident or the 'free' credit monitoring service.)

<u>FAQs</u>

Q: Why didn't you offer credit monitoring to everyone right away when this happened? Why now?
Our initial focus was on customers that our investigation confirmed that their personal data was were impacted by the breach. Through our investigation we have learned that the personal data of former customers was included in the information accessed and taken by the unauthorized third party. Out of an abundance of caution and to ensure a level of protection and reassurance for our customers, we are now expanding our offer free credit monitoring to ALL customers, past and present, regardless of whether you received a letter from us about the incident.

Q: Why wasn't 5- years of credit monitoring offered from the start? Is it because your insurance will only cover 2 years?
We've heard from our customers and know they are concerned about the safety of their personal information. We listened to their feedback that additional credit monitoring protection would provide more reassurance and have decided to offer five years of coverage to ALL Nova Scotia Power customers, both past and present.

Q: What are you doing to reach former customers who no longer live in the province to provide the credit monitoring?
Given that we do not have updated contact information for many of our former customers, and given that we are still working to determine the full scope of data that may be impacted, we are working to share a 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-years of credit monitoring services.

Q: Was my data impacted?
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.

Q: I'm a current customer, but I did not get a letter. Does that mean I was not affected?
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.to all current and former customers

Q: 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?
To receive your unique activation code that will enable you to sign up for credit monitoring, please visit our website at nspower.ca and click on the Customer Verification. 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).

Q: My name could not be found in the Customer Verification tool. Can I still get an activation code for free credit monitoring?
Yes. I can help you . I'll take a look in our customer information system.
****CSAs -Please follow the escalation path to obtain a code for the current or former customer.*

Q: If I received a letter because I was affected, should I use this new customer verification lookup?
You should use the code on your letter, as that code will not be in the lookup tool on our website.

Q: I've already signed up for 2 years of credit monitoring. Do I need to sign up again to get 5?
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.

Q: Will credit monitoring be paid for via customers and rates?
Customers will not pay for any costs incurred by Nova Scotia Power for credit monitoring resulting from this incident.

Q: Will there be a rate increase as a result of this cyber incident?
We have cyber incident insurance, which we anticipate will cover the majority of related costs. Customers will not pay for any costs incurred by Nova Scotia Power related to the free credit monitoring service being provided.

Q: I do not have an email address or a computer.
Please contact TransUnion at 1-877-884-3441 who will be able to assist you in obtaining a copy of your credit report and helping put a fraud alert on your credit report. The alert informs creditors of possible fraudulent activity and request that creditor contact you prior to establishing any accounts in your name

Q: I need help setting up credit monitoring services. Can you help?
For tips on registering for myTrueIdentity® along with additional steps to help protect you from identity theft are available at nspower.ca/cyberhelp. If you are having difficulty setting up myTrueIdentity® online credit monitoring service and require technical support, please contact TransUnion at 1-877-884-3441.

Q: Are you coming to my community? I saw an advertisement about Nova Scotia Power providing customers with in-person support.
I do not have a schedule for the next sessions.

Q: You said that the threat actor has published my stolen data. Where has my information been shared?
A: 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".

Through our forensic investigation with third-party cyber security experts, we have learned that this is where the threat actor has published some of the data. If you received a letter from us informing you that your personal information was impacted, we encourage you to follow the steps to sign up for TransUnion's credit monitoring service, myTrueIndentity.

Q: What happens now that [a portion of our data] is now online? Isn't the threat to my personal data greater than before?
A: We are actively working with cybersecurity experts to assess the nature and scope of the information that may have been exposed.

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.

Q. Why did you not just pay the hackers when Emera makes so much profit from Nova Scotians?
A: 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.

Q: What personal data was compromised?
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.

Q: Can you confirm exactly what information of mine was included in the incident?
We sincerely apologize that this issue has occurred. If you receive a notice about this incident, it means that we have identified that your information was impacted in connection with the recent cyber incident.

Please refer to the notice you received for details about what type of information may have been impacted.

We encourage individuals who receive a notification to sign up for the credit monitoring service that we have made available at no cost.

Q: I received a letter. Can you confirm exactly what information of mine was included in the incident?
We sincerely apologize that this issue has occurred. If you received a notice, we have identified that your information was impacted in connection with the recent cyber incident.

The type of information that may have been impacted varied by customer and depended in part on what information a customer provided to us.

Please refer to the notice you received for details about what type of information may have been impacted.

We encourage individuals who receive a notification to sign up for the credit monitoring service that we have made available at no cost.

Q: Can you confirm if my SIN# was breached in this incident?
We sincerely apologize that this issue has occurred. If you receive a notice about this incident, it means that we have identified that your information was impacted in connection with the recent cyber incident.

Please refer to the notice you received for details about what type of information may have been impacted. If your Social Insurance Number (SIN) was mentioned in the letter, it does mean that your SIN may be among the data that may have been impacted.

We recommend customers take advantage of the free 5-year credit monitoring service.

Q: Why do you keep SINs in your database?
SINs were used in certain circumstances for customer authentication purposes. We are committed to permanently deleting all instances of SINs from our systems as soon as our investigation allows. Out of an abundance of caution we recommend customers take advantage of the free 5-year credit monitoring service.

