

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: M12273 Administrative Demand for Structural Redress – NSUARB Oversight Failure and NS Power Identity Breach
Date: May 23, 2025 10:11:33 AM
Attachments: [Administrative Demand for Structural Redress — Identity Breach and Unlawful Contracting Structures Enabled by NSERBT Oversight - 2025-05-22.pdf](#)
[NSERBT Decision – Matter M11099 \(August 2023\).pdf](#)
[Formal Response to NSERBT – May 25 2023.pdf](#)
[Public Letter of Comment – Matter M11411 \(January 29 2024\).pdf](#)
[NSERBT Decision – Matter M11099 \(August 2023\).pdf](#)

From: Nicole Connor [REDACTED]
Sent: May 22, 2025 2:01 PM
To: Executive Council <Executive.Council@novascotia.ca>; Justice Minister <JUSTMIN@novascotia.ca>
Cc: Wallace, Lisa <Lisa.Wallace@novascotia.ca>; Adair, Kim <Kim.Adair@novascotia.ca>
Subject: Administrative Demand for Structural Redress – NSUARB Oversight Failure and NS Power Identity Breach

Some people who received this message don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

To:

Michael Savage acting as Chief Executive Officer of the Province of Nova Scotia

Tim Houston acting as President of the Province of Nova Scotia

Becky Druhan acting as Minister of Justice and Attorney General for the Province of Nova Scotia

Please find attached an **Administrative Demand for Structural Redress** concerning the ongoing use of unconscionable contracting mechanisms by Nova Scotia Power (NS Power), and the resulting governance failures of the Nova Scotia Energy and Regulatory Boards Tribunal (NSERBT) - *formally known as the Nova Scotia Utility and Review Board (NSUARB)*, for which your office holds administrative oversight.

This submission is made in good faith, not as a personal grievance, but as a civic demand for lawful correction. I am in possession of a formal identity breach notification from Nova Scotia Power due to an event that confirms what I previously warned through formal channels: that NS Power's "deemed" contracting model lacks lawful consent and structural integrity, and is materially unsafe.

The attached letter outlines:

- The absence of lawful contract formation under Regulation 2.2
- NSERBT's refusal to correct this despite clear procedural evidence
- The identity breach as confirmation of system-wide administrative failure
- My exhaustion of all internal remedy pathways

This matter now sits squarely within your jurisdiction. I am requesting formal review, structural accountability, and a clear response from the Executive Council Office as the body responsible for the composition and oversight of the NSERBT.

Please confirm receipt of this email and attached demand. Should this communication be misdirected, I request immediate referral to the appropriate authority.

Respectfully,
Nicole Connor

Without prejudice. All rights reserved.

Cc:

Lisa Wallace acting as Chief Clerk of the Nova Scotia Energy and Regulatory Boards Tribunal

Kim Adair acting as Auditor General for the Office of the Auditor General of Nova Scotia

Email constitutes delivery per: [cf] Leoppky v. Meston, 2008 ABQB 45 (CanLII), <<https://canlii.ca/t/1vgsq>>, retrieved on 2025-05-22

ADMINISTRATIVE DEMAND FOR STRUCTURAL REDRESS

25 May 2023

To: Michael Savage acting as Chief Executive Officer of the Province of Nova Scotia
Tim Houston acting as President of the Province of Nova Scotia
Becky Druhan acting as Minister of Justice and Attorney General for the Province of Nova Scotia

Subject: Administrative Demand for Structural Redress — Identity Breach and Unlawful Contracting Structures Enabled by NSERBT Oversight

I am a resident of Nova Scotia who has undertaken a thorough examination of the structural failures governing the province's regulatory and contractual relationship with Nova Scotia Power (NS Power). I am in possession of a formal identity breach notification issued by NS Power. This breach did not occur in isolation. It appears to be the direct result of systemic governance failures that I have previously identified and submitted through multiple administrative channels.

This letter constitutes a formal administrative demand for investigation, oversight correction, and structural redress. I do not hold a personal contract with NS Power. I am not seeking personal remedy. I am evidencing, through this breach, that unlawful and unconscionable contracting mechanisms approved and upheld by the Nova Scotia Energy and Regulatory Boards Tribunal (NSERBT) - *formally known as the Nova Scotia Utility and Review Board (NSUARB)*, have now resulted in material risk to residents of this province.

I submit this demand in good faith, not as a threat or adversarial challenge, but as a necessary act of civic accountability in response to structural conditions that have proven materially unsafe.

Summary of Structural Breakdown

1. Contracts Without Capacity, Consent, or Jurisdiction

NS Power has been permitted to "deem" contractual relationships into existence with residential customers under Board-approved Regulation 2.2. This allows an essential service to be delivered under presumed consent, with no signed agreement, no visible terms at the point of entry, and no clear evidence of jurisdictional authority. Residents are not offered the Regulations, Domestic Tariff, or the option to request a formal contract (as permitted by 2.1) during the application process. There appears to be no opportunity or avenue for lawful contracting.

2. NSERBT Denial of Remedy Despite Structural Invalidity

In Matter M11099, I formally contested these conditions. While the NSERBT acknowledged that the Regulations were not in plain sight and required multiple navigational steps to locate, the Board still upheld the deemed contract as valid. No signed agreement was produced. No record of informed digital acceptance was provided. The Board's position - treating passive access as lawful consent - confirms that the regulatory system is enforcing what appears to be contracts of adhesion in direct contradiction to Canadian legal standards of equity and consent.

3. Identity Breach as Confirmation of Administrative Failure

I am in possession of an identity breach notification issued by NS Power to a customer whose relationship with the company is governed by the same presumed contract structure I contested. This breach is not a personal grievance. It is evidence that NSERBT-approved contracting frameworks appear to be materially incapable of protecting residents. The breach is the predictable consequence of a system that does not secure jurisdiction before it binds, nor demonstrates capacity before it collects. There is no legal authority to hold or transmit sensitive personal information without a valid contract.

4. Administrative Exhaustion and Lack of Remedy

I have pursued structural remedy through formal submissions, appeals, and letters of comment - including my public letter in Matter M11411. At each stage, I have been met with jurisdictional deferral or regulatory minimization. My position is now clear: residents of Nova Scotia appear to be bound to a monopoly utility through structurally invalid contracts, with no ability to negotiate terms, opt out, or receive remedy. The NSERBT appears to have failed in its duty of care, and the Executive Council that oversees its appointments and mandate must now be held accountable.

Demands for Structural Redress

As the public authority responsible for overseeing the composition, mandate, and accountability of the NSERBT, I demand the following:

1. A formal administrative review of the NSERBT's continued enforcement of Regulation 2.2 as lawful contracting authority
2. An investigation into whether residents of Nova Scotia are being unlawfully subrogated into contracts of adhesion with NS Power without informed consent
3. A public disclosure of how the NSERBT monitors, enforces, or assesses fiduciary compliance by monopoly utilities in the absence of signed agreements

4. A moratorium on all rate increase approvals until Nova Scotia Power can demonstrate its contractual relationships are based on informed, express, and lawful consent
5. A clear statement of ministerial responsibility confirming which Office or Department holds direct accountability for regulatory approval and oversight of NS Power's residential contracts

This demand is not ideological. It is lawful. It is not about one resident. It is about a provincial system that appears to have failed to ensure just, equitable, and lawful service delivery in a monopolized sector. Should any assertions be inaccurate, I request formal clarification and evidence to the contrary. Should this demand be misdirected, I expect an immediate referral to the appropriate governing body.

If a full and complete point-by-point response is not received by 12 June 2025, silence, deferral, or failure to intervene will be taken as confirmation of administrative complicity and potential negligence in the ongoing harm enabled by this regulatory structure.

Respectfully, without prejudice and all rights reserved.

Nicole Connor



Cc:

Lisa Wallace acting as Chief Clerk of the Nova Scotia Energy and Regulatory Boards Tribunal

Kim Adair acting as Auditor General for the Office of the Auditor General of Nova Scotia

Enclosed Documentation

1. NSERBT Decision – Matter M11099 (August 2023)
2. Formal Response to NSERBT – May 25, 2023
3. Identity Breach Notification – May 13, 2025
4. Public Letter of Comment – Matter M11411 (January 29, 2024)

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: M12273 FW: NSP Data breach
Date: May 23, 2025 2:55:37 PM

From: Katie Campbell [REDACTED]
Sent: May 23, 2025 2:49 PM
To: Premier <PREMIER@novascotia.ca>; Board, NSUARB <Board@novascotia.ca>; katie campbell [REDACTED]
Subject: NSP Data breach

Some people who received this message don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hello,

I am writing to add my perspective to the ongoing data breach at NSP.

I received a letter informing me that my data was accessed, and am offered a two year subscription to a monitoring service to check for unauthorized activity. This activity has been downloaded to me. And if there is unauthorized activity?? What then??

We have no choice in our use of NSP, and under privatization we have suffered horrendous price increases, service interruptions, and now this. I think it is quite enough.

As you know, the cost of mitigating and repairing the technical aspects as a cost will be downloaded to the voters who are also customers. Where is the fairness? NSP has not maintained upgrades to the grid in an acceptable manner, nor to its data infrastructure.

I am very angry about this as I have no alternatives to NSP. Give us free markets or bring power distribution back in house as a government service.

Respectfully,

K.

Katie Campbell
[REDACTED]

Appeal - NS Power Dispute Resolution Officer (DRO)

Reference Number: 250523001

Submitted on: Friday, May 23 2025 at 03:33:52 PM (ADT)

Contact Information

Name on account: Susan Joudrey

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

DRO made decision on:	May 13 2025
Type of complaint:	Other
Additional details:	My private information was released on the internet. There were no instructions provided by Nova Scotia Power about whether or not I should open a new bank account. I have no idea why NS Power might have collected my social insurance number, and whether I should try and replace my SIN. The notice of the cyber breach came two months after the breach occurred, which isn't a timely manner. This entire incident was handled poorly and has not been sufficiently resolved. The date submitted as a "decision" is the date of the letter I received from Nova Scotia Power. A copy can be provided, if necessary.
How do they want the complaint resolved?	I want more detailed information about the breach including more specific information about my account. For example, if I don't use pre-authorized payments, do I need to worry about my bank information? Or, why would Nova Scotia Power store my social insurance number? And, anyone who had information stolen and released on the internet should receive financial compensation because if customers need to worry about identity theft, they're not receiving adequate service from Nova Scotia Power.
Supporting documents uploaded:	• NS Power letter SJoudrey.pdf



PO Box 910 Halifax,
Nova Scotia B3J 2W5

May 13, 2025

00766-ADPSON 1014 AUTO *138000



Susan Joudrey
[Redacted Address]

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 myTrueIdentity) at no cost to you. Please refer to the attachments included with this notice for additional information about TransUnion myTrueIdentity, 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.



From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: M12273 - FW: NOVA SCOTIANS vs. NOVA SCOTIA POWER
Date: May 26, 2025 9:15:18 AM
Attachments: [May 25.docx](#)

From: Susan Simons [REDACTED]
Sent: May 25, 2025 2:54 PM
To: Premier <PREMIER@novascotia.ca>; Board, NSUARB <Board@novascotia.ca>; PC_Caucus <PCCaucus@novascotia.ca>; Information Privacy Commissioner for Nova Scotia <oipcns@novascotia.ca>
Subject: NOVA SCOTIANS vs. NOVA SCOTIA POWER

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hello,

I have attached a letter regarding the above-noted business.

I am totally disgusted, as are most Nova Scotians with the most recent problems that NSPower has dumped on us.

These current issues have far more serious, far reaching outcomes, than NSP's usual ongoing issues.

In addition to the content of my letter, I wish to add;

I read a copy of the Premiers' Mandate Letter to Nova Scotians, and I cite the following statements:

"It is an honour to serve Nova Scotians as their Premier...A brighter future starts with a shared belief in what our province can do. A belief in each other. A belief in our communities. A belief in fellow Nova Scotians. We can put Nova Scotians on the path to financial sustainability....We have committed to listen to and respect all Nova Scotias."

It appears our Premier has dropped the ball on this, and I submit this written request to ask him to pick up the ball, and start running with it.

I would ask for a response to my email.

May 25, 2025

Sent Via Email

Premier Tim Houston
Office of the NS Privacy Officer

I am writing to formally complain about Nova Scotia Power's handling of its recent security breach.

I am deeply concerned about both the theft of my personal information and Nova Scotia Power's inadequate response to this serious security breach. According to NS Power's letter:

- My personal data was stolen by an authorized third part on or around March 19, 2025.
- Nova Scotia Power discovered this breach on April 25, 2025.
- Nova Scotia Power didn't notify me of the breach or that my information had been stolen until May 22, 2025 – more than two (2) months after the breach, and a month after provincial authorities were made aware of it.

While NS Power's letter acknowledges that my personal information had been stolen by an unauthorized third party, this letter did not meet acceptable standards for breach notification, as follows:

- No specific information relating to my NS Power Personal Profile, nor my personal data stolen. As a victim of NS Power's security breach, and according to the Personal Information Protection and Electronic Documents Act (PIPEDA), I have a legal right to know the full scope of My Personal Data Theft.
- The NS Power letter provided no guidance on what steps to take to protect myself from potential identity theft or fraud resulting from this breach. I contacted the Federal Privacy Commissioner's Office on my own to get this essential information. The NS Power letter provided information to contact a TransUnion office and enroll their services to provide credit reports; given that this company is under the umbrella of Emera, the parent company for NS Power, it appears that NS Power views this unimaginable security breach of over half (1/2) of the population of the Province of Nova Scotia, as a potential additional source of income, whereby Nova Scotia victims would have to pay for continued use of this service. This act alone, on the part of NS Power, affirms their only interest in this massive security breach is to find more ways to take money, from those in this province, who NS Power made victims of.

I hereby request that the Province of Nova Scotia immediately instruct NS Power to provide me with the following:

- 1) A Detailed, Specific Account of exactly what Personal Information of mine was stolen in this security breach;
- 2) A lawful explanation as to the communication delay between discovering the security breach on April 25, 2025, and the communication that I received on May 22, 2025;

.../2

- 3) Provide comprehensive identity protection through a credible provider;
- 4) Provide in writing, a clear acknowledgement that NS Power was the care holder of my Personal and Private information, as they had requested it from me, before they would provide power service to me; and whereby NS Power did not have sufficient security on their website, to withstand a cyberattack, my personal and private information was stolen, along with same of more than 280,000 Nova Scotians; and
- 5) Provide in writing, an explanation as to why Nova Scotians should ever again trust NS Power with their Personal and Private Information? I support the request of this question with the following facts: NS Power gave no thought, nor showed any concern, to Nova Scotians privacy, as clearly evidenced by the extraordinary delay in releasing any information of this security breach to Nova Scotians. That, in itself is a major breach of trust, during an ongoing security breach. Even now, NS Power will not provide the basic NS Power profile information to a customer calling in and requesting same.

I was born in this province and have lived here most of my life; I have always been very proud of home, and I have shared that sentiment with others inside this province, within Canada, and further abroad. This incident has actually sickened me; with all the problems that NS Power has dumped on customers all through the years, lack of infrastructure maintenance which has caused frequent power outages, constant power rate increases in the past 1 ½ years to where at present, Nova Scotians are now struggling to pay power bills and put food on the table in a lot of homes. This past year many NS Power customers have turned down their heat during the winter to try to reduce bills to no avail. Now Nova Scotians know that NS Power also did not maintain proper security on its' website, and did not meet the most basic of security breach requirement – inform impacted customers – quickly. NS Power has put Nova Scotians' in the position of experiencing potential credit theft, potential inability to renew their mortgages due to this theft, and on and on it could go, most likely for the remainder of our lives.

I ask this government if you consider this acceptable? And, if not, I would ask exactly what you plan to do about it.

Sincerely,

Martha Newcombe

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: NOVA SCOTIA POWER - FURTHER COSTLY OUTCOMES TO ALL CANADIANS
Date: May 26, 2025 9:24:14 AM

From: Susan Simons [REDACTED]
Sent: May 25, 2025 5:27 PM
To: Premier <PREMIER@novascotia.ca>; Mark.Carney@parl.gc.ca; Executive Council <Executive.Council@novascotia.ca>; LEGCOMM <LEGCOMM@novascotia.ca>; Board, NSUARB <Board@novascotia.ca>; jessica.fancy-landry@parl.gc.ca
Subject: NOVA SCOTIA POWER - FURTHER COSTLY OUTCOMES TO ALL CANADIANS

Some people who received this message don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

To All Parties,

One of the far reaching devastating potential outcomes from NS Power's security breach, is the leverage that it has now given to scammers and terrorists to steal money from all Canadians tax dollars.

Given that there was over 280,000 Nova Scotians' personal and private information put out there on the dark web, for any criminal to grab and run with, this has created a wide open scope for criminal activity to start and continue for some time. This would result in devastation to both Nova Scotians and Canadians across this country.

During the Pandemic, criminals were stealing personal and private information from Canadians and creating new accounts from that information. This led to CRA sending out \$Millions of Canadians' tax dollars to deceased people, as well as new accounts from innocent Canadians who had their information stolen. That money for obvious reasons will never be collected or returned. All Canadians, and all levels of government in Canada, should be concerned about the potential for these criminal acts being repeated, on a much larger scale, as a result of NS Powers' security breach.

The provinces of British Columbia, Alberta and Quebec, all have privacy legislation for organizations operating in the private sector. Nova Scotia, my birthplace, does not. WHY NOT? would be the burning question. Nova Scotians have a right to be protected from non-public service companies who exhibit low standards of security. I will quantify the definition of "low standards of security", with the following facts: 1) NS Power did not maintain it's

infrastructure for years, which finally led to the breakdown of same, and the constant and continuous power outages that we experience; 2) NSPower has failed its' Service Standards for years, and does not appear to care about it, other than to try and get the Standards definition lowered; so it is not a surprise to most Nova Scotians, that they did not maintain their security on their website either. The Federal Government of Canada has a Federal Privacy Commission for federal public services, and the Provincial Government has a Provincial Privacy Commission for provincial public services, yet, for a service as critical as power, there is no privacy legislation for private sector companies, and again, the question is Why Not?

In the fall of 2024, Nova Scotia Power had secured the full \$500-million loan guarantee from Ottawa that was on the table to bail the utility out of a precarious financial situation and prevent a massive rate hike for its customers. Well, that didn't work so well, because Nova Scotians were hit with 3 increases from 2024 to 2025 - as a result of these continued increases, there are at present, Nova Scotians in this province cutting back on food to pay utility bills; cutting back on heat during the winter to pay utility bills, and still the outrageous bills come from NS Power.

It would appear that given, the CEO of NS Power receives an annual salary of \$1.73 million, and their 1st priority is their investors, it's self-explanatory why Nova Scotians do not receive proper service for the outrageous power bills put upon them.

I have 2 questions here:

1. To the Premier of Nova Scotia, Mr. Houston - when can Nova Scotians expect the tabling of "privacy legislation for private companies" to be discussed in the NS Legislature? and,
2. To the Prime Minister of Canada, Mr. Carney - what protections have been put in place in the federal government to reassure Canadian Taxpayers that the fiasco of the Pandemic lost \$Millions will not be repeated, given the NS Power security breach?

A reply is requested and sincerely would be appreciated, by both levels of government to both questions.

Thank you.

General Complaint - NS Power and municipal electric utilities

Reference Number: 250525001

Submitted on: Sunday, May 25 2025 at 02:05:42 PM (ADT)

Contact Information

Name on account: [REDACTED]

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

Cyber Security management negligence: I have contacted the NS Energy Board regarding the NS Power cyber security breach on 23 May 25. I noted that on 10 Mar 25 CBC (Blair Rhodes) issued a story that NS Power had requested \$6.8M in cyber security upgrades, surprisingly close to the breach date. 12 CRITICAL sites were identified in NS Energy Board submission Master #12117 request. This document makes abundantly clear how exposed and vulnerable NS Power is to malicious cyber actors. NS Power is VERY aware that it does not have the in-house expertise now (nor has for some substantial time) to manage and monitor remotely critical infrastructure sites and consumer personal information. Approximately 7000 hrs of effort is proposed to accomplish the \$6.8M dollars of Phase 1 (initial) effort to properly protect and monitor critical infra and personal info. In this same document NS Power outlines that this effort required is a CORE SERVICE. Why aren't such Core services BASELINE funded internally, especially considering the present Threat posture and substantial vulnerability? NS Power should not have to seek Regulatory Board approval for an effort that the Public Utility is clearly legally obliged to action to meet Federal standards without delay.

Did they contact the utility? Yes**How did the utility respond?**

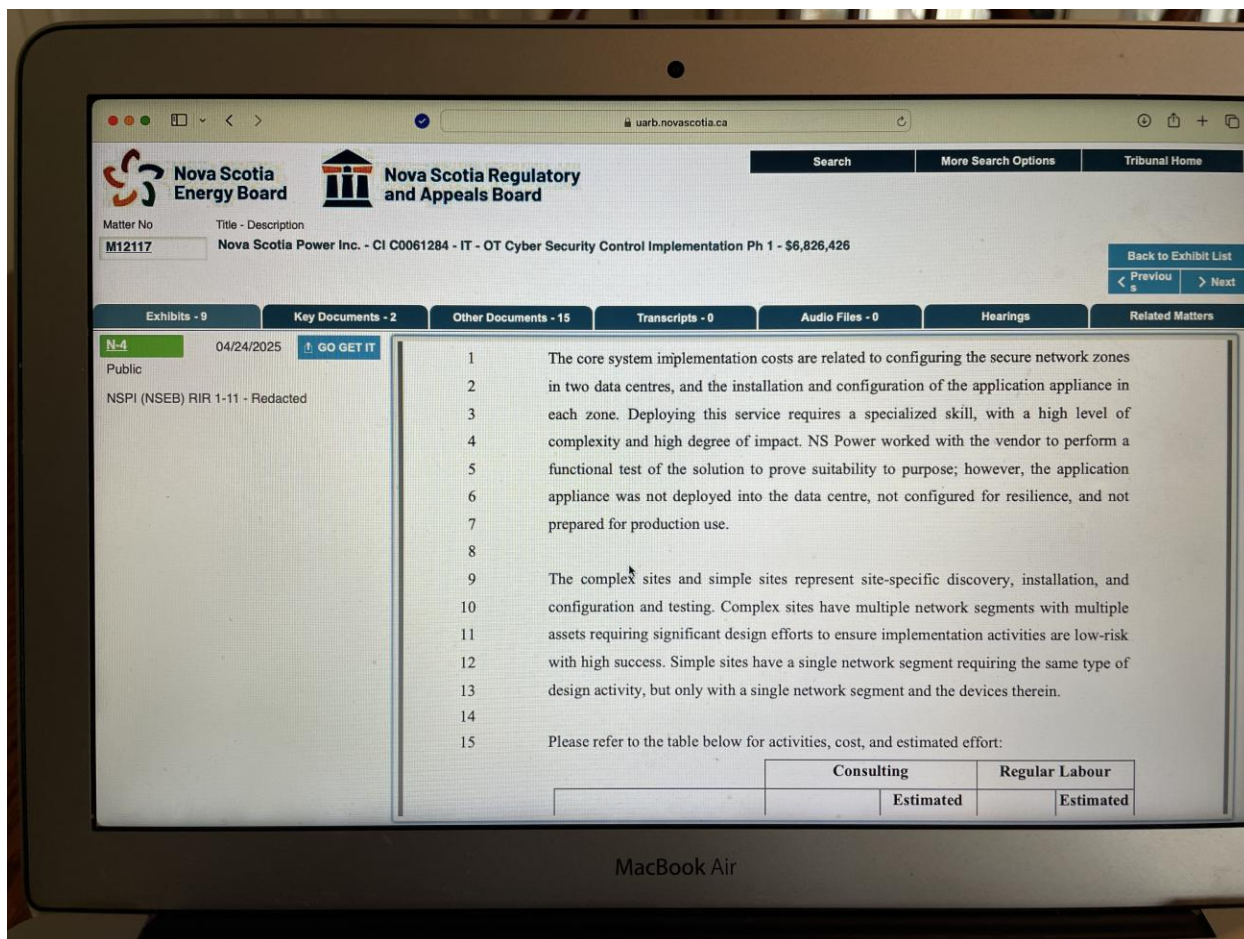
How do they want the complaint resolved?

I expect PROMPT action from the NS Energy Board on this ongoing cyber threat. The fact that the NS Energy Board continued to pursue a standard 90 day review period without triaging and expediting this project approval has made you complicit and put me and other consumers at substantial risk. You need to seriously look closely at HOW you assess and review incoming submissions for their risk and act accordingly. Further, why wasn't NS Power expected to self-fund this CORE service and not delay further considering the inherent risk? Does NS Power not have contingency money to act in high risk circumstances? Could a Special Board have been convened, once the risk to consumers was quickly acknowledged, to give NS Power quick approval in this unique instance? I expect in the interim for NS Power to expeditiously self-fund this critical cyber security (software and hardware) 7000 hour effort that it is accountable for as a Core Service to Nova Scotians. Realize that there are still two other additional phases of vulnerability that are beyond the 12 initial critical NS Power sites affected.

You have the opportunity NOW to get these defined by NS Power formally without delay and get the project MOVING! NS Power's negligence by NOT making cyber security vulnerabilities a priority has resulted in mine and 280,000 other Nova Scotians vital credit information to be stolen and sold on the Dark Web. My financial vulnerability was wholly avoidable if NS Power had acted much earlier knowing what they knew. 2 years of free credit monitoring does not prevent my data being used at any time thereafter. I expect much more from the NS Energy Board in assessing submissions and protecting consumers. I expect further formal discussion with the NS Energy Board as this progresses. This will be escalated.

Supporting documents uploaded:

- IMG_2619.JPG
- IMG_2620.JPG
- IMG_2621.JPG
- IMG_2618.JPG



Nova Scotia
Energy Board



Nova Scotia Regulatory
and Appeals Board

Search

More Search Options

Tribunal Home

Matter No

Title - Description

M12117

Nova Scotia Power Inc. - CI C0061284 - IT - OT Cyber Security Control Implementation Ph 1 - \$6,826,426

Back to Exhibit List

Previous

Next

Exhibits - 9

Key Documents - 2

Other Documents - 15

Transcripts - 0

Audio Files - 0

Hearings

Related Matters

N-4

04/24/2025

GO GET IT

Public

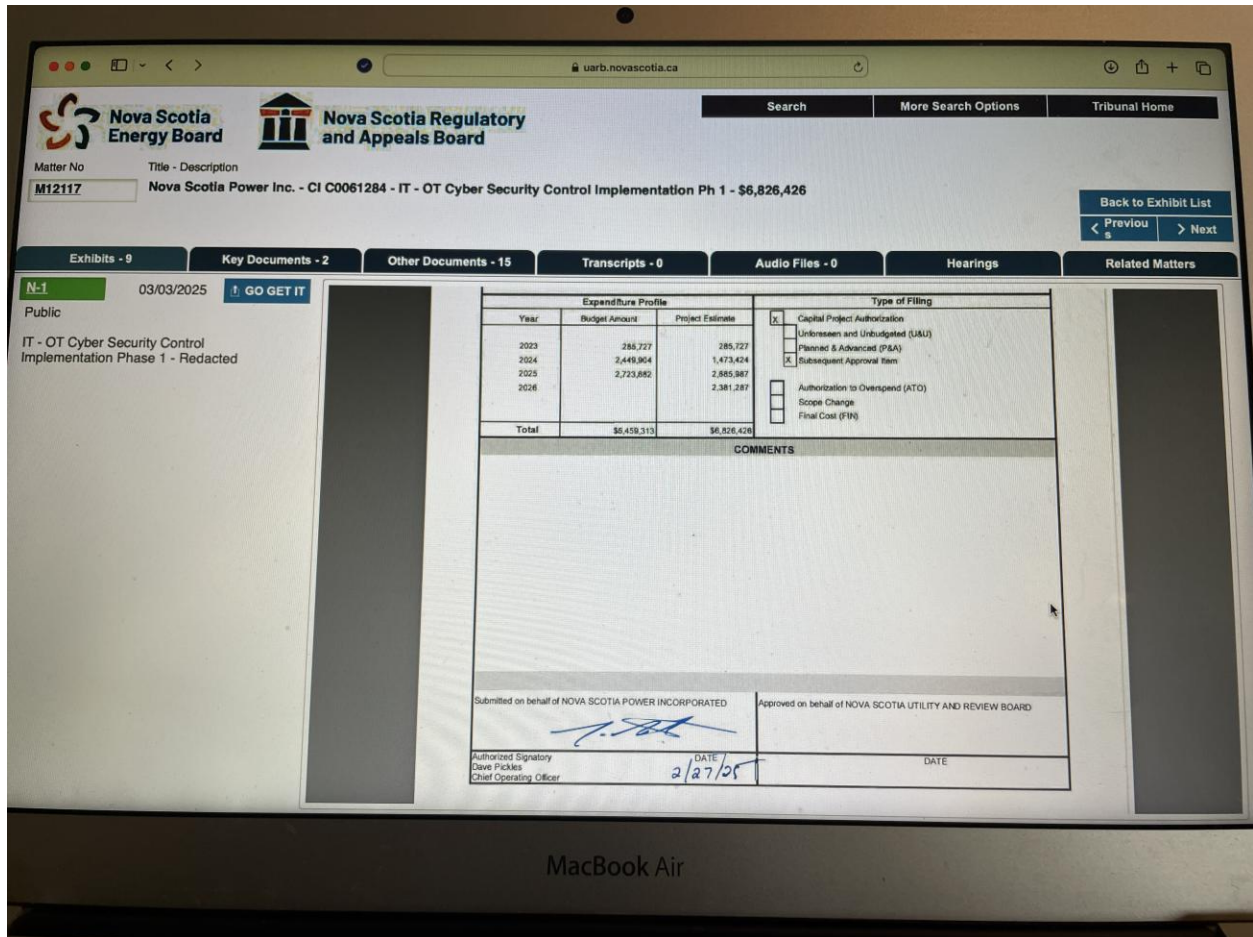
NSPI (NSEB) RIR 1-11 - Redacted

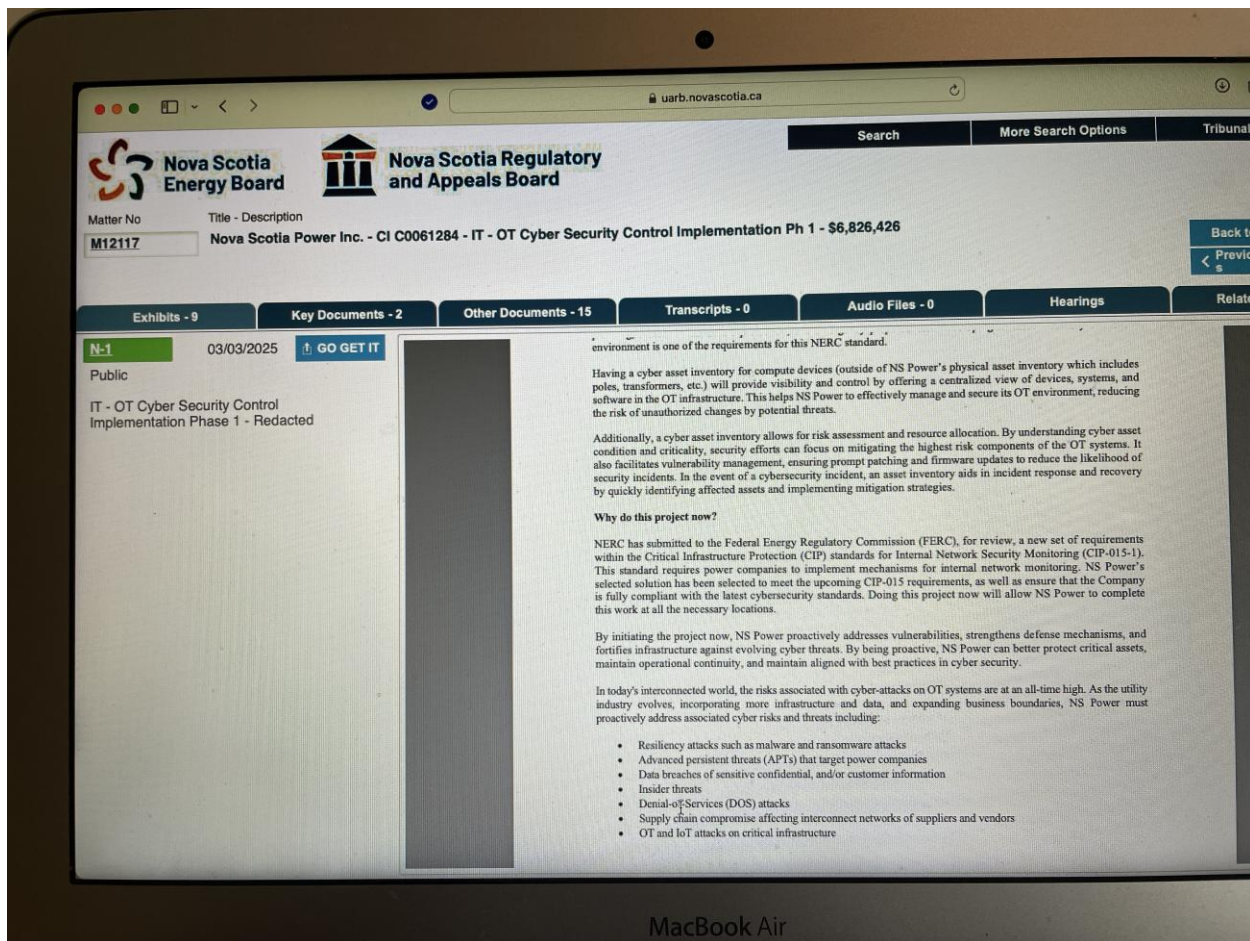
1 The core system implementation costs are related to configuring the secure network zones
2 in two data centres, and the installation and configuration of the application appliance in
3 each zone. Deploying this service requires a specialized skill, with a high level of
4 complexity and high degree of impact. NS Power worked with the vendor to perform a
5 functional test of the solution to prove suitability to purpose; however, the application
6 appliance was not deployed into the data centre, not configured for resilience, and not
7 prepared for production use.