Q: Do you have my SIN on file?
Social Insurance Numbers (SINs) were used in certain circumstances for customer authentication purposes. We do not have access to confirm what data was on your account from your initial account setup.

We have sent notices to individuals who have been impacted by the recent cyber incident. If you received a letter, please refer to the notice for details about what type of information may have been impacted. If your Social Insurance Number (SIN) was mentioned in the letter, it does mean that your SIN may be among the data that may have been impacted. We encourage individuals who receive a notification to sign up for the credit monitoring service that we have made available at no cost.

We are committed to permanently deleting all instances of SINs from our systems as soon as our investigation allows.

*****If customer pushes for confirmation as to whether their actual SIN was on file:**

Response: *The type of impacted information varied by customer, and depended, in part, on the information provided by each customer.*
*****If further pushed: CSAs please escalate internally. (Privacy Office)**

Q. Can you please remove my SIN from your system?
We are committed to permanently deleting all instances of SINs from our systems as soon as our investigation allows.

*****If customer escalates, please record the customer's contact information.** Response: *Your request has been forwarded to our Privacy Officer. They will respond to you within 1-2 weeks.*

**Record customer information and send email to privacy.officer@nspower.ca*

Q: If a spouse is also listed on the account, has their information been compromised too? And if so, will they receive a letter and credit monitoring services?
Notifications have been mailed to impacted individuals, which include detailed information about resources and support. CSA: *I can confirm if your spouse is listed on the account. Let me look that up for you now*.

***IF the customer is interested in the TransUnion credit monitoring service, please follow the escalation path to provide a code to the customer.

Q: What is the March 19 date I read in the letter I received?
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.

Q: Why did it take almost a month to detect the third party on your network?
We are actively working to investigate this incident, and we are unable to speculate or share unverified information while the investigation remains ongoing.

Q: Do you know why specific customers had their data impacted and not others?
Our investigation continues. We cannot speculate or share unverified information while the investigation is ongoing. Out of an abundance of caution we recommend customers take advantage of the free 5-year credit monitoring service.

Q: Was my banking information included in this data breach?
The types of impacted personal information varied by individual customer and depended, in part, on the information provided by each customer. Bank account numbers may also have been impacted, if you provided this information for pre-authorized payments.

As a precautionary measure, arrangements have been made with the consumer reporting agency, TransUnion, to provide you with a 5-year subscription to a comprehensive credit monitoring service (TransUnion myTrueIdentity) at no cost to you.

Q: Should I shut down MyAccount and go back to paper billing – how do I know my info is safe?
We appreciate your patience. Billing is currently delayed due to our system issues however customers will not incur late fees or penalties, or service disruptions or disconnections for non-

payment as we work to resolve this issue. We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future. E-billing and My Account remain an effective and convenient service option for customers.

Q: Were My Account passwords stolen?
This remains an active investigation. We cannot speculate or share unverified information while the investigation is ongoing.

Q: Should I trust Nova Scotia Power with my bank account information on payments?
We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future. There are numerous options to pay your Nova Scotia Power bill including through your bank via online banking.

Q: I'm no longer comfortable making online payments in MyAccount or having automated payments? How can I pay my bill securely?
I understand your concerns at this time. Safety and security are very important to us. Paying through your bank is one of the safest options for paying your bill.

Q: Why do we not have MFA for My Account? Will that be coming after this?
We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future. We will share additional information as it becomes available.

Q: I prefer Equifax for credit bureau monitoring, can you pay for that?
TransUnion is consumer reporting service that Nova Scotia Power has engaged to provide potentially impacted customers with a 5-year subscription to a comprehensive credit monitoring service (TransUnion myTrueIdentity) at no cost. Nova Scotia Power is unable to reimburse you for other products.

Q: Why can't you sign everyone up for TransUnion, why is the onus on the customer?
Consistent with industry practice, TransUnion requires individuals to complete their own enrollment for the credit monitoring services. TransUnion will engage directly with potentially impacted account holders to ensure they are properly enrolled in the comprehensive credit monitoring service at no cost to them.

Q: How will you ensure this won't happen again in the future?
We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future.

Q: When will your customer service systems be fully restored?
We continue to work to restore our systems safely and securely. Currently, we are not able to provide a timeline for full restoration. The latest information is posted on our website at nspower.ca.

Q: Is your network currently secure?
We are working around the clock, along with our external cybersecurity experts, to do everything we can to restore affected systems in a safe and secure manner.

Q: Who/What is responsible for the incident?
Our IT team is actively working with external cybersecurity experts to investigate this incident. We have also notified law enforcement and regulatory authorities. We cannot speculate or share unverified information while the investigation is ongoing.

Q: What is Nova Scotia Power doing to address this cyber incident?
Although we are still actively investigating this cyber incident, we have taken the following steps:

- Engaged external 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.
- Commenced notifying impacted account holders with further details about the cyber incident, including providing resources and support.
- Actively working to restore our systems and continuing to expand our interim business processes where needed to ensure business continuity to serve our customers.

<u>FAQ -Commercial Customer Banking Information</u>

Q: Has my company's bank account been compromised?
I do not have that information, and our investigation remains ongoing. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution with which the account is maintained

From [Frequently Asked Credit Questions | TransUnion Canada]

Q. How can I place a fraud warning on a deceased consumer file if fraud has occurred?
A. In order to release personal information on a deceased person, TransUnion requires a copy of the Death certificate or the will/certificate of appointment, stating that this person is the next of kin or executor/executrix.