9 The complex sites and simple sites represent site-specific discovery, installation, and
10 configuration and testing. Complex sites have multiple network segments with multiple
11 assets requiring significant design efforts to ensure implementation activities are low-risk
12 with high success. Simple sites have a single network segment requiring the same type of
13 design activity, but only with a single network segment and the devices therein.

15 Please refer to the table below for activities, cost, and estimated effort:

Consulting		Regular Labour	
	Estimated		Estimated





From: [Allan Cardinal](#)
To: [Henwood, Crystal D](#)
Cc: peter.gregg@nspower.ca
Subject: NS Power breach
Date: May 25, 2025 10:32:46 AM

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hello,

I understand that the NS energy board is investigating the NSP response to the breach that occurred. Perhaps the investigation should include the fact that those of us who received a letter to sign up for credit monitoring includes an activation code that does not work. Not only did NSP fail its customers and breached our privacy they are failing in the response and support to those who were affected. This is a serious issue not to be taken lightly yet NSP does not seem to care, instead sending out fake activation codes. I do hope that the board seriously investigates the lack of and misleading response by NSP in this matter.

Allan Cardinal

From: [Allan Cardinal](#)
To: Info@trevorboudreau.ca; [Henwood, Crystal D](#)
Subject: Ns power
Date: May 25, 2025 1:19:20 PM

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hello

I understand that your department will be investigating the NS power privacy breach and NSP response.

I received a letter from NSP that i was one of the affected. The only thing that nsp is doing in respect to us the clients who were affected is to sign up for credit monitoring. The link they provided in the letter did not work. The second link allowed me to start the process but then stopped saying my email cannot be used. This email has been used by me for 20+ years and has never been compromised, until now. Peter Gregg, president of nsp has publicly stated that they will support those affected, well where are they now. Their offices are closed and no support is being offered. If nsp took this situation seriously they would have a dedicated response team to address the concerns and issues clients like me are facing, even during weekends, but no. All talk and no action. I do hope your department takes a long hard look at this serious issue and lack of support/concern from nsp as thus is completely unacceptable.

Allan Cardinal

[REDACTED]

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Privacy Complaint Regarding NS Power Data Breach and Use of Insecure Remedy Platform
Date: May 26, 2025 10:10:54 AM
Attachments: [NS Power Privacy Complaint YungYu Yeh.pdf](#)
[Executive Summary Security Risks of Entering Credit Card Information on mytrueidentity.ca from MengCheng Yeh.pdf](#)
[SecurityHeaders_Grade_A_With_Warnings.pdf](#)
[Raw-Headers_CSP_UnsafeEval_Inline.pdf](#)
[Mozilla_Observatory_Grade_C.pdf](#)
[Raw-Headers_Missing_Policies.pdf](#)
[Obfuscated_JS_Snippet.pdf](#)
[Missing-Headers_Summary.pdf](#)
[Footer_2019_Timestamp.pdf](#)

From: Jame Y [REDACTED]
Sent: May 26, 2025 7:06 AM
To: access@novascotia.ca; home@nspowert.ca; nspdputeresolution@gmail.com; chief.privacy.officer@equifax.com; gbscanada@equifax.com; Board, NSUARB
<Board@novascotia.ca>
Cc: [REDACTED]
Subject: Privacy Complaint Regarding NS Power Data Breach and Use of Insecure Remedy Platform

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Dear Office of the Information and Privacy Commissioner,

I am submitting a formal privacy complaint concerning the recent data breach at Nova Scotia Power, and the subsequent recommendation of the mytrueidentity.ca website as a remedy platform for affected individuals.

Attached, you will find:

1. A formal complaint letter outlining the incident, technical analysis, and risks posed by the remedial platform;
2. An email with evidence from Meng Cheng Yeh. (Meng Cheng Yeh is a formal privacy complaint concerning the recent data breach at Nova Scotia Power, he is also a student specializing in IT Systems Management and Security.)

I believe this matter requires your urgent review, as the provided solution potentially exposes affected individuals to further cyber risks.

If you require any additional information or documentation, I would be happy to provide it.

Sincerely,

YungYu Yeh

[REDACTED]

[REDACTED]

[REDACTED]

Formal Privacy Complaint Letter

To: Office of the Information and Privacy Commissioner for Nova Scotia

Subject: Formal Privacy Complaint Regarding NS Power Data Breach and Insecure Remedial Platform (mytrueidentity.ca)

Dear Commissioner,

My name is YungYu Yeh, A victim of NS power's customer data breach. I am writing to formally file a privacy complaint regarding the recent cyber incident involving Nova Scotia Power, which has resulted in the confirmed leak of my personal data.

While I appreciate that NS Power has offered a form of remedy through the identity protection service "mytrueidentity.ca," I must express deep concern over the significant security flaws discovered on the site.

Based on MengCheng Yeh technical analysis, mytrueidentity.ca does not meet modern security standards for handling sensitive information such as credit card data, SINS, or identity verification materials. Here are the key security issues:

1. Unsafe Content Policies and Headers:

- No proper Content Security Policy (CSP).
- Permissive settings like 'unsafe-inline' and 'unsafe-eval', known to expose users to cross-site scripting (XSS) attacks.
- Missing 'Permissions-Policy' and 'Referrer-Policy' headers.

2. Broken Code and Functionality:

- Numerous 404 and 403 errors affecting JavaScript validation.
- Obsolete or broken jQuery implementations attempting to access non-existent DOM elements.

3. Lack of Proper HTTPS Enforcement:

- The site does not enforce HTTPS redirection, enabling possible man-in-the-middle attacks.

4. Overreliance on Third-Party Scripts:

- Dozens of external scripts are loaded, increasing the potential for third-party exploits.

5. Indications of Neglect:

- Outdated copyright (2019).
- Use of deprecated security practices (e.g., X-XSS-Protection).
- No evidence of recent updates or audits.

Given these findings, I strongly believe that this "remedial" service may further endanger Nova Scotians by subjecting them to additional cyber risks, particularly in the wake of an already serious privacy breach.

I respectfully request that your office investigate:

- The due diligence (or lack thereof) exercised by NS Power in selecting this service provider;
- Whether this solution aligns with industry-standard safeguards as expected under Nova Scotia's privacy laws;
- The potential harm to individuals encouraged to submit sensitive data to this platform.

Thank you for your time and consideration. I am happy to provide technical documentation or evidence upon request.

Sincerely,

YungYu Yeh

A large black rectangular redaction box covering the signature area.

Filed: May 24, 2025

Executive Summary: Security Risks of Entering Credit Card Information on mytrueidentity.ca

2025年5月24日 晚上8:37

收件者: Grace C [REDACTED]

Based on a thorough technical analysis of the mytrueidentity.ca website due to the recent cyber incident impacting Nova Scotia Power, it is not recommended for Nova Scotians—or any users—to input sensitive information such as credit card details on this platform at this time. Multiple indicators suggest the site is outdated, insecure, and poorly maintained, putting users' financial and personal data at unnecessary risk. Key Security Concerns:

Missing or Unsafe Security Headers:

The site lacks a proper Content Security Policy (CSP) and dangerously permits 'unsafe-inline' and 'unsafe-eval' scripts—both are known vectors for cross-site scripting (XSS) attacks.

Missing headers such as Permissions-Policy and Referrer-Policy reduce privacy and increase the risk of data leakage.

Broken JavaScript and 404 Errors:

Critical resources like JavaScript files fail to load (404/403 errors), potentially leading to broken form validation or security checks during credit card submission.

jQuery errors show attempts to interact with missing page elements—an indicator of outdated or untested code.

No Proper HTTP to HTTPS Redirection:

The site does not force HTTPS redirection, leaving open the possibility for man-in-the-middle attacks if users mistakenly access it over HTTP.

Overloaded and Permissive Third-Party Dependencies

The site loads scripts from dozens of external domains, increasing the attack surface and potential for third-party compromise.

Stale Copyright and Obsolete Practices:

Copyright footer dates back to 2019, suggesting a lack of ongoing maintenance or security review.

Use of deprecated practices like X-XSS-Protection and reliance on legacy JavaScript libraries further confirms this.

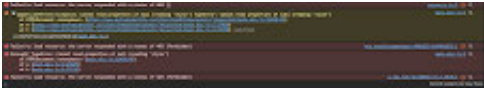
Conclusion:

mytrueidentity.ca does not meet modern web security standards for handling sensitive financial information. Until critical security policies, headers, and coding practices are addressed, entering credit

card data into this site exposes users to unnecessary cyber risks. It is strongly advised that Nova Scotian residents avoid submitting any payment or personal information on the platform.

Meng Cheng Yeh
IT Systems Management and Security Student
[REDACTED]

8 個附件



Console_Errors_And_403_404.png
58K



Missing_Headers_Summary.png
65K



Obfuscated_JS_Snippet.png
239K



Footer_2019_Timestamp.png
34K



Mozilla_Observatory_Grade_C.png
114K



Raw-Headers_Missing-Policies.png
249K



Raw-Headers_CSP_UnsafeEval_Inline.png
168K



SecurityHeaders_Grade_A_With_Warnings.png
70K

Security Report Summary



Site: https://www.mytrueidentity.ca/CreditView/welcome_page?enterprise=mytrueidca

IP Address: 104.18.39.171

Report Time: 24 May 2025 23:11:15 UTC

Headers:

✓ X-Frame-Options

✓ Content-Security-Policy

✓ X-Content-Type-Options

✓ Strict-Transport-Security

✗ Referrer-Policy

✗ Permissions-Policy

Warning: Grade capped at A, please see warnings below.

Advanced: Great grade! Perform a deeper security analysis of your website and APIs:

[Try Now](#)

Missing Headers

Referrer-Policy

[Referrer Policy](#) is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

Permissions-Policy

[Permissions Policy](#) is a new header that allows a site to control which features and APIs can be used in the browser.

Warnings

Content-Security-Policy

This policy contains 'unsafe-eval' which is dangerous in the style-src directive. This policy contains 'unsafe-inline' which is dangerous in the script-src directive. This policy contains 'unsafe-eval' which is dangerous in the script-src directive.

Raw Headers

HTTP/2	200
date	Sat, 24 May 2025 23:11:15 GMT
content-type	text/html; charset=UTF-8
x-xss-protection	1; mode=block
x-frame-options	SAMEORIGIN
default-src	'self' blob: *.kampyle.com *.medallia.com http://notify.bluecoat.com/ https://oap7.sprintpcs.com http://oap7.sprintpcs.com https://device.payfone.com:4443 http://device.payfone.com https://auth.swcs.verizon.com:22790 maps.googleapis.com *.iovation.com scripts.neuro-id.com https://cdn.inpwrd.net *.iesnare.com *.adsafeprotected.com l.betrad.com c.evidon.com smartasset.com cdn-assets-prod.s3.amazonaws.com *.lpsnmedia.net *.liveperson.net stats.g.doubleclick.net omns.americanexpress.com nexus.ensighten.com r.3gl.net aerest.tui.transunion.com *.google-analytics.com g.3gl.net *.googletagmanager.com icm.aexp-static.com aeresource.tui.transunion.com *.aexp-static.com *.americanexpress.com *.qualtrics.com *.transunion.com *.truelink.com *.trustev.com *.entrust.net *.googlesyndication.com *.junametrics.com *.bluecoat.com *.mpsnaresnare.com mpsnaresnare.com rules.quantcount.com sp.analytics.yahoo.com *.google.ca adservice.google.ca *.quantcount.com *.yahoo.com *.amazon.adsystem.com *.visualwebsiteoptimizer.com *.brightcove.com *.brightcovedn.cloudfront.net *.prodboitdns.net *.adobedtm.com *.force.com *.my.salesforce.com *.doubleclick.net frame-src 'self' *.kampyle.com *.medallia.com http://notify.bluecoat.com/ *.iovation.com *.adobedtm.com *.iesnare.com *.adsafeprotected.com l.betrad.com c.evidon.com *.evenfinancial.com aexp.demdex.net cdn-assets-prod.s3.amazonaws.com *.lpsnmedia.net *.liveperson.net stats.g.doubleclick.net omns.americanexpress.com nexus.ensighten.com r.3gl.net aerest.tui.transunion.com *.google-analytics.com g.3gl.net *.googletagmanager.com icm.aexp-static.com aeresource.tui.transunion.com *.aexp-static.com *.americanexpress.com *.qualtrics.com *.chase.creditviewdashboard.com *.creditviewdashboard.com *.mycredguide.americanexpress.com membership.trueidentity.com membership.tui.transunion.com *.amazon-adssystem.com *.amazon.adssystem.com smartasset.com *.transunion.com *.truelink.com *.doubleclick.net *.qnsr.com *.trustev.com *.mediaplex.com *.credit.com *.go2cloud.org *.googlesyndication.com *.cordlessmedia.go2cloud.org *.bluecoat.com *.facebook.com usbank.demdex.net *.google.ca adservice.google.ca sp.analytics.yahoo.com rules.quantcount.com *.quantcount.com *.yahoo.com *.amazon.adsystem.com *.google.com *.googletagservices.com transunion.ifgza3.net *.brightcove.net *.force.com *.my.salesforce.com https://directnstrk.com https://insight.adsrvr.org/ https://screencapture.kampyle.com https://nebula-cdn.kampyle.com https://resources.digital-cloud-west.medallia.com identity-force.svj.io canada.pxfl.io https://transunion.demdex.net https://p.leads.tv https://ledge.leads.tv connect-src 'self' wss: https://*.g.doubleclick.net https://*.googletagmanager.com https://*.analytics.google.com https://*.google-analytics.com *.kampyle.com *.medallia.com http://hotify.bluecoat.com/ maps.googleapis.com mpsnaresnare.com *.adobedtm.com *.iovation.com receiverneuroid.cloud *.iesnare.com *.sundaysky.com x.bidswitch.net tags.srv.stackadapt.com *.taboola.com dev.visualwebsiteoptimizer.com *.google.ca aetracking.tuciservices.com *.evenfinancial.com click.linksynergy.com cdn-assets-prod.s3.amazonaws.com *.mpsnaresnare.com *.lpsnmedia.net *.liveperson.net stats.g.doubleclick.net omns.americanexpress.com nexus.ensighten.com r.3gl.net aerest.tui.transunion.com g.3gl.net icm.aexp-static.com aeresource.tui.transunion.com *.aexp-static.com *.qualtrics.com *.mytrueidentity.com mpsnaresnare.com *.mycredguide.americanexpress.com *.americanexpress.com members.transunion.ca translate.googleapis.com *.creditviewdashboard.com offers.creditviewdashboard.com smartasset.com smetrics.usbank.com *.transunion.com *.truelink.com *.quinstreet.com *.nextinsure.com *.shrinktapi.com *.surehits.com *.demdex.net dr5dyrnrxhdzh.cloudfront.net *.3gl.net *.smartasset.com api.mixpanel.com *.smrtLas.cdn.mxpnl.com *.google-analytics.com *.doubleclick.net *.facebook.net *.myfonts.net *.scorecardresearch.com *.voicefive.com *.chase.com *.googletagservices.com *.googletagmanager.com *.qnsr.com *.trustev.com *.bing.com *.google.com *.gstatic.com *.facebook.com *.smartasset.com smetrics.sdcvisil.com adservice.google.ca sp.analytics.yahoo.com rules.quantcount.com *.quantcount.com *.yahoo.com *.amazon.adssystem.com transunion.ifgza3.net pagead2.googlesyndication.com *.brightcovedn.com *.brightcove.com manifest.prod.boitdns.net *.force.com *.my.salesforce.com https://cm.leads.tv https://l.leads.tv https://pixelconnector.pixeltracker.co https://pixelconnector.pixeltracker.co https://resources.digital-cloud-west.medallia.com https://ubt-lb.digital-cloud-west.medallia.com https://sbt-prod.kampyle.com https://nebula-cdn.kampyle.com https://udc-neb.kampyle.com *.tl.omtrdc.net https://d2hrivdxn8eknb.cloudfront.net https://d1lu3pmaz2lpx.cloudfront.net https://dvqigh9b7wa32.cloudfront.net https://d330aiyyva2oww.cloudfront.net identity-force.svj.io canada.pxfl.io https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com https://*.g.doubleclick.net https://api.company-target.com https://transunionprod.1122o7.net style-src 'self' 'unsafe-eval' 'unsafe-inline' *.kampyle.com *.medallia.com https://www.gstatic.com/ http://hotify.bluecoat.com/ *.cloudfront.net *.adsafeprotected.com l.betrad.com c.evidon.com *.google.ca cdn-assets-prod.s3.amazonaws.com *.lpsnmedia.net *.liveperson.net stats.g.doubleclick.net omns.americanexpress.com nexus.ensighten.com r.3gl.net aerest.tui.transunion.com *.google-analytics.com g.3gl.net *.googletagmanager.com icm.aexp-static.com aeresource.tui.transunion.com *.aexp-static.com *.americanexpress.com membership.tui.transunion.com membership.trueidentity.com *.chase.creditviewdashboard.com *.transunion.com *.truelink.com 'unsafe-inline' *.myfonts.net *.googleapis.com *.bing.com *.google.com *.trustev.com adservice.google.ca sp.analytics.yahoo.com rules.quantcount.com *.quantcount.com *.yahoo.com *.amazon.adssystem.com *.force.com *.my.salesforce.com *.doubleclick.net https://resources.digital-cloud-west.medallia.com https://screenaptue-cdn.kampyle.com https://nebula-cdn.kampyle.com script-src 'self' blob: https://*.googletagmanager.com http://pixel.admedia.com *.kampyle.com *.medallia.com https://static.cdn-apple.com/ http://notify.bluecoat.com/ https://myjobhelper.advertserve.com maps.googleapis.com *.iovation.com scripts.neuro-id.com https://cdn.inpwrd.net *.adobedtm.com *.iesnare.com *.adsafeprotected.com l.betrad.com c.evidon.com play.sundaysky.com tags.srv.stackadapt.com *.taboola.com aetracking.tuciservices.com *.google.ca secure.rspcdn.com www.rsprack.com *.evenfinancial.com cdn-assets-prod.s3.amazonaws.com *.amazonsaws.com rules.quantcount.com sp.analytics.yahoo.com *.lpsnmedia.net *.liveperson.net stats.g.doubleclick.net omns.americanexpress.com r.3gl.net aerest.tui.transunion.com g.3gl.net icm.aexp-static.com aeresource.tui.transunion.com *.aexp-static.com *.pulseinsights.com *.qualtrics.com *.mytrueidentity.com *.mycredguide.americanexpress.com *.dashlane.com *.creditviewdashboard.com *.creditprofile.transunion.ca secure.truecredit.com mycredguide.amerianexpress.com membership.trueidentity.com members.transunion.ca *.chase.creditviewdashboard.com 'unsafe-eval' 'unsafe-inline' *.yahoo.com *.quantcount.com *.americanexpress.com mpsnaresnare.com dpn.demdex.net adservice.google.ca *.transunion.com *.truelink.com *.entrust.net *.pulseinsights.com *.doubleclick.net *.bing.com *.3gl.net *.ycurscoreonline.com *.gofreecredit.com *.creditcheckingtoday.com *.naturaltracking.com *.credit.com *.facebook.com *.entrust.net *.pulseinsights.com *.quantserve.com *.ymg.com *.ensighten.com *.d39se0hzufakd.cloudfront.net/js/tu.js *.adsprotection.com *.quinstreet.com *.nextinsure.com nexus.ensighten.com smetrics.usbank.com metrics.usbank.com cas.cluep.com *.trustev.com cdn.mxpnl.com *.myfonts.net *.scorecardresearch.com *.voicefive.com adfarm.mediaplex.com *.dotomi.com *.chase.com *.googletagservices.com *.qnsr.com *.googleapis.com tagmanager.google.com *.google.com *.transunion.ca connect.facebook.net amplify.outbrain.com *.trustev.com *.img-cdn.mediaplex.com *.gstatic.com *.googleadtagger.com *.google-analytics.com *.googleadservices.com *.bing.com *.3gl.net *.creditcheckinotoday.com *.googleadservices.com *.googleadtagger.com *.ethio io
content-security-policy	

Scan summary: www.mytrueidentity.ca



Score: 50 / 100
Scan Time: 4 minutes ago
Tests Passed: 7 / 10

Rescan

[Scan another website](#)

Scan results

Scoring CSP analysis Cookies Raw server headers Scan history Benchmark comparison

Test	Score	Reason	Recommendation
Content Security Policy (CSP)	-25	Content Security Policy (CSP) header not implemented	Implement one, see MDN's Content Security Policy (CSP) documentation .
Cookies	0*	All cookies use the <code>secure</code> flag, session cookies use the <code>HttpOnly</code> flag, and cross-origin restrictions are in place via the <code>SameSite</code> flag.	None
Cross Origin Resource Sharing (CORS)	0	Content is not visible via cross-origin resource sharing (CORS) files or headers.	None
Redirection	-20	Does not redirect to an HTTPS site.	Redirect to the same host on HTTPS first, then redirect to the final host on HTTPS.
Referrer Policy	0*	<code>Referrer-Policy</code> header set to <code>no-referrer</code> , <code>same-origin</code> , <code>strict-origin</code> or <code>strict-origin-when-cross-origin</code> .	None
Strict Transport Security (HSTS)	0	<code>Strict-Transport-Security</code> header set to a minimum of six months (15768000).	Consider preloading: this requires adding the <code>preload</code> and <code>includeSubDomains</code> directives and setting <code>max-age</code> to at least <code>31536000</code> (1 year), and submitting your site to https://hstspreload.org/ .
Subresource Integrity	-	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin.	Add SRI for bonus points.
X-Content-Type-Options	-5	<code>X-Content-Type-Options</code> header not implemented.	Set to <code>nosniff</code> .
X-Frame-Options	0	<code>X-Frame-Options</code> (XFO) header set to <code>SAMEORIGIN</code> or <code>DENY</code> .	Implement frame-ancestors CSP.
Cross Origin Resource Policy	-	Cross Origin Resource Policy (CORP) is not implemented (defaults to <code>cross-origin</code>).	None

content-security-policy

*mytrueidentity.com *mycreditguide.americanexpress.com *.dashlane.com *.creditviewdashboard.com *.creditprofile.transunion.ca
secure.truecredit.com mycreditguide.americanexpress.com membership.trueidentity.com members.transunion.ca *.chase.creditviewdashboard.com
unsafe-eval unsafe-inline *.yahoo.com *.quantcount.com *.americanexpress.com mpsnare.iesnare.com dpm.demdex.net adservice.google.ca
*.transunion.com *.trueink.com *.entrust.net *.pulseinsights.com *.doubleclick.net *.bing.com *.sgi.net *.yourscoreonline.com *.gotfreecredit.com
*.creditcheckingtoday.com *.naturaltracking.com *.credit.com *.facebook.com *.entrust.net *.pulseinsights.com *.quantserve.com *.yming.com
*.ensighten.com *.d39se0h2uvfakd.cloudfront.net/js/tu.js *.adsprotection.com *.quinstreet.com *.nextinsure.com nexis.ensighten.com
smetrics.usbank.com metrics.usbank.com cas.cluep.com *.trustev.com cdn.mxpri.com *.myfonts.net *.scorecardresearch.com *.voicefive.com
adfarm.mediaplex.com *.dotomi.com *.chase.com *.googletagservices.com *.qnsr.com *.googleapis.com tagmanager.google.com *.google.com
*.transunion.ca connect.facebook.net amplify.outbrain.com *.trustev.com *.img-cdn.mediaplex.com *.gstatic.com *.googletagmanager.com *.google-
analytics.com *.googleadservices.com *.bing.com *.3gl.net *.creditcheckingtoday.com *.googleadservices.com *.googletagservices.com *.ethn.io
*.quora.com ethn.io *.googlesyndication.com smartasset.com *.quantcount.com *.yahoo.com *.amazon.adssystem.com *.visualwebsiteoptimizer.com
d.impactradius-event.com *.brightcove.com *.brightcove.net *.cloudfront.net *.d39se0h2uvfakd.cloudfront.net *.force.com *.my.salesforce.com
*.salesforcelliveagent.com https://p.teads.tv https://tracker.pixeltracker.co https://js.adsrvr.org https://screencapture.kampyle.com
https://screencapture-cdn.kampyle.com https://resources.digital-cloud-west.medallia.com https://sbt-prod.kampyle.com https://nebula-
cdn.kampyle.com https://udc-neb.kampyle.com https://a.snrtrk.net/ https://www.upsellit.com https://utl.impactcdn.com
https://*.googletagmanager.com tags.tiqcdn.com *.usbank.com *.omtrdc.net *.lcomtrdc.net *.demdex.net; img-src 'self' data:
https://*.doubleclick.net https://*.analytics.google.com https://*.googletagmanager.com https://*.google-analytics.com *.kampyle.com
*.medallia.com *.cloudfront.net cdn.wallethub.com goto.eagledata.biz etracking.tucservices.com http://notify.bluecoat.com/
https://auth.svcs.verizon.com:22790 https://oap7.sprintpcs.com http://oap7.sprintpcs.com http://device.payfone.com
https://device.payfone.com:4443 www.dianomi.com *.googleusercontent.com gwmtracking.com https://auth.svcs.verizon.com oap7.sprintpcs.com
device.payfone.com https://affracc.com maps.googleapis.com *.iovation.com *.adobedtm.com *.iesnare.com *.adsafeprotected.com l.betrad.com
c.evidon.com hds.sundaysky.com play.sundaysky.com srv.stackadpt.com x.bidswitch.net pixel.rubiconproject.com rtt-sync.smartadserve.com
i.ladm.com trc.taboola.com *.taboola.com cx.atdmt.com merchant.linksynergy.com adfarm.mediaplex.com cdn-assets-prod.s3.amazonaws.com cdn-
assets-prod.s3.amazonaws.com *.ipsnmedia.net *.liveperson.net stats.g.doubleclick.net omnis.americanexpress.com nexis.ensighten.com *.3gl.net
aeres.tui.transunion.com g.3gl.net icm.aexp-static.com *.aexp-static.com *.pulseinsights.com aeresource.tui.transunion.com
membership.trueidentity.com membership.tui.transunion.com smetrics.usbank.com mycreditguide.americanexpress.com secure.truecredit.com
*.chase.creditviewdashboard.com *.creditprofile.transunion.ca *.creditviewdashboard.com *.secure.truecredit.com *mytrueidentity.com
*.mycreditguide.americanexpress.com *.americanexpress.com members.transunion.ca translate.googleapis.com adservice.google.ca
offer.creditviewdashboard.com adfarm.mediaplex.com *.demdex.net *.transunion.com *.trueink.com *.e-tui.transunion.com *.entrust.net
*.pulseinsights.com *.convertro.com *.krxd.net *.surehits.com *.capitalone.com *.creditcheckingtoday.com *.domdex.com *.doubleclick.net
*.ensighten.com *.facebook.com *.fastclick.net *.gotfreecredit.com *.googleadservices.com *.google-analytics.com *.gstatic.com *.iclicktracker.com
*.media6degrees.com *.msn.com *.naturaltracking.com *.outbrain.com *.quantserve.com *.trkot.cake.adz.net *.tubemogul.com *.turn.com
*.yahoo.com *.yming.com *.yourscoreonline.com *.googletagservices.com hqx-qmp.quinstreet.com imageserver.quinstreet.com *.ricdn.com
cas.cluep.com *.trustev.com dr5dymisxhdzh.cloudfront.net *.smrCas *.smartasset.com img.mediaplex.com secure.img-cdn.mediaplex.com
*.chase.com *.bing.com *.google.com *.transunion.ca *.adnxs.com *.googletagmanager.com *.emjcd.com *.3gl.net *.admarketplace.net
*.adsprotection.com *.adstrackmobile.go2cloud.org *.advertising.com *.amazon.adssystem.com *.commissionsoup.com *.credit.com *.e-
tui.transunion.com *.googletagservices.com *.acl2.net *.go2cloud.org *.emjcd.com *.quora.com *.ethn.io *.adstrck.com *.dotomi.com *.android.com
*.qnsr.com *.nextinsure.com *.serving-sys.com *.nextinsure.com *.bluecoat.com *.googlesyndication.com *.nextinsure.com *.everesttech.net
*.google.ca sp.analytics.yahoo.com rules.quantcount.com *.quantcount.com *.yahoo.com *.amazon.adssystem.com *.qualtrics.com
*.visualwebsiteoptimizer.com transunion.ifgza3.net www.ojrq.net tapestry.tapad.com logs-01.loggly.com idsync.ricdn.com *.evenfinacial.com
*.visualforce.com *.my.salesforce.com cfstatic.efddevhub.info https://l.teads.tv https://l.teads.tv https://screencapture-cdn.kampyle.com
https://resources.digital-cloud-west.medallia.com https://udc-neb.kampyle.com https://nebula-cdn.kampyle.com https://insight.adsrvr.org https://aff-
tag.evenfinacial.com https://s3.amazonaws.com/images.evenfinacial.com ad.doubleclick.com identity-force.sly.io canada.pxf.io
https://www.ojrq.net https://tapestry.tapad.com https://logs-01.loggly.com https://idsync.ricdn.com https://*.google-analytics.com
https://*.googletagmanager.com https://*.analytics.google.com https://*.g.doubleclick.net https://transunionprod.112.2o7.net
https://cm.teads.tv/v3/conversion https://nextinsure.com https://trkn.us; font-src 'self' data: *.kampyle.com *.medallia.com
http://notify.bluecoat.com/ *.cloudfront.net maps.googleapis.com *.iovation.com *.adobedtm.com *.iesnare.com *.adsafeprotected.com
l.betrad.com c.evidon.com *.google.ca cdn-assets-prod.s3.amazonaws.com *.ipsnmedia.net *.liveperson.net stats.g.doubleclick.net
omnis.americanexpress.com nexis.ensighten.com *.3gl.net aeres.tui.transunion.com *.google-analytics.com g.3gl.net *.googletagmanager.com
icm.aexp-static.com aeresource.tui.transunion.com *.creditviewdashboard.com *.creditprofile.transunion.ca *.chase.creditviewdashboard.com
*.secure.truecredit.com secure.truecredit.com mycreditguide.americanexpress.com membership.tui.transunion.com membership.trueidentity.com
fonts.googleapis.com *.mytrueidentity.com *.mycreditguide.americanexpress.com *.americanexpress.com members.transunion.ca
translate.googleapis.com *.aexp-static.com *.transunion.com *.trueink.com *.gstatic.com adservice.google.ca sp.analytics.yahoo.com
rules.quantcount.com *.quantcount.com *.yahoo.com *.amazon.adssystem.com *.doubleclick.net https://resources.digital-cloud-west.medallia.com
https://nebula-cdn.kampyle.com *.nextinsure.com; media-src 'self' blob: data: http://notify.bluecoat.com/ maps.googleapis.com *.iovation.com
*.adobedtm.com *.iesnare.com *.ipsnmedia.net *.liveperson.net *.adsafeprotected.com l.betrad.com c.evidon.com *.web.sundaysky.com
hds.sundaysky.com mpsnare.iesnare.com *.google.ca adservice.google.ca stats.g.doubleclick.net sp.analytics.yahoo.com rules.quantcount.com
*.quantcount.com *.yahoo.com *.amazon.adssystem.com *.brightcove.com *.brightcovecdn.com *.prod.boltdns.net *.transunion.com blob:
fl.media.brightcove.com *.doubleclick.net; child-src 'self' *.brightcove.net *.transunion.com https://directnstrk.com