The request must also include two pieces of the identification of the next of kin or executor/executrix requesting the file as well as one piece of identification for the deceased that verifies address. If the deceased address is noted on the Death Certificate, TransUnion will accept it as viable address verification for the deceased.

Additionally, if the appropriate information has been given, the file will be processed and sent to the executor's/next of kin's address. If the Death Certificate has a Social Insurance Number ("SIN"), the SIN will be added to a High Risk Fraud Alert database to indicate that the SIN is deceased. The SIN number will remain in a protective state indefinitely and a note will also be placed onto the credit report to indicate that the consumer is deceased.

Note: If there is more than one appointee, TransUnion requires identification for each executor/executrix to process the request unless they receive an additional letter of direction that the executor/ executrix can act separately.

Correspondence in English
TransUnion Fraud Victim Assistance Department
3115 Harvester Road,
Suite 201 Burlington ON L7N 3N8

Q. How do I add a Potential Fraud Alert to my credit file
A. If you think you may be a victim of fraud but there has been no reported misuse of your credit or no confirmed misuse of your personal information, you can place a Potential Fraud Alert on your credit file. If, for example, you've lost a purse or wallet, placing a Potential Fraud Alert will tell potential lenders that you may be a victim of fraud and provide them with your contact phone number.

- A Potential Fraud Alert can be placed on your credit file.
- An alert can also be placed on your Social Insurance Number (SIN).
- A Potential Fraud Alert on your credit file will remain in place for 6 years unless you request to have the alert removed earlier.
- An alert on your Social Insurance Number (SIN) will remain in place for at least 1 year.
- If fraudulent misuse of your personal or credit information is confirmed, please contact us by phone or in writing to add a Confirmed Fraud Alert to your credit file.

There are three ways you can add a Potential Fraud Alert to your credit file:

- Online: Visit our self-service website. To promote our online Potential Fraud Alert service, sign-up is free for a limited time.
- Over the telephone: call 1-800-663-9980 and select option 3 to use our Interactive Voice Response (IVR) system to place your alert. Please note that SIN protection is not available through the IVR.
- In writing: View additional information to add a potential fraud alert in writing.

Q. How do I receive a free copy of my TransUnion Personal Credit report?
A. You can obtain a free copy of your Consumer Disclosure online through our self-service website. Click Here to visit our self-service website.

You can also request a copy of your Consumer Disclosure by phone or mail, and it will be mailed to you. To review the options for receiving a copy of your Consumer Disclosure, please refer to the Consumer Disclosure section of our website

Q. How old do I have to be before I can have a credit file at TransUnion?
A. TransUnion does not maintain credit records for individuals under the age of majority in their current province of residence. Our file creation rules comply with the age of majority in the individual provinces and territories of Canada as listed below:
Province Age of Majority

- Alberta 18
- British Columbia 19
- Manitoba 18
- New Brunswick 19

- Newfoundland and Labrador 19
- North West Territories 19
- Nova Scotia 19
- Nunavut 19
- Ontario 18
- Prince Edward Island 18
- Quebec 18
- Saskatchewan 18
- Yukon Territories 19

Q. How do I add a Fraud Alert to my credit report?
A. Please contact the Fraud Victim Assistance Department:

For English speakers in all provinces except Quebec, please contact us between the hours of 8:00 a.m.-8:00 p.m. ET at 1-800-663-9980

Undertaking U-13:

To provide the volume of data in the July 2021 cut in the Azure staging area.

Response U-13:

The volume of data from the July 2021 cut for My Energy Insights was approximately 0.005TB.

Undertaking U-14:

Re: Exhibit N-17(i), Attachment 2, Retention Disposition Schedule, to advise what the difference is between "Internal Audit Document" and "Internal Audit Document Set".

Response U-14:

There is no difference between these two content types. The Internal Audit Document Set was created for a specific SharePoint technical requirement.

Undertaking U-15:

To provide the size or volume of data contained in the NAS device at the time of the cyberattack.

Response U-15:

The approximate volume of data contained in the NAS device at the time of the cyberattack was 2.5PB which is 2500TB. The threat actor accessed 7TB which is 0.28% of the volume of data held in the NAS.

Undertaking U-16:

To advise whether Nova Scotia Power pays any fees on a monthly basis based on the amount of data in the Data Lake.

Response U-16:

Yes, NS Power pays a variable monthly fee that is based on the amount of data that is being stored in the Data Lake.

Undertaking U-17:

To provide the billing inserts, with the dates they were provided to customers.

Response U-17:

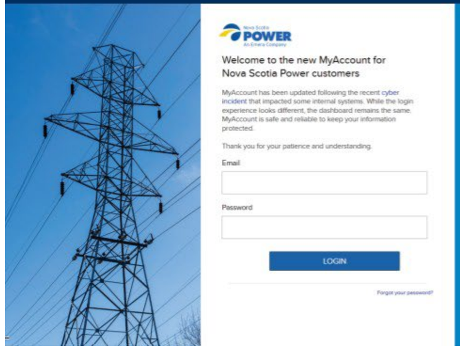
Please refer to Attachment 1 for copies of billing inserts from June 2025 to July 2026.


Bill Inserts (June 2025 to July 2026)

REDACTED (CONFIDENTIAL INFORMATION REMOVED)

Important Information About this Bill

Our teams continue working to restore all services safely and securely following the recent cyber incident.
We know the pause in billing has been a concern for customers, and we are now able to provide you with a bill.



Reintroducing MyAccount

Thank you for your patience as we worked to update and bring MyAccount safely back online. While the login experience looks different, the dashboard remains the same. Your current passwords will work for logging in and for continued safety, **we suggest changing those passwords before logging in.**

We recommend paying your bill through MyAccount or through your bank's website by setting Nova Scotia Power up as a payee.

June 2025 Bill Insert (Estimated Bills)

A webpage dedicated to the latest information on the post cyber billing experience was launched and promoted to customers. NSPOWER.CA/BILLING is the single source of truth. This website was also featured in the corner ad message of all bills.

Billing Process

Meters continue to accurately record energy usage, however we are not currently able to retrieve this information and apply it to your bill. To get billing back on schedule for our customers, so balances don't add up, we will now provide an estimated bill.

What does this mean for you?

Your energy usage after April 24th will be estimated based on your historical usage during the same time period in 2024. When we are able to retrieve your current energy usage data from your meter, your bill will be adjusted to reflect your actual usage. We want to reassure our customers of our continuing promise that **you will never pay for power you don't use.** To learn more about what this means for you, please visit **nspower.ca/billing**.

We're here to work with you and encourage customers with concerns to call Customer Care at **1-800-428-6230** to discuss options. For more information on billing, please visit **nspower.ca/billing**.

30094-I-0152

Nova Scotia POWER An Emera Company

Important Information About this Bill

On April 25, we detected unusual activity on our network and began actively responding to what we now know was a sophisticated ransomware attack on our company and our customers. As part of the incident response, billing was paused.

The enclosed bill reflects your actual power usage for the billing period up to April 24th - prior to billing being paused. The due date on this bill does not reflect the delay between your billing period and when you are receiving this bill. You are not required to pay by this date. **Please know that there are no late fees or service disruptions as a result of this incident and delay in billing.** At this time, we recommend paying your bill through your bank by setting Nova Scotia Power up as a payee. We remain sincerely sorry that this issue has occurred.

Nova Scotia POWER An Emera Company

30094-I-0150

You can stay up to date on our website at **nspower.ca.**

June 2025 Bill Insert (Bills based on actual usage)

This insert was specifically for customers receiving a bill with actual usage collected before the cyber incident. The insert also assured customers that the bill due date does not reflect the pause in billing i.e. they are not required to pay the balance on the date shown.

Important Billing Information

We are continuing to work on restoring all regular services to our customers following the recent cyber incident. While meters continue to accurately record energy usage, we are not currently able to retrieve this information and apply it to your bill. We know billing accuracy is important to our customers and we have temporarily returned to physical meter reading. If meter readers are unable to access a meter, the bill will be estimated.

Meter Reading

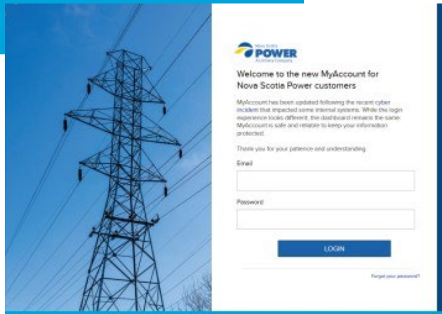
Meter readers are now working to gather energy use data from residential and business meters across the province. Reading a meter takes only minutes and you do not need to be home for your meter to be read. Our meter readers wear Nova Scotia Power branded clothing and have a Nova Scotia Power identification badge. **If meter readers are unable to access your meter, you will receive an estimated bill.**

Estimated Billing

Estimated bills are based on an average of the previous energy used at your property during a similar time of year. If your bill was estimated, it will be noted at the top of your bill. When we are able to retrieve your current energy usage from your meter, your bill will be adjusted to reflect your actual usage. **We want to reassure our customers that you will never pay for power you do not use.**

July/August 2025 Bill Insert

The post cyber billing experience continued to be detailed on NSPOWER.CA/BILLING. MyAccount is brought back online and awareness of its safety and the need to change passwords begins.



Reintroducing MyAccount

Thank you for your patience as we worked to update and bring MyAccount safely back online. While the login experience looks different, the dashboard remains the same. Your current passwords will work for logging in and for continued safety, **we suggest changing those passwords before logging in.**