x-content-type-options	nosniff
set-cookie	Enterprise=mytrueidca; path=/; secure; HttpOnly; Max-Age=2147483647; Expires=Fri, 12-Jun-2093 02:25:22 GMT
strict-transport-security	max-age=31536000; includeSubDomains
cache-control	no-cache, no-store, must-revalidate, max-age=0
cf-cache-status	DYNAMIC
vary	accept-encoding
set-cookie	JSESSIONID=UbpRK0-tj45_k66GaxCX3pahyeVMBT3RRUmB43FW.creditviewcanilivesite-c67db9674-cfgsr; path=/
set-cookie	TUCILBCookie=IOSbXlHHQYaf0mfDjX5CzXp4Shk/R5VXob4ec5qmbF9Y/WFgXLEbNchF1VkO3pwsORstBu9S50VDVQ=; path=/; HttpOnly; Secure
set-cookie	_cf_brr=8QdPUP49gdWq_gwvPQ3hr1ADw7Wk4da2WtKSX0775KdU-1748128275-1.0.1.1-HIEC1QG.Gt3j4tA6y8qhw19rTMIW8hJ25sJdQ1LqVuSNG4PbjHxMLBile0a7ENMqNQNwpGmTp632ajje6NUTXoRbN9GgWWCOGjOHhLN0; path=/; expires=Sat, 24-May-25 23:41:15 GMT; domain=*.mytrueidentity.ca; HttpOnly; Secure; SameSite=None
server	cloudflare
cf-ray	94507890c8b1bdb1-DUB
content-encoding	gzip

```
▼<script type="text/javascript" id charset>
```

</script>

Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

x-xss-protection	X-XSS-Protection sets the configuration for the XSS Auditor built into older browsers. The recommended value was "X-XSS-Protection: 1; mode=block" but you should now look at Content Security Policy instead.
x-frame-options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
content-security-policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect reports about problems on your site.
x-content-type-options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
strict-transport-security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.
set-cookie	The 'httpOnly' flag is not set on this cookie. The 'secure' flag is not set on this cookie. There is no Cookie Prefix on this cookie. This is not a SameSite Cookie .
server	Server value has been changed. Typically you will see values like "Microsoft-IIS/8.0" or "nginx/1.7.2".

This site is hosted and operated by TransUnion Interactive, Inc., a wholly owned subsidiary of TransUnion, LLC. Copyright 2019 TransUnion Interactive. All Rights Reserved.



A TransUnion® Information Solution

[FAQs](#)

[Terms and Conditions](#)

[Privacy Policy](#)

[Accessibility](#)

Security Analysis by Meng Cheng

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Nova Scotia Power Privacy
Date: May 26, 2025 10:48:51 AM

From: Melissa Marsh [REDACTED]
Sent: May 26, 2025 9:54 AM
To: privacy.officer@nspower.ca
Cc: Board, NSUARB <Board@novascotia.ca>; mlahantseast@gmail.com; Premier <PREMIER@novascotia.ca>; Information Privacy Commissioner for Nova Scotia <oipcns@novascotia.ca>
Subject: Nova Scotia Power Privacy

Some people who received this message don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Attn: Nova Scotia Power Privacy Officer

I am writing to formally complain about Nova Scotia Power's handling of its recent security breach. According to the letter your company sent, my personal information was affected, though the letter didn't specify exactly what information was taken.

I am deeply concerned about both the theft of my personal information and Nova Scotia Power's inadequate response to this serious security breach. According to your letter:

- My personal data was stolen by an unauthorized third party on or around March 19, 2025.
- Nova Scotia Power discovered this breach on April 25, 2025.
- Nova Scotia Power didn't notify me of the breach or that my information had been stolen until May 23, 2025 – two months after the breach and almost one month after your organization knew about it.

As mentioned, I received your notification letter on May 23, 2025. While your letter acknowledged that my personal data had been stolen by an unauthorized third party, it didn't meet acceptable standards for breach notification in several important ways:

1. Lack of Specific Information: The letter mentioned broad categories of compromised data but didn't specify what particular information was stolen. As a victim of your company's security breach, and according to the Personal Information Protection and Electronic Documents Act (PIPEDA), I have a legal right to know the full scope of my personal data exposure.
2. No Guidance on Next Steps: Your letter provided no guidance on what steps to take to protect myself from potential identity theft or fraud resulting from this breach. I contacted the federal Privacy Commissioner's office on my own to get this essential information.
3. Minimal Support and Resources: The only support Nova Scotia Power offered was "... a dedicated phone number 1-844-818-0376 for customers who have questions about this incident," and a code to set up an account with TransUnion credit monitoring services. When I called the number, I was connected with TransUnion. This limited response is not enough support for victims of a data breach of this size.

In closing, I request that Nova Scotia Power immediately:

1. Provide me with a detailed, specific account of exactly what personal information of mine was compromised in this breach.
2. Explain the delay between discovering the breach (April 25) and notifying me (May 23).
3. Offer comprehensive identity protection services beyond basic credit monitoring.
4. Provide clear, detailed guidance on all steps I should take to protect myself from potential consequences of this data exposure.
5. Implement improved cybersecurity protocols and procedures, and explain what those are, to ensure any future incidents are handled quickly, transparently, and appropriately.

Data security breaches are serious and can have lasting consequences for those of us affected by them. Nova Scotia Power's customers deserve better protection of their personal information and, when breaches happen, a response that prioritizes speed, transparency, specific details, and comprehensive support. Your organization's current approach doesn't adequately address the legitimate needs

and concerns for specific information about my stolen data.

I look forward to your prompt reply addressing my concerns and requested corrective actions. Please confirm that you have received this complaint and provide a timeline for your response.

Sincerely,

Melissa Marsh

CC: Nova Scotia Provincial Government

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Electricity Inquiry: Nova Scotia Power Personal Information Breach [REDACTED]
Date: May 27, 2025 8:01:06 AM

From: [REDACTED]
Sent: May 26, 2025 4:18 PM
To: Henwood, Crystal D <Crystal.Henwood@novascotia.ca>
Subject: Electricity Inquiry: Nova Scotia Power Personal Information Breach [REDACTED]

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hi Ms. Henwood,

I hope that all is well. I received correspondence dated 13 May 25 from Nova Scotia Power (NSP) regarding the access of my personal information by unauthorized third party. NSP was vague regarding any specifics of my personal information that was accessed. NSP, in the aforementioned correspondence, offered a two year account with credit reporting agency Transunion.

I have specific concerns and questions that need to be addressed with NSP and the Government of NS at this time. I reached out to NS Power today via its residential contact number, 1-800-428-6239, where an automated voice message directed me, as a customer impacted by the unauthorized access of my personal information, to contact a number, 1-844-818-0376, dedicated to impacted clients. I called the number and was greeted by an automated voice identifying itself as the Transunion office. I was then place don hold for the next available agent and after about six minutes the call was cut off. This is not acceptable in the least as I was not afforded the opportunity to speak to a representative of NSP to address my concerns. Furthermore, being cutoff while on hold was completely unsatisfactory. I called the NSP number, 1-800-428-6239, again, and selected the option for "other inquiries", and was placed on a hold for an extraordinary amount of time and was required to hang up as I had other matters to address. In addition, I am unable to find an appropriate email with which to address my questions and concerns with NSP.

In the meantime, I am stating my questions and concerns below. If you are in a position to address my questions and concerns it would be very much appreciated; otherwise, would you mind forwarding them to a responsible party due to the fact that I cannot find the name, email, or phone number of a responsible party which is also unacceptable.

My NSP account number is [REDACTED] and my questions and concerns are as follows:

- Precisely what personal information of mine was on file with you at the time your server was breached by an authorized third party?
- If I accept the Transunion account does that, from the perspective of NS Power, prevent me from entering a class action lawsuit versus NS Power regarding the breach of its security and the subsequent release of my personal information to an unauthorized third party?
- Will NS Power extend the Transunion account indefinitely beyond the two years currently offered considering the significantly elevated risk and real threat of grave and irreparable damage to my financial well-being that I am now faced with as a result of NS Power's failure to protect my personal information?
- If my personal information is used for unlawful purposes, such as, but not limited to, the creation with my personal information of a mortgage, personal loan, line of credit, credit card, other form of equity liability, will NS Power cover these losses in full including all associated legal fees and all other actions necessary to restore my finances and credit rating to good standard?
- Did NS Power receive personal information from any other entity such as my solar provider? If so, which entities and what information was received, and, if applicable, what specific information, including the entity from which the information was derived, did an unauthorized third party gain access?
- What level of accountability will NSP and/or the Government of Nova Scotia undertake in this matter to ensure that I do not bear any impact whatsoever, now or in the future, regarding the unauthorized access of my personal information? The Government of NS placed its constituents, including myself, in this egregious circumstance by selling its power entity to a private company, NSP, that obviously did not take the necessary precautions and/or put in the requisite safeguards to protect the private information of its clientele. The Government of NS should have ensured that the buyers of its power entity were able to safeguard constituent personal information. Also, the Government of NS exacerbated the situation by permitting NSP to have a monopoly.

Thank you for your assistance with this extremely important matter.

Warm Regards,

[REDACTED]

[REDACTED]

[REDACTED]

General Complaint - NS Power and municipal electric utilities

Reference Number: 250526001

Submitted on: Monday, May 26 2025 at 05:03:37 PM (ADT)

Contact Information

Name on account: Bonnie Lavigne

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

I'm one of the thousands of people who's personal and financial information was compromised by a ransomware attack against NS Power. We are now vulnerable to identity thieves who picked up our sensitive information on the dark web when NS Power refused to pay the ransom. The company has sent a letter explaining the situation and offered a two-year subscription to TransUnion where we can track suspicious activity affecting our financial accounts, and that is all. The credit website is convoluted for many of us and only offers monitoring services, which we, the victims, are responsible keep track of. There is no legal protection. If the utility was under the umbrella of the government instead of a private for-profit company the likelihood of this happening would be remote. Government websites are known for their very tight security and firewalls. I ask that you take a look at the situation to see if any further action can be taken to protect the consumers who were compromised. Your input would be taken more seriously than NS Power customers, who were not given any notice of the threat when discovered and no decision-making options when the company was considering whether or not to pay the ransom.

We obviously don't count. I appreciate your attention in this matter. Many thanks.

Did they contact the utility? No

How did the utility respond?

How do they want the complaint resolved?

Legal protection against identity threat. Compensation from the utility for any theft. Improved transparency including policy changes regarding notifying stake-holders (customers) of major threats or incidents. More active resolution to tangibly protect customers who are compromised beyond simple monitoring. Longer subscription to TransUnion. Town halls to explain above actions and help with the aftermath. A list of contacts (lawyers, consumer advocacy groups, government representatives, police departments) we can follow up with if/when there is an issue.

Supporting documents uploaded:

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Submitting a Statement to the Board
Date: May 27, 2025 10:24:21 AM
Attachments: [Dear Nova Scotia Power.docx](#)

From: diane betts [REDACTED]
Sent: May 26, 2025 5:16 PM
To: Brown, Rebecca <Rebecca.Brown@novascotia.ca>
Subject: Re: Submitting a Statement to the Board

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

I am writing of my experience with the negligent data breach from NS Power. On May 15, I checked my bank account only to discover that there were two transactions made without our knowledge. Our bank, [REDACTED] was closed so I was not able to contact them until Friday, May 16. They informed me someone called, with all my banking information, date of birth, etc. and they gave them access to my account. Tuesday Morning May 20, we received a call from the [REDACTED], who was extremely helpful and who walked us through the process of shutting down the account, calling Equifax and TransUnion Canada etc. At this point, we still did not know how someone could possibly get into our account. We called the Halifax Regional Police and they arrived at our home shortly after our call. They queried us as to whether we had been involved in a scam or we entered a site we shouldn't have but they quickly realized we did nothing like this. One week later, we receive the form letter from NS Power stating that our personal data including, but not limited to, our bank information, SIN number, date of birth, address, name and phone number has been compromised. We now found the connection. With regards to the letter, it was vague and unhelpful. The tone of the letter was not urgent and while I certainly took immediate action, when I called the TransUnion number for additional technical help, I was given the outage line number. The blatant, irresponsibility of NS Power is shocking. The breach occurred March 19th and yet customers were not notified until May 23, 2025 - two months after the incident!! I have to wonder if we have been notified immediately, we might have been able to prevent having \$30,000 stolen from our bank account. NS Power is responsible and I am hoping they will admit as such and they need to rectify my situation of reimbursement of our money.

Regards

Diane Newman Betts
Michael Betts

Dear Nova Scotia Power,

I am writing to lodge a formal complaint against Nova Scotia (NS) Power for your extreme negligence in safeguarding customer data, communications with customers about their recent data breach, delays in the communications process, and the subsequent distribution of my personal identity data without consent. **As a direct result of this negligence, my husband and I were both victims of theft.** With Nova Scotia Power's data breach and distribution of our personal information (including, but not limited to, our bank information and Social Insurance Numbers), hackers were able to directly contact my bank, [REDACTED], and use our personal information (from NS Power) to steal \$30,000 by fraudulently transferring the money from [REDACTED].

While I have received no response or communication from Nova Scotia Power, I have been in contact with [REDACTED], an investigator with [REDACTED], and he has been walking us through this arduous journey. Our goal is to recover the \$30,000 that was stolen because of Nova Scotia Power distributing our personal information.

The blatant disregard for the private personal information of your customers is horrifying. The breach occurred March 19th and yet customers were not notified until May 23, 2025 – two months after the incident! I have to wonder if we had been notified immediately, we might have been able to prevent having \$30,000 stolen from our bank accounts.

Additionally, the "To Whom it May Concern" letter that was distributed to your customers is general, vague and unhelpful. The tone of the letter was not urgent and while I certainly took immediate action, when I contacted NS Power to inquire about next steps, I was ignored and then transferred to the Outages department. A clear dismissal of my concerns and no assistance, even though the issues I am facing are a direct result of your negligence. To be clear, in no way, did I "click on a suspicious link" or "fall for a scam". You released my personal information, and as a result, a criminal was able to use my personal information to access my accounts and steal money. NS Power is 100% responsible for this issue and I expect you to contact me immediately to rectify it.