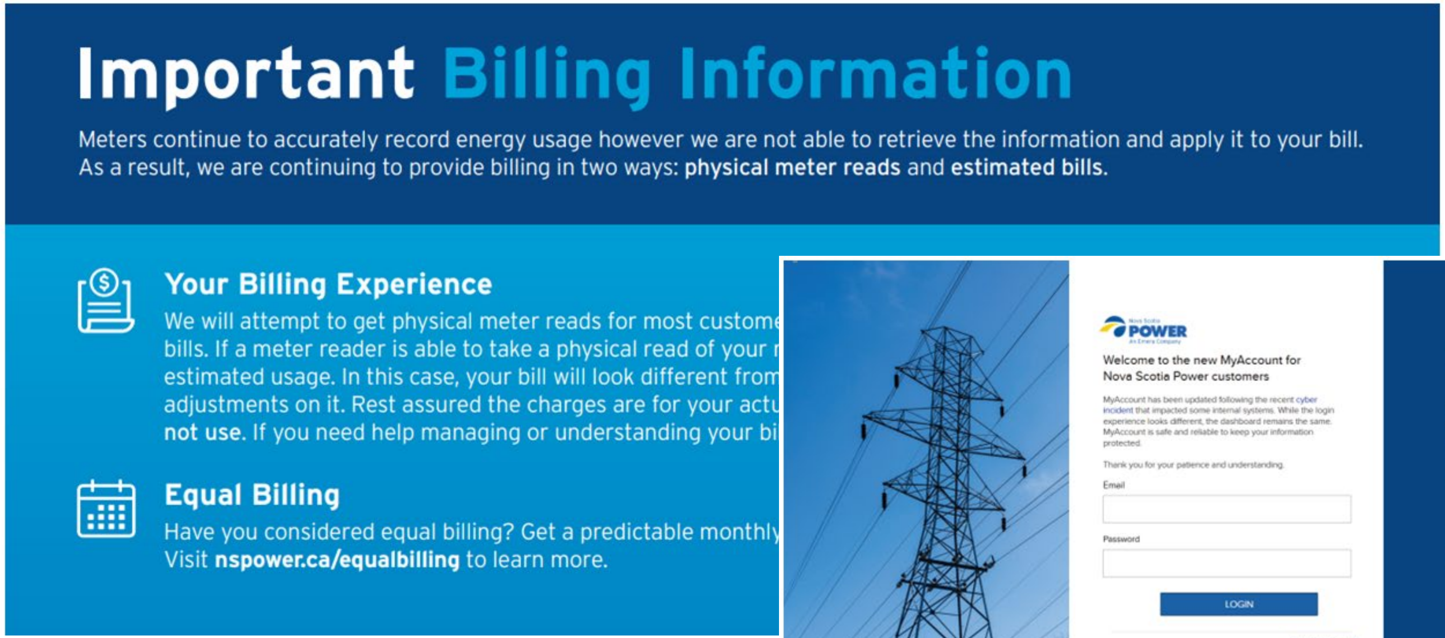
We recommend paying your bill through MyAccount or through your bank's website by setting Nova Scotia Power up as a payee.

We're here to support you. Please call our customer care team at **1-800-428-6230** for help with questions, as well as resources and options. For more information on billing, please visit **nspower.ca/billing**.

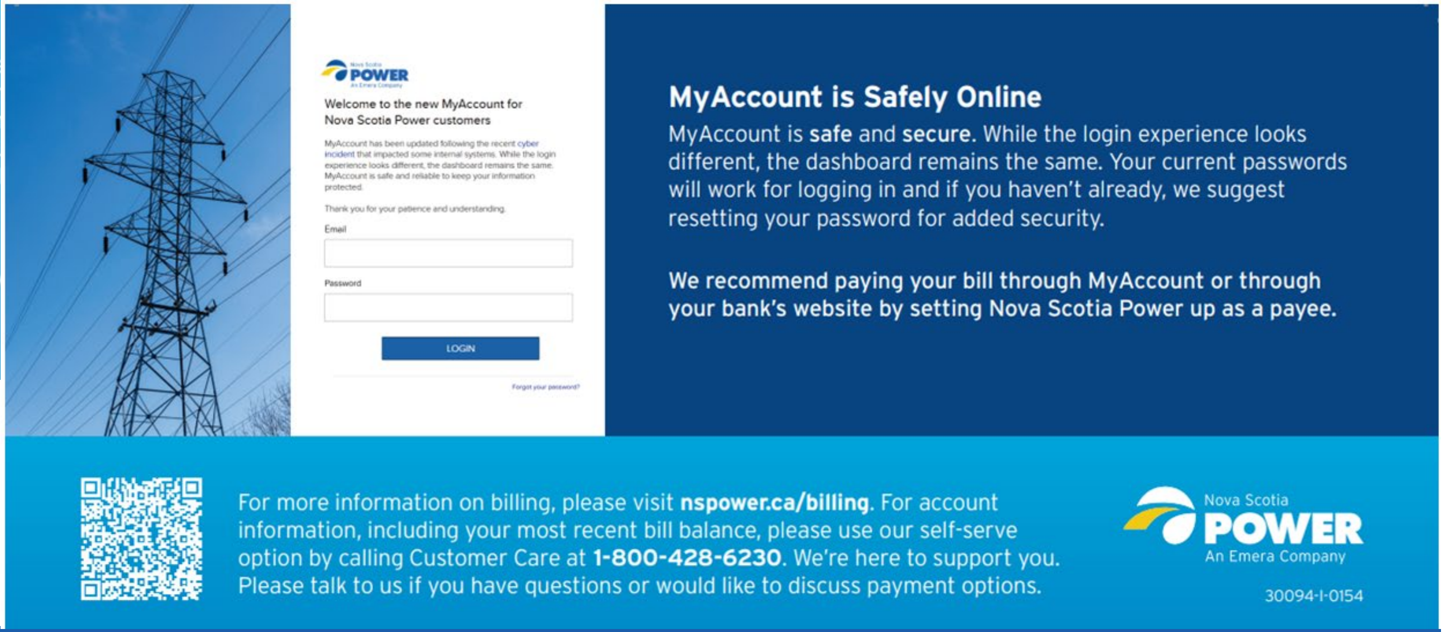
30094-I-0153

Nova Scotia POWER An Emera Company

September/October 2025 Bill Insert



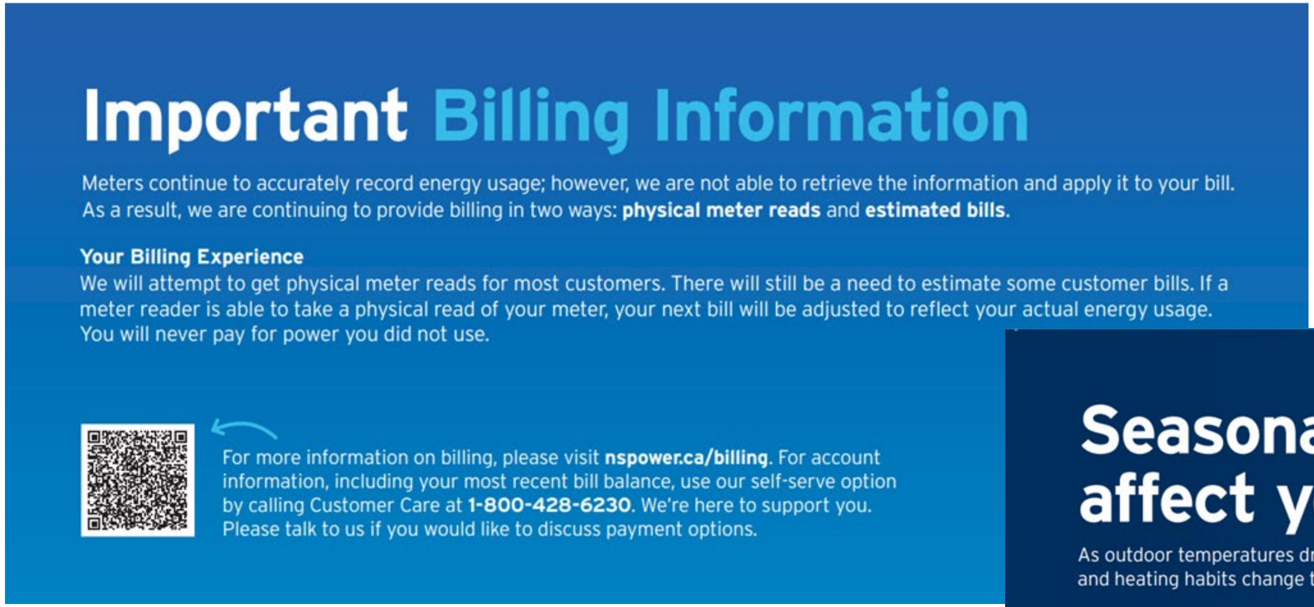
The post cyber billing experience continued to be detailed on NSPOWER.CA/BILLING. The safety of MyAccount and awareness of the need to change passwords continues.

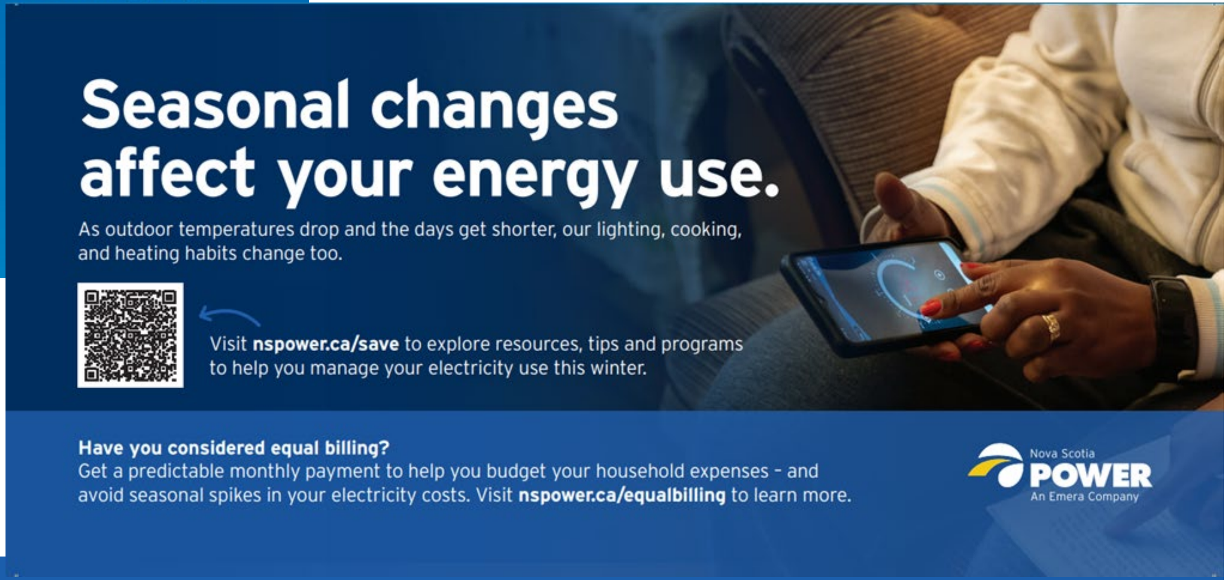


November/December 2025 Bill Insert

Continued awareness of the need to estimate customer usage. Focus moves to the post meter read experience including adjustments that will appear on the next bill. NSPOWER.CA/BILLING is expanded with videos explaining bill adjustments.