We have been in touch with the following organizations to file a complaint:

- The Privacy Commissioner of Canada
- The Utility and Review Board
- CTV NEWS and have been interviewed
- Halifax Regional Police Fraud Division Incident no. [REDACTED]
- We are currently waiting for a reply from Premier Houston's office
- We are currently waiting for a reply from CBC GO PUBLIC

Please advise as soon as possible with how you will be rectifying this issue, including a formal apology, immediate compensation for the \$30,000 that was stolen as a direct result of NS Power negligence, and a timeline for when I can expect it to be completed.

Regards,

Diane Newman Betts

Michael Betts



PO Box 910 Halifax,
Nova Scotia B3J 2W5

May 13, 2025

LETTER NUMBER 0004 AUTO 1001147



Michael Betts

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 myTruIdentity) at no cost to you. Please refer to the attachments included with this notice for additional information about TransUnion myTruIdentity, 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.



Services Description

We have retained the assistance of TransUnion Canada, Inc. ("TransUnion Canada"), one of Canada's leading consumer reporting agencies and arranged a 24-month subscription to myTrueIdentity®, 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 insurance¹.
- ✓ 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 myTrueIdentity®, please contact TransUnion Canada at 1-877-884-3441.

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



General Complaint - NS Power and municipal electric utilities

Reference Number: 250527002

Submitted on: Tuesday, May 27 2025 at 08:48:19 PM (ADT)

Contact Information

Name on account: Lisa Winch

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

Breach of all my personal information: I'm one of the thousands of people whose personal and financial information was compromised by a ransomware attack against NS Power. We are now vulnerable to identity thieves who picked up our sensitive information on the dark web when NS Power refused to pay the ransom. The company has sent a letter explaining the situation and offered a two-year subscription to TransUnion where we can track suspicious activity affecting our financial accounts, and that is all. *So far thieves have been using my credit card on a shopping spree in Ontario. Other effects so far are: *endless Phishing emails *weird phone calls *I feel queasy and can't sleep at night. I've always been so careful with my information but NS Power wouldn't hook me up without doing credit checks and having my credit card number. So that's that. They just gave away my personal info that could have financial repercussions for the rest of my life. The credit website is convoluted for many of us and only offers monitoring services, which we, the victims, are responsible keep track of. There is no legal protection.

What I have been able to do so far is: -Informed my credit card company of the fraud -I have registered for mytrueidentity and somehow managed to get help putting a fraud alert on my Trans union file. I still haven't been able to get that done with Equifax. They offered me a free report but that's it. -I have also called CRA and they won't give out new SIN numbers and will lock out my account if I ask but then I can't get access to it. If the utility was under the umbrella of the government instead of a private for-profit company the likelihood of this happening would be remote. Government websites are known for their very tight security and firewalls. I ask that you take a look at the situation to see if any further action can be taken to protect the consumers who were compromised. Your input would be taken more seriously than NS Power customers, who were not given any notice of the threat when discovered and no decision-making options when the company was considering whether or not to pay the ransom. We obviously don't count. I appreciate your attention in this matter. Many thanks.

Did they contact the utility? No

How did the utility respond?

How do they want the complaint resolved?

Legal protection against identity threat. Compensation from the utility for any theft. More active resolution to tangibly protect customers who are compromised beyond simple monitoring. (Personally, I want new everything: new bank accounts, new SIN, new License, new phone numbers, new utility account numbers. I would even go so far as to getting a new name and Passport with the old SIN locked not to be used again) Longer subscription to TransUnion. Improved transparency including policy changes regarding notifying stake-holders (customers) of major threats or incidents. Town halls to explain above actions and help with the aftermath. A list of contacts (lawyers, consumer advocacy groups, government representatives, police departments) we can follow up with if/when there is an issue.

**Supporting documents
uploaded:**

- 1000004479.jpg



PO Box 910 Halifax,
Nova Scotia B3J 2W5

May 13, 2025

03766-ADPWH01 1016 APPO 1000199



Lisa Winch
[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 *myTrueIdentity*) at no cost to you. Please refer to the attachments included with this notice for additional information about TransUnion *myTrueIdentity*, 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.

General Complaint - NS Power and municipal electric utilities

Reference Number: 250529001

Submitted on: Thursday, May 29 2025 at 09:31:29 AM (ADT)

Contact Information

Name on account: Angela Rafuse

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

The recent cyber attack at NS Power has left me feeling vulnerable. The 2 yr credit monitoring with Transunion offered is cumbersome and tedious; - if one already had credit monitoring, you must cancel and delete your account by phone with Transunion. You are then required to re-registered, cancelling out all alert and information you provided. This cannot be completed online and one must remain on hold for a lengthy period of time. Additionally, if I remember correctly, one was required to provide their social insurance number when registering for an account at NS Power. I have a mortgage and auto loan without having had to provide any of this. Why is NS Power required to ascertain our SIN?

Did they contact the utility? No

How did the utility respond?

How do they want the complaint resolved?

I want NS Power to offer something better in terms of storing and protecting our information. No customer should ever be required to provide their SIN to receive service, and NS Power should cease this practice immediately. Additionally, the customers and public require better measures to protect their data released to hackers / in the ransomware attack. Transunion is not effective in managing the monitoring.

Supporting documents uploaded:

General Complaint - NS Power and municipal electric utilities

Reference Number: 250529002

Submitted on: Thursday, May 29 2025 at 08:04:27 PM (ADT)

Contact Information

Name on account: Carol Moore

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

I received a letter on May 20, 2025 from NS Power indicating that my personal information was stolen in a data breach. The letter I received is dated May 13, 2025. The letter indicates that the incident was discovered on April 25. The notice to me is a full 18 days later, this is not quick enough. The "incident" occurred on March 19. I was not notified until 8 weeks later. This is unacceptable. The matter was not dealt with urgently. The letter provides a phone number to call for further information. I called that number and reached a representative of Trans Union, not NS Power. I asked her exactly what info of mine was on the file of NS Power, did it include my SIN, date of birth, etc. She said that they would respond to my question in 5 days. I was not happy with this service.

Did they contact the utility? Yes

How did the utility respond?

How do they want the complaint resolved?

I expect NS Power to tell me, in writing, exactly what information on my file was stolen. Secondly I want NS Power to extend the credit monitoring with Trans Union to a full 10 years. Thirdly, I want financial compensation for my time and suffering. As a senior, this has caused my anger, anxiety and frustration.

Supporting documents uploaded:

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: NSPower
Date: May 30, 2025 11:12:34 AM

From: Jared Juckiewicz [REDACTED]
Sent: May 29, 2025 3:58 PM
To: Board, NSUARB <Board@novascotia.ca>
Subject: NSPower

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Dear sir or madam.

I am writing in response to the inevitable request by NSPower for yet another rate hike to recoup costs incurred by the recent cyber attack.

I feel that ratepayers should not be penalized because the utility failed to invest sufficiently in cyber security.

I have been repeatedly disappointed by the boards continuous approval of NSPowers requests for rate increases despite the cost of living in Nova Scotia already being at all time highs and wages not keeping pace with inflation.

If the board continues to act as a rubber stamp for the utility's blatant attempt at profiting off the backs of hard-working maritimers without any improvement in service, I will be continue my representatives about its failure to represent the needs of Nova Scotians in favour of funneling money to Emera.

Sincerely
Jared Juckiewicz
Dissatisfied ratepayers.

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: NSP Cyber Breech
Date: June 2, 2025 9:25:44 AM

From: d ellis [REDACTED]
Sent: May 31, 2025 10:36 AM
To: Henwood, Crystal D <Crystal.Henwood@novascotia.ca>; info@emera.com;
webmaster@priv.gc.ca; rodwilson@nsmla.ca; lenametlege.diab@parl.gc.ca
Subject: NSP Cyber Breech

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

David Ellis

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Peter Gregg
President & CEO
Nova Scotia Power

Re: Nova Scotia Power Cyber Breech

Dear Mr. Gregg,

I am in receipt of your May 13, 2025 correspondence regarding the NSP cyber breach. Two weeks have past and I remain in utter disbelief that your organization has totally failed in this regard.

Your correspondence has done nothing to calm my fear and stress. I have contacted Transunion however what little protection that this might provide is limited to two years. I am also following up with credit reports and placing a fraud alert. Then what? Myself and every other impacted customer now has their personal information on the "dark web" to be used for nefarious purposes for the duration of our life. How comforting!

Your correspondence was generic. It stated that the impacted personal information may have included: name, phone number, email address, ... driver's license number, and Social

Insurance Number. I could not understand why I would ever have provided the scope of this information and in particular, my SIN. I now understand that the SIN was potentially collected for credit check purposes. I request that NSP forward to me an itemized list of my specific personal information which was released.

I find it unbelievable that this public utility does not have a robust IT security system. There is no excuse. I would suggest that, in part, the rationale for an electric monopoly is that the public is not best served by the lowest cost provider when it comes to such matters as security.

Emera's stated "Values" include "We put customers at the centre of everything we do. We listen to our customers, and we are working hard to meet and exceed expectations." Emera has failed. Unfortunately, if I want electricity, I have no choice other than to remain a customer of NSP.

Regards,

David Ellis

Cc Office of the Privacy Commissioner of Canada

Crystal Henwood, Clerk of the Board, Nova Scotia Energy and Regulatory Boards
Tribunal

Rod Wilson, MLA Halifax Armdale

Lena Metlege Diab, MP Halifax West

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: [REDACTED] FW: NS Power Cyber Breach - Corporate network vulnerabilities
Date: June 4, 2025 9:30:11 AM
Attachments: [Sae527zh1f0_share.png](#)
[TechRadar article - published March 21, 2025.pdf](#)
[Johnathan Rhynold's post.png](#)
[Senior ServiceNow Analyst Job posting - closing May 2, 2025.pdf](#)
[Glassdoor Job posting - closing May 2, 2025.jpg](#)
[TechCrunch article - published March 20, 2025.pdf](#)
[image002.png](#)
[CSO article - published July 30, 2024.pdf](#)

From: [REDACTED]
Sent: June 3, 2025 8:59 PM
To: Brown, Rebecca <Rebecca.Brown@novascotia.ca>
Subject: NS Power Cyber Breach - Corporate network vulnerabilities

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercice caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Good evening,

As discussed today, please consider this synopsis of a potential source of the cyber breach on the NS Power corporate (non-operational) network. For your further review and further investigation.

On or about 20 May 2025, I received a letter dated 13 May 2025 signed by Peter Gregg, CEO NS Power acknowledging a cyber breach which resulted in my personal information being stolen. As a result of this, I have chosen to do some investigating utilizing whatever resources are available. I have used the NS Energy Board public access database primarily to source information related to historical NS Power network security and like projects endorsed by the NS Energy Board.

The primary document of interest I found is M09301, entitled: CI 49093, IT - Security Operations Centre (SOC) and Security Information Event Monitoring (SIEM) REDACTED dated 2 July, 2019. Additionally, I have reviewed at length N-2 NSPI (NSUARB) RIR-1 to RIR-21 Responses to NSUARB Information Requests REDACTED dated 28 August, 2019.

As per the description, this aforementioned project procured and implemented the “required hardware and software to run an SIEM tool and connection to a SOC service that provides real-time monitoring and detection of cyber threats and attacks.” The SOC service is provided by a third party vendor named *Service Now*. The costs for this vendor have not been reflected anywhere in this capital project. I suggest that NS Power be asked to disclose what they have spent for this SOC service from the inception of this project to its close.

The SOC “is designed to identify in real time attacks and provide early warning to security staff so that protective steps can be taken” including system shutdown in response to an attack or installation of software upgrades or patches to mitigate access. So, it is conceivable that the limited internal staff will have to conduct software updates throughout the life of the procured software across myriad locations that serve and access the corporate network architecture. The question is: have the necessary software updates been performed throughout the use of the SOC and SIEM tool as NS Power chose the ‘hybrid’ lower cost option was chosen. This chosen option appears to have left the onus with internal NS Power IT employees to setup new server hardware and software and to perform routinely and timely software updates on this new software as required.

As I understand it, NS Power is obliged from a regulatory point of view to focus internal resource priority on the operation and maintenance of the Operational IT network elements. As the safeguarding of the corporate network is much lower priority in comparison to the operational network, and is likely not part of the regulatory oversight, this project effort appears to have languished from 2016 inception to a 2022 conclusion. This is apparent as NSPI (NSUARB) IR-2 page 1 of 1 states “work associated with this project was put on hold during 2017 and 2018 as dependencies with other IT work were assessed”. Although this project need is based on real cyber security threats was conceived in 2016, it is surprising that this project clearly explains on NSPI (NSUARB) IR-3 page 2 of 2 that “this capability does not exist today”. With well know threats and vulnerabilities, it appears that NS Power carried on operating the corporate network for years without suitable safeguarding.

It is not clear how long NS Power has contracted the SOC vendor services from *Service Now*. NSPI (NSUARB) IR-17 page 1 of 2 states “...2021 will be the first year of operation. In 2020, the SOC service is forecasted to be in operation from the mid-year point on”. IR-4 asks about the length of the contract, but it is not clear when initial operating capability (IOC) of the service was actually established nor when full operational capability (FOC) was reached. This is information the regulatory board should be aware of, as it establishes when NS Power had actual safeguards in place to protect the corporate network as the project demands. Further, regarding IR-6, it is not clear how the ‘hybrid’ approach allowed NS Power to safely and securely establish a network connection to Service Now while using Service Now SOC services.

IR-20 discusses the in-house and hybrid solutions. What is not clear at this juncture is whether the ‘hybrid’ option is still being utilized. Although NS Power says at NSPI (NSUARB) IR-20 page 1 of 1 that “If NS Power were to implement an internal SOC, operational costs are estimated to exceed those of the hybrid approach and NS Power would also be exposed to the risk that it would not effectively deliver the SOC services”. I say that it is not clear what option is being utilized at this time, since very recently NS Power advertised three internal positions for hire of *Service Now* Intermediate (2) and Senior (1) Analysts. Screenshots follow:

12:26



Johnathan Rhynold's Post



Johnathan Rhynold

ServiceNow Platform Lead

1mo



I'm **#hiring** THREE **#ServiceNow** professionals to join our growing platform team in Halifax!

2x Intermediate ServiceNow Analyst

1x Senior ServiceNow Analyst (focus on ITOM)

Lots of cool tech to build on including ITOM, ITSM, SecOps, SAM, Integration Hub, Workflow Studio and more

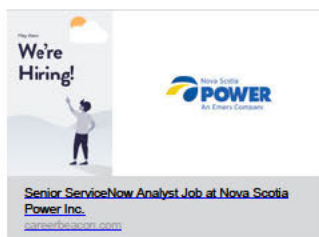
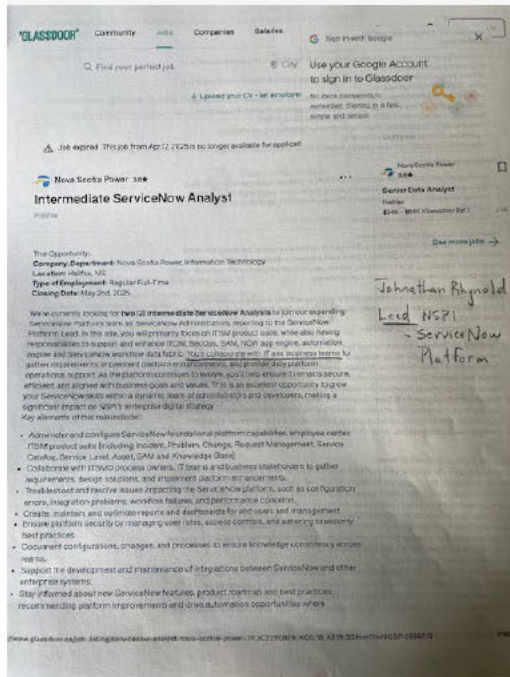
Apply or share with your network!

<https://lnkd.in/g2kNT424>



Nova Scotia Power Careers | Home

careers.emera.com



I recommend that the NS Energy Board, in the service of its formal investigation of NS Power's cyber security breach of its corporate network infrastructure, seek out **how** NS Power was able to safely and securely establish a network connection with the third party vendor *Service Now* for SOC services since IOC. This response is essential as it is known that on or about 10 July 2024 *Service Now* identified critical vulnerabilities in its software that had been widely exploited by malicious cyber actors. A link follows explaining these severe vulnerabilities and their impact on myriad industry corporate networks.

<https://www.csoonline.com/article/3478933/critical-servicenow-vulnerabilities-expose-businesses-to-data-breaches.html>

According to this reference link, these three vulnerabilities CVE-2024-4879 (Critical), CVE-2024-5217 (Critical) and CVE-2024-5178 (Medium) in *Service Now* let anyone run code on the platform remotely without needing to log in. According to Resecurity, CVE-2024-4879 and CVE-2024-5217 are input validation vulnerabilities in *Service Now*'s "Vancouver" and "Washington DC" versions that allow unauthenticated remote attackers to execute arbitrary code with relative ease. CVE-2024-4879 is related to Authentication Bypass. This flaw lets attackers bypass authentication and access the *Service Now* platform without permission. They can remotely execute code by exploiting this vulnerability. CVE-2024-5217 pertains to Arbitrary Data Access. This vulnerability lets attackers access and extract any data stored in the *Service Now* system. **This includes sensitive information, customer data, and internal communications, posing a serious threat to business operations and data privacy.** The third one, CVE-2024-5178, is related to Privilege Escalation and allows attackers to increase their access level within the *Service Now* system. With elevated permissions, attackers can gain administrative control, making it easier to alter data and system settings.

It is not clear if internal NS Power employees (when employing the hybrid option) were able to ensure that *Service Now* software critical vulnerabilities identified on 10

July 2024 were addressed. My concern is that the software patches were NOT done across myriad NS Power locations employing the *Service Now* software and thus leaving the corporate network remarkably vulnerable. This must be investigated, as on or about **19 March 2025**, hackers sought out organizations who had not yet performed the updates to alleviate these vulnerabilities. This link explains:

<https://techcrunch.com/2025/03/20/hackers-are-ramping-up-attacks-using-year-old-servicenow-security-bugs-to-break-into-unpatched-systems/>

Further, I do not believe that it is a coincidence that **19 March 2025** is also the date that NS Power identified in its press release that “certain customer information stored on impacted servers was accessed and later taken by an unauthorized party”.

Please direct any questions related to this to the undersigned,



Sent from my iPhone



THE BUSINESS TECHNOLOGY EXPERTS



Sign in

TRENDING

Best website builder

Best web hosting

Best office chairs

Expert Insights

Pro > Security

ADVERTISEMENT

Hackers are targeting unpatched ServiceNow instances that exploit 3 separate year-old vulnerabilities

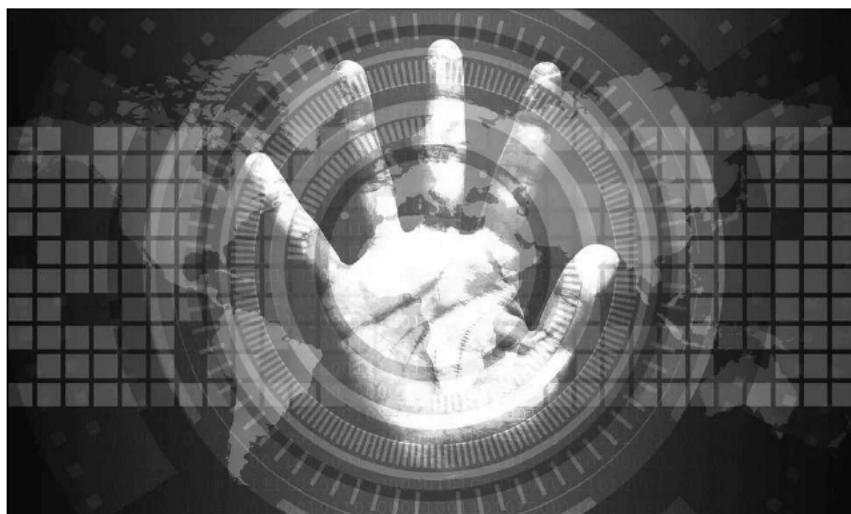
News By Sead Fadilpašić published March 21, 2025

The vulnerabilities can also be chained together



Comments (0)

When you purchase through links on our site, we may earn an affiliate commission. [Here's how it works.](#)



- ServiceNow fixed three flaws in May 2024, but researchers from GreyNoise saw a resurgence of abuse
- The flaws can be used for full database access
- Users should patch immediately to make sure they are protected

There has been a “notable resurgence” in the abuse of three concerning ServiceNow security vulnerabilities, experts are warning.

In May 2024, security researchers from Assetnote found vulnerabilities, tracked as CVE-2024-4879, CVE-2024-5178, and CVE-2024-5217, which ServiceNow patched the same day.

However, it seems that many organizations did not get the memo (which was released in July the same year, when CVEs were released as part of a coordinated effort with Assetnote), since their instances remained unpatched, and have now become a target, according to researchers from GreyNoise.

ADVERTISEMENT

LATEST VIDEOS FROM TECHRADAR

PLAY SOUND



YOU MAY LIKE

- **These two Ivanti bugs are allowing hackers to target cloud instances - so patch now**
- **Cisco smart licensing system sees critical security flaws exploited**
- **Ivanti Neurons for ITSM could be targeted by authentication bypass flaw, so watch out**

Chaining the bugs

The researchers found there has been a significant uptick in the attacks abusing these flaws, and although they couldn't attribute the attacks to any known threat actors, they did note that almost three-quarters (70%) of the attacks targeted Israeli firms. Notable activity was also spotted in Germany, Japan, and Lithuania.

LATEST ARTICLES

- 1 I spent three weeks testing the Hisense C2 Ultra projector and was amazed at how consistently it served up scintillating visuals
- 2 Quantum computing startup wants to launch a 1000-qubit machine by 2031 that could make the traditional HPC market obsolete
- 3 8 new horror movies on Netflix, Shudder, HBO Max, and more

The vulnerabilities can be abused separately, but when they're chained, they grant "full database access," GreyNoise added, which puts vulnerable organizations at immense risk, since ServiceNow is used to handle sensitive employee information.

The attackers would inject a payload which checks for a specific result in the server response. If it gets the appropriate one, it deploys a second-stage payload that checks the contents of the database.

The last step is to dump user lists and account credentials. While most of the time the credentials are hashed, there are some examples where the credentials were dumped in plaintext.

Are you a pro? Subscribe to our newsletter

Sign up to the TechRadar Pro newsletter to get all the top news, opinion, features and guidance your business needs to succeed!

SIGN ME UP

- ☐ Contact me with news and offers from other Future brands
- ☐ Receive email from us on behalf of our trusted partners or sponsors

By submitting your information you agree to the [Terms & Conditions](#) and [Privacy Policy](#) and are aged 16 or over.

That can lead to account compromise which, in turn, can carry devastating consequences, such as ransomware attacks.

ServiceNow is a cloud-based platform that provides enterprise IT service management (ITSM) and automation solutions.

It helps organizations streamline workflows, automate business processes, and improve efficiency across IT, HR, customer service, security, and other departments.

ServiceNow has almost 300,000 internet-exposed instances, making it quite a popular solution.

Some of its clients include Coca-Cola (uses it for streamlining IT service management), Dell (IT service automation and management), Deloitte (IT service automation and optimization), and the State of California (managing state-wide IT services and operations).

Via TechCrunch

YOU MIGHT ALSO LIKE

- Several ServiceNow flaws are reportedly being linked together to attack companies and organizations
- We've rounded up the best password managers
- Take a look at our guide to the best authenticator app

in June 2025

4 Walmart's mega summer sale is live – 29 deals I'd buy on TVs, grills, vacuums and more

5 Say goodbye to fuzzy, hazy, and low resolution webcam video with this free app

ADVERTISEMENT

ADVERTISEMENT

Sead Fadilpašić



Sead is a seasoned freelance journalist based in Sarajevo, Bosnia and Herzegovina. He writes about IT (cloud, IoT, 5G, VPN) and cybersecurity (ransomware, data breaches, laws and regulations). In his career, spanning more than a decade, he's written for numerous media outlets, including Al Jazeera Balkans. He's also held several modules on content writing for Represent Communications.

Conversation

[FOLLOW](#)[LOG IN](#) | [SIGN UP](#)

Please follow our [community guidelines](#).



< Start the conversation

ALL COMMENTS

NEWEST ▾



LOAD NEW CONTENT

tion

ADVERTISEMENT

READ MORE



These two Ivanti bugs are allowing hackers to target cloud instances - so patch now

ADVERTISEMENT



Senior ServiceNow Analyst

Nova Scotia Power Inc. - 20 Jobs

Halifax, NS

✦✦ Am I a good fit?

Closed



This position has been closed and is no longer accepting applicants.

Job Details:

In-person

Full-time

Experienced

The Opportunity

Company, Department: Nova Scotia Power, Information Technology

Location: Halifax, NS

Type of Employment: Regular Full-Time

Closing Date: May 2nd, 2025

Join our growing ServiceNow Platform team as a **Senior ServiceNow Analyst** reporting to the ServiceNow Platform Lead. In this role, your primary focus will be on managing and optimizing the ITOM suite, including Discovery, MID Server infrastructure, and Event Management. You'll also contribute to broader platform administration tasks and support core ITSM processes as needed. Collaborating with IT, infrastructure, and security teams, you'll play a critical role in improving visibility, automation, and operational health across our technology landscape. This is an excellent opportunity to grow your ServiceNow skills within a dynamic team of

administrators and developers, making a significant impact on NSPI's enterprise digital strategy.

Key elements of this role include:

- Administer and maintain ServiceNow ITOM capabilities, with a focus on Discovery, MID Server deployment and tuning, and Event Management.
- Collaborate with network, server, and application teams to ensure accurate and complete service mapping and infrastructure visibility.
- Monitor and optimize MID Server performance, availability, and upgrades.
- Support the configuration and tuning of Event Management rules, alert correlation, and operational dashboards.
- Help troubleshoot issues across the platform, including performance concerns and integration errors.
- Document processes, configurations, and updates to maintain clear and current knowledge across the team.
- Stay current with ServiceNow releases and ITOM best practices, recommending platform improvements and drive automation opportunities where appropriate.

These skills will make you successful:

Qualifications:

- Bachelor's degree in Information Technology, Computer Science, or a related discipline, or equivalent practical experience.
- Strong understanding of IT infrastructure and networking concepts (servers, databases, firewalls, load balancers, etc.).
- At least 3 years of experience in ServiceNow administration or a technical operations/infrastructure support role.
- In-depth knowledge and work experience with CMDB and CI relationship mapping
- Solid troubleshooting skills and a problem-solving mindset.

- Experience working in Agile environments.
- Ability to communicate effectively across technical and non-technical teams.

Preferred Qualifications:

- ServiceNow certifications such as CSA or CIS-Discovery.
- Exposure to JavaScript and experience building workflows or automation in ServiceNow.
- Hands-on experience with ServiceNow Discovery, Event Management, and MID Server administration.
- ITIL 4 or v3.2011 foundation certification

Learn more about our culture and values

At the Emera Group of Companies, you'll be part of an inclusive, respectful workplace where everyone is welcomed and supported. Come build a career as unique as you are: making an impact from Atlantic Canada to the world. Your experience and perspective will help us to safely deliver cleaner, more reliable energy to our customers.

If working in an innovative environment, challenging yourself, and shaping a cleaner energy future inspires you, we want to hear from you. Apply by **May 2nd, 2025** and let us know why this role is right for you.

The perks of joining our team? We offer:

- **Health & Wellbeing:** A comprehensive benefits plan, 24/7 access to virtual health care services for you and your family through Dialogue, access to a free on-site fitness centre, Employee and Family Assistance Program, parental leave top-up plan and wellness benefits.
- **Grow Your Career:** Opportunities to advance within and between our affiliate companies, a focus on employee development and available sponsored education programs.

- **Community Engagement & Care:** Corporate investments in the places where our people live and work, mentoring opportunities, fundraising-matching, volunteer programs, various committees and employee resource groups, and scholarships for children of employees.
- **Competitive Compensation:** Short-term incentive plans and a Defined Contribution Pension Plan.

Diversity, Equity & Inclusion at Emera

As one of Atlantic Canada's largest publicly traded companies, we are ranked one of Canada's Top 100 Employers, Top Employers for Young People and Top Diversity Employers. We know our success is driven by our dedicated teams and we strongly encourage applications from all qualified candidates, including persons who identify as racially visible, Indigenous, persons with disabilities, women in underrepresented roles and members of the 2SLGBTQ+ community.

Applicants from these equity groups may self-identify through the online application process. We support candidates and employees with access and accommodation needs and encourage you to let us know when you require accommodation.

Recruitment & Promotion Policy

The success of the Emera Company is driven by its people: a strong team with a shared commitment to support the Emera Company mission and values. The purpose of our recruitment policy is to provide a consistent framework to support fair and equitable attraction, hiring, and retention of the best talent for vacant positions. We are dedicated to maintaining a fair hiring process that provides equitable opportunities to all our applicants and is guided by our company values.

Competition Number: 4159

Company Website: <http://www.nspower.ca>

#Information Technology jobs



About Nova Scotia Power Inc.

Our Greatest Source of Energy is Our People

At Nova Scotia Power our people are our greatest source of energy. We have a passion for energy—producing and delivering it safely every day to customers across Nova Scotia. Collaboration, innovative thinking and a commitment to sustainability is driving us towards a greener and smarter energy future and we are currently looking for like-minded people to join us.

Interested in learning more about what it's like to be part of our team? As an employer, our focus is on delivering an exceptional employee experience from the moment you join us. This includes:

- **A Culture Focused on Safety** – As a member of our team, you join a workplace that lives by the motto “everybody goes home safe everyday”.
- **Keeping Health and Wellness Top of Mind** – Throughout your career with us, you will be offered a range of services and programs that will help you take charge of your overall well-being.
- **Celebrating Diversity** - We see the inclusion of diversity of our team as one of our strengths – and something we continue to focus on and strengthen with the help and guidance from our employees on what's most important to them.
- **Developing Our Teams and Leaders** - Leadership isn't just for our senior team members – all of our employees are leaders. Our focus is on developing our team by providing opportunities for growth, development, and mentorship to ensure the success of our business while we prepare our leaders for the future.
- **Giving Back** – We're Nova Scotians which means it's important to lend a helping hand in the communities where we live and work across the province.

Does this sound like a team you want to be part of? If so, visit nspower.ca/careers to find out how.

You can also learn more about us at www.nspower.ca.



Advertisement

Latest Security
Startups AI
Venture Apps
Apple

Events
Podcasts
Newsletters



Hackers are ramping up attacks using year-old ServiceNow security bugs to target unpatched systems

Carly Page 9:04 AM PDT · March 20, 2025

IMAGE CREDITS: SMITH COLLECTION/GADO / GETTY IMAGES

Hackers are ramping up their attempts to exploit a trio of year-old ServiceNow vulnerabilities to break into unpatched company instances, security researchers warned this week.

Threat intelligence startup GreyNoise said in a [blog post](#) on Tuesday that it had observed a “notable resurgence of in-the-wild activity” targeting the three ServiceNow vulnerabilities, tracked as CVE-2024-4879, CVE-2024-5178, and CVE-2024-5217.

Advertisement

The vulnerabilities were first disclosed by [researchers at Assetnote](#) on May 14, 2024 and patched by ServiceNow on the same day, ServiceNow spokesperson Erica Faltous told TechCrunch. Details of the bugs were publicly disclosed later in July 2024.

GreyNoise said that all three flaws have seen a resurgence in targeted exploitation attempts in the past week. It's not known exactly who is behind this latest wave of targeting, but GreyNoise said that 70% of the malicious activity it observed in the past week targeted systems based in Israel, with activity also seen in Germany, Japan, and Lithuania.