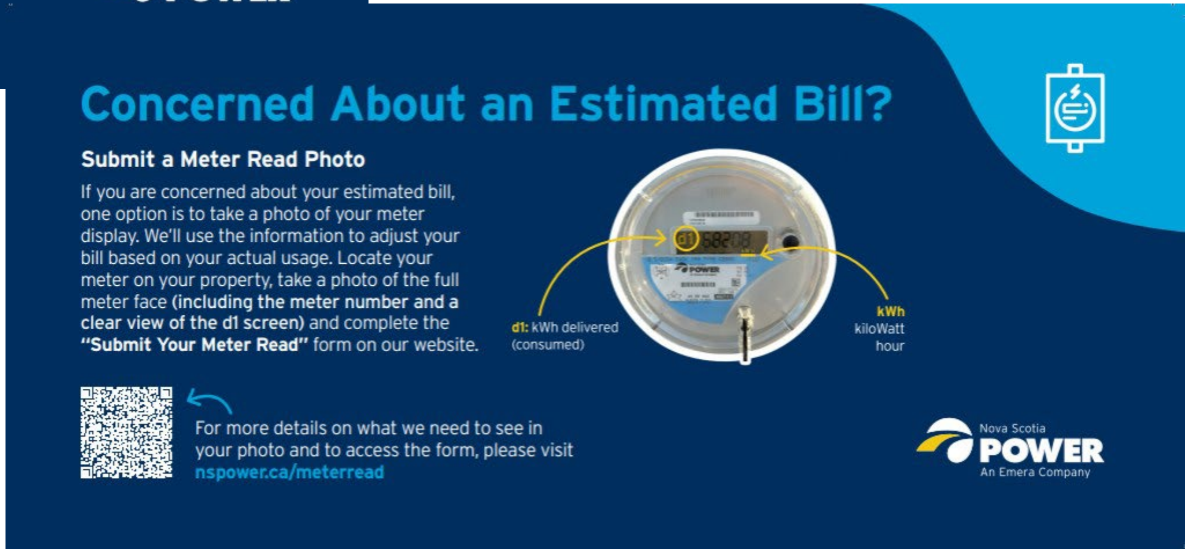
Our annual seasonal awareness of temperature changes and its impact on electricity usage begins.





January/February 2026 Bill Insert

Remote meter reads begin in late December 2025, and we continued to support customers who were still receiving an estimated bill. Launched an online form to submit a meter read photo and have a bill reissued based on actual usage (form launched Nov 2025).



February/March 2026 Bill Insert

Most customer bills are now reflecting actual usage data. Seasonal temperature awareness continues.

Added *Our Commitment to You: Billing* on February 19, 2026

To our customers,

We know that over the past year, you have had a lot of questions about the cyber incident and the impacts on our billing systems.

For over a century, Nova Scotia Power has been a part of this province. Our team of 2,200 employees are your neighbours, friends, and family. We take our responsibility to provide an essential service seriously, and we are committed to earning your trust, one interaction at a time.

Here is what you can expect from us as we move forward:

IMPROVING YOUR BILLING EXPERIENCE

The cyber incident disrupted our ability to read meters. We are working diligently to fix this:

Meter Reconnection
Most meters have been reconnected to our digital billing system. We expect this process to be **complete by March 31, 2026.** With the ability to remotely read meters restored, your bills will return to normal and the need to estimate bills will be significantly reduced.

No Penalties
To ease the transition, we are continuing to not apply late charges or penalties on outstanding balances, and your credit score will not be impacted. We will provide notice before reintroducing any late fees.

Billing Accuracy
If you received an estimated bill, it will be reconciled automatically once your meter is read (either remotely or in person). You will either receive a credit on your account, or we can work with you to smooth out any amounts owing over future bills.

SUPPORTING YOU

Many of you have additional questions and want to discuss options related to your bill. We are here to help.

Flexible Payment Options
Our team can provide interest-free payment plans or enroll you in Equal Billing to help manage monthly costs. **If you need assistance, please call us at 1-800-428-6230.**

In-Person Support
We will continue holding community engagement sessions throughout 2026 to answer your questions directly.

Thank you for your continued patience and for the kindness you've shown to our teams and crews.

Sincerely,

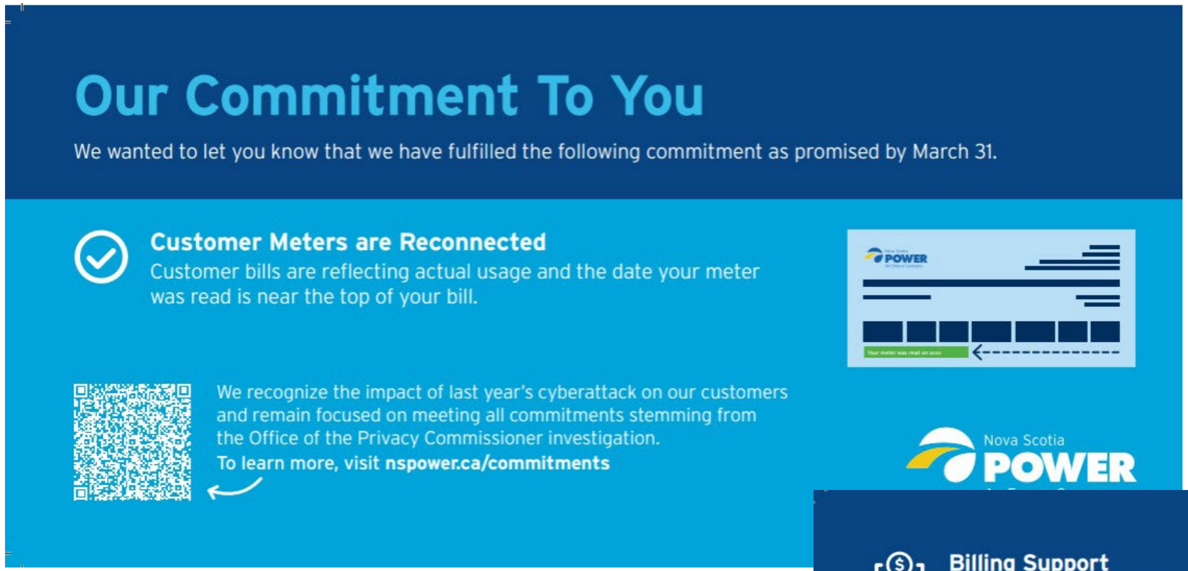
The Nova Scotia Power Team

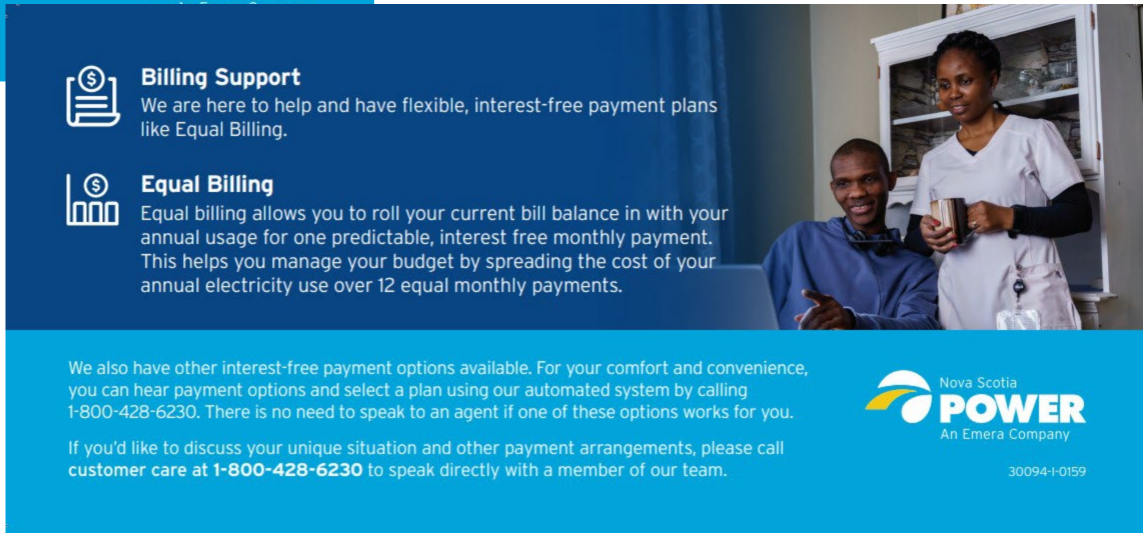
Vivek's commitment letter was added to the February/March bill cycle.

May/June 2026 Bill Insert

Shared update on the billing system restoration and highlighted customer supports like Equal Billing.

Our webpage nspower.ca/billing continues to have the latest information.





July/August 2026 Bill Insert

Provided the advance notice we committed to – and making sure customers are aware of the interest-free payment plans that are available to them to avoid being impacted by the return of late fees October 1st .

Late fees are returning

Now that bills are no longer being estimated and customers have had multiple bills with their actual usage, reintroducing late fees is the next step as we return to normal operations.

We want to let you know ahead of time that **late fees will be returning on October 1st for unpaid balances on your bill**. We have not been charging late fees since April of 2025. Earlier this year we made a commitment to provide notice to our customers in advance of their return to give customers lots of time and flexible options to catch up.

Support remains available for those who may need it, and we are here to help.

Please see the reverse side for customer support options or visit nspower.ca/billing.

30094-I-0161

Nova Scotia POWER
An Emera Company

Customer Support

We understand that everyone's situation is unique and we are here to help with flexible, interest-free payment plans.

- Equal billing allows you to roll your current bill balance in with your annual usage for one predictable, interest-free monthly payment. This helps you manage your budget by spreading the cost of your annual electricity use over 12 equal monthly payments.
- We have other interest-free payment options available. You can explore payment options and select a plan using our automated system by calling 1-800-428-6230. There is no need to speak to an agent if one of these options works for you.

If you'd like to discuss other payment arrangements, **please call Customer Care at 1-800-428-6230** to speak directly with a member of our team.

Nova Scotia POWER
An Emera Company