As first noted by Assetnote last year, GreyNoise also confirms that the vulnerabilities can be chained together for "full database access" of affected ServiceNow instances. Organizations often use the ServiceNow platform to host sensitive data about their employees, including their personally identifiable information and HR records related to their employment.

ServiceNow told TechCrunch that the company first learned of the vulnerabilities "nearly a year ago," and, "to date, we have not observed any customer impact from an attack campaign."

Following Assetnote's disclosure of the flaws last year, [U.S. security firm Resecurity warned](#) that foreign threat actors had attempted to exploit the three ServiceNow vulnerabilities to target both private sector companies and government agencies around the world.



Save now through June 4 for TechCrunch Sessions: AI

Save \$300 on your ticket to TC Sessions: AI—and get 50% off a second. Hear from leaders at OpenAI, Anthropic, Khosla Ventures, and more during a full day of expert insights, hands-on workshops, and high-impact networking. These low-rate deals disappear when the doors open on June 5.

Berkeley, CA | June 5

REGISTER NOW

Resecurity said it saw targeted attempts at an energy company, a data center organization, a Middle Eastern government agency, and a software

developer.

Cybersecurity company Imperva released another [report](#) in July 2024 warning that it had also observed exploitation attempts across 6,000 sites across various industries, with a focus on the financial services sector.

Amended the third paragraph to note that ServiceNow issued a fix on the same day as Assetnote's disclosure.

Advertisement

Topics: [cybersecurity](#) [Security](#) [security](#) [ServiceNow](#) [vulnerability](#)



Carly Page

Sr. Reporter, Cybersecurity

Carly Page was a Senior Reporter at TechCrunch, where she covered the cybersecurity beat. Prior to that, she had spent more than a decade in the technology industry, writing for titles including...

[View Bio](#) >

by Gyana Swain

Critical ServiceNow vulnerabilities expose businesses to data breaches

News

Jul 30, 2024 • 5 mins

Data Breach

Vulnerabilities

The vulnerabilities have exposed sensitive information from over 105 organizations including government agencies, data centers, energy providers, and software development firms.



Credit: JHVEPhoto / Shutterstock [<https://enterprise.shutterstock.com/image-illustration/close-up-of-servicenow-sign-on-the-building-at-its-headquarters-in-santa-clara-california-usa-june-11-2023-servicenow-is-an-american-software-company-2356641345>]

Three **critical vulnerabilities** [<https://www.csoononline.com/article/572239/nearly-70-of-servicenow-instances-leaking-data.html>] in the **ServiceNow** [<https://www.cio.com/article/3477783/servicenow-latest-news-and-insights.html>] IT service management platform have been disclosed and reported to have been under active exploitation.

The vulnerabilities have exposed **sensitive information** [<https://www.csoononline.com/article/572365/servicenow-adds-new-features-to-major-security-incident-management-workspace.html>] from over 105 organizations including government agencies, data centers, energy providers, and software development firms.

Threat actors are actively exploiting the flaws, CVE-2024-4879, CVE-2024-5217, and CVE-2024-5178, to steal email addresses, hashed passwords, and other sensitive data, **according to cybersecurity firm Resecurity** [<https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign>]. The first two vulnerabilities have a CVSS score of 9.3 and 9.2 respectively.

Another research firm **Assetnote** [<https://www.assetnote.io/resources/research/chaining-three-bugs-to-access-all-your-servicenow-data>] added one more bug (CVE-2024-5178), with less severity, to the list, but said, that when chained together, hackers can exploit the vulnerabilities to access the ServiceNow database.

“These vulnerabilities enable unauthenticated remote attackers to execute arbitrary code within the Now Platform, potentially leading to compromise, data theft, and disruption of business operations,” Resecurity wrote in a blog post.

To add fuel to the fire, a report by DarkReading has claimed that the vulnerabilities have been exploited and data of various organizations have been stolen. More so, the stolen data, acquired using these vulnerabilities, is being offered for sale on the dark web for a mere \$5,000, **DarkReading reported** [<https://www.darkreading.com/cloud-security/patchnow-servicenow-critical-rce-bugs-active-exploit>] citing BreachForums.

Resecurity said it is expected that the bad actors would “increasingly target” ServiceNow because of these vulnerabilities.

“There has been identified chatter on multiple underground forums on the Dark Web highlighting threat actors seeking compromised access to IT service desks, corporate portals, and other enterprise systems that typically provide remote access to employees and contractors,” Resecurity wrote in a blog. “These systems could be used for pre-positioning and attack planning, as well as reconnaissance.”

The firm further added that **initial access brokers (IABs)** [<https://www.csoononline.com/article/572249/whos-who-in-the-cybercriminal-underground.html>] “will be monetizing access to compromised enterprise portals and applications on the Dark Web, leveraging infostealers (malware) and digital identity leaks, due to poor network hygiene (on the customer side).” “This vulnerability affects a significant number of ServiceNow sites across various industries, highlighting the importance of immediate action to secure these environments,” **wrote Imperva** [<https://www.imperva.com/blog/imperva-customers-protected-against-critical-servicenow-vulnerability/>], a Thales company, in its blog post explaining the vulnerabilities.

CSO Smart Answers [Learn more](#)

Explore related questions

- [How do ServiceNow vulnerabilities impact specific industries?](#)
- [Why do unpatched old vulnerabilities pose significant cybersecurity risks?](#)
- [How do known vulnerabilities impact government organizations?](#)
- [What are the cybersecurity risks of unencrypted services?](#)
- [What risks do misconfigured ServiceNow KB articles pose?](#)

Ask a question



According to ServiceNow, it learned of the vulnerability on the Now Platform impacting instances running on the Vancouver and Washington, D.C. family releases on May 14, 2024. “That day, we deployed an update and have since issued a series of patches designed to address the issue,” a ServiceNow spokesperson said.

The company added that based on its investigation to date, it has not observed evidence that the activity mentioned in the Resecurity blog post is related to instances that ServiceNow hosts. “We have encouraged our self-hosted and ServiceNow-hosted customers to apply relevant patches if they have not already done so. We will also continue to work directly with customers who need assistance in applying those patches, as we have from day one,” the spokesperson said.

Understanding the vulnerabilities

The vulnerabilities in ServiceNow let anyone run code on the platform remotely without needing to log in. According to Resecurity, CVE-2024-4879 and CVE-2024-5217 are input validation vulnerabilities in ServiceNow's "Vancouver" and "Washington DC" versions that allow unauthenticated remote attackers to execute arbitrary code with relative ease.

CVE-2024-4879 is related to Authentication Bypass. This flaw lets attackers bypass authentication and access the ServiceNow platform without permission. They can remotely execute code by exploiting this vulnerability.

CVE-2024-5217 pertains to Arbitrary Data Access. This vulnerability lets attackers access and extract any data stored in the ServiceNow system. This includes sensitive information, customer data, and internal communications, posing a serious threat to business operations and data privacy.

The third one, CVE-2024-5178, is related to Privilege Escalation and allows attackers to increase their access level within the ServiceNow system. With elevated permissions, attackers can gain administrative control, making it easier to alter data and system settings.

The US **Cybersecurity and Infrastructure Security Agency** [<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>] (CISA) has already added these vulnerabilities to its known exploited vulnerabilities catalog, urging federal civilian executive branch agencies to apply the patches by August 19 or discontinue the use of ServiceNow until remediation.

Resecurity emphasized that some affected organizations were using outdated or poorly maintained instances and were unaware of the released patches. This underscores the critical need for organizations to maintain up-to-date software and apply security patches promptly to mitigate risks.

"It is crucial for organizations using ServiceNow to apply these updates immediately to protect their systems and data from potential attacks," Resecurity suggested in the blog.

Sponsored Links

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: DRO 31 May re Sean Kelly re Data Breach
Date: June 4, 2025 9:50:04 AM

From: Sean Kelly [REDACTED]
Sent: June 3, 2025 10:27 PM
To: nspdisputeresolution@gmail.com
Cc: customerrelations@nspower.ca; Wallace, Lisa <Lisa.Wallace@novascotia.ca>; Premier <PREMIER@novascotia.ca>; Board, NSUARB <Board@novascotia.ca>; info@iainrankin.ca
Subject: Re: DRO 31 May re Sean Kelly re Data Breach

You don't often get email from [REDACTED]. [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

I am shocked at how poorly these regulations are written. I question why we have a board or a dispute resolution when the regulations are all written to protect the company and very little are written to protect the people who are forced to deal with a monopoly. It is standard practice in most regulations that there be a clause respecting and or dealing with customer privacy and or data security. Most if not any organization dealing with government contracts have to be CMMC data security (I am happy to explain this data security certification as my company is spending 1 million dollars to achieve as forced on us by the US and Canadian governments) certified by the end of this year. Why is the board not doing these things to protect Nova Scotians?

The regulations do not even state in their own document who is responsible for making the regulations. An example most regulations that are enacted are done so by the Governor in council and it is described how he/she may do that. I assume that the board can change the regulations? If so I request a meeting with the board to discuss why these regulations have little to no protections for its customers.

I wish to escalate this to a higher authority. Our personal data has been compromised and we have only been offered a very rudimentary security measure and not even a real apology.

Premier sir, I think this needs action and government intervention, ASAP. I am requesting a meeting.

I fear those affected will need to arrange a Class action lawsuit and name the board as a co-defendant as they should have foreseen this coming and added a data security

clause in the regulations as is the normal practice.

Respectfully,
Sean Kelly

[REDACTED]
[REDACTED]

On May 31, 2025, at 4:41 p.m., nspdisputeresolution@gmail.com wrote:

Don Farmer, P. Eng., Dispute Resolution Officer (D.R.O.)
Telephone (902)
428-6202, Toll-free 1-877-428-6202, Fax (902) 835-7744
nspdisputeresolution@gmail.com

Sean Kelly

In reponse to your immediately following email request :

See <https://www.nspower.ca/docs/default-source/default-document-library/nspowerregulations.pdf>

My working copy of current Board approved Regulations is also attached

Only the NSEB can consider an extension on the 12 day limit. The Nova Scotia Energy Board (NSEB) contact information is: P.O. Box 1692, Unit M, Suite 300, 1601 Lower Water St. Halifax, N.S., B3J 2S3; Email - board@novascotia.ca ;Telephone - 902-424-1332 ,Toll Free in NS: 1-833-809-0040 ; Fax - 902-424-3919

Don Farmer, P.Eng.
Dispute Resolution Officer

From: Sean Kelly [REDACTED]
Sent: May 31, 2025 10:39 AM
To: nspdisputeresolution@gmail.com
Cc: customerrelations@nspower.ca

Subject: Re: 26 May email to the DRO from Sean Kelly re Data Breech

I would like to have a copy of all regulations regarding NSPower, and based on this I request a extension to the 12 days as I need to review the regulations before I may appeal. The regulations are not readily available.

Respectfully,
Sean

On May 27, 2025, at 9:46 a.m., nspdisputeresolution@gmail.com
wrote:

Don Farmer, P. Eng., Dispute Resolution Officer
(D.R.O.)

Telephone (902) 428-6202, Toll-free 1-877-428-6202, Fax (902) 835-7744
nspdisputeresolution@gmail.com

Sean Kelly

In response to your following and attached email messages, I will begin with my Role Statement as Dispute Resolution Officer (DRO) in matters of dispute between N.S.Power and their Customers : **I am not an employee of Nova Scotia Power or the Nova Scotia Energy Board.** I am appointed by Nova Scotia Power to satisfy the Regulations of the Board with respect to dispute resolution. My role is to address, and hopefully resolve, disputes with Nova Scotia Power that cannot be resolved through normal Customer channels. **In my role I investigate N.S.Power's interpretation, and application, of Board approved Regulations. I do not have any jurisdiction over N.S.Power's day-to-day operations.** My Decisions are binding on Nova Scotia Power but not on the Customer. Customers may appeal my Decisions (within 12 days of receipt of Final Written Decision) to the Board.

As your dispute does not relate to a NSUARB approved Regulation, I can not be of assistance to you, other than to advise N.S.Power (via copy of this message) of your concern.

Don Farmer, P.Eng.

Disput

e Resolution Officer

From: Sean Kelly [REDACTED]
Sent: May 26, 2025 7:19 PM
To: nspdisputeresolution@gmail.com
Subject: Data Breach

I am writing on behalf of myself and my wife Michelle Kelly. We live at [REDACTED] Nova Scotia. We have received a letter from NS Power that our data may have been stolen and now we are learning that the information did indeed get published. This is unacceptable and having 2 years of credit coverage is not near enough of a response as we value our privacy. I am writing for several issues.

1. We were not notified if our data had been compromised but that it may be compromised.
2. We had to find out that the data had been published by the media and not by NS Power.
3. There should have been better security on our data and you should have a better communication plan.
4. 2 years credit coverage is not compensation for the privacy breach, it is a damage control measure if there is something done with our data. However our privacy has still been breached.
5. We will accept the 2 year coverage but in no way accept this as settling our case against Nova Scotia Power or Emera.

What we expect.

We expect a fair amount of compensation based on previous data breaches such as the class action settlement with Dell etc.

Please contact me as soon as you can.

Sincerely,
Sean Kelly and Michelle Kelly

[REDACTED]
[REDACTED]
[REDACTED]

General Complaint - NS Power and municipal electric utilities

Reference Number: 250604001

Submitted on: Wednesday, June 04 2025 at 06:40:19 AM (ADT)

Contact Information

Name on account: Jodi Brown

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

I am writing to file a formal complaint regarding the data breach involving Nova Scotia Power (NS Power), which reportedly occurred in March 2025, but was not disclosed to affected customers until over two months later, in May 2025. I am one of approximately 280,000 individuals whose personal information was compromised in this breach. According to the letter I received from NS Power, highly sensitive data, including my Social Insurance Number (SIN), was accessed without authorization. This has caused significant concern, inconvenience, and distress. I believe NS Power's handling of this breach has been insufficient, delayed, and lacking transparency. Key Concerns 1. Delayed Notification A breach involving this level of sensitivity should have triggered immediate disclosure. The significant delay placed affected customers at greater risk of identity theft, fraud, and misuse of personal data. 2. Lack of Transparency The notification provided very little detail. It failed to clearly state what information was accessed, how the breach occurred, and whether our data has been used maliciously.

We are left unsure of what steps to take or what risks we truly face. 3. Inadequate Support NS Power offered 2 years of free credit monitoring via TransUnion of Canada Inc. While somewhat helpful, this offer falls short. Experts in data protection and privacy law have publicly stated that such short-term monitoring is insufficient. As an affected customer, I have had to: Change passwords and personal email accounts Update billing and banking information Monitor credit and financial activity Take personal steps to secure my identity — all at my own expense Endure stress and loss of trust in your service 4. Concerns Over Data Retention Practices Why did NS Power retain highly sensitive data, such as SINS? Was it legally necessary, and were appropriate data minimization and security safeguards in place? Should NS Power be permitted to continue retaining this level of personal information without customer knowledge or consent? I believe a thorough review of your data retention policies and compliance practices is urgently needed. 5. Request for Meter Inspection and Billing Review I am also requesting an inspection of my power meter, as my bills have been unusually high.

Given recent events, my trust in your systems and practices has been compromised, and I would like assurance that I am being billed accurately. Please arrange to have my meter inspected and provide a detailed report of my billing history and usage. What I Am Requesting A full investigation into NS Power's data collection, retention, and security practices Determination of whether NS Power acted in accordance with provincial and federal privacy laws Stronger communication from NS Power outlining: What data was accessed What has been done to secure systems How victims can be fully protected Expanded protection for affected customers, including: At least 10 years of credit monitoring Identity theft insurance A dedicated support line for breach victims Full cooperation with any independent investigation or privacy authority This breach has deeply impacted my sense of security, trust, and financial well-being. I have taken significant steps on my own to protect my identity and accounts, and I now expect NS Power to take full accountability.

Did they contact the utility? No

**How did the utility
respond?**

**How do they want the
complaint resolved?**

**Supporting documents
uploaded:**

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: M12273 FW: Formal Complaint – Mishandling of Personal Information and Inadequate Customer Support
Date: June 6, 2025 7:42:36 AM

-----Original Message-----

From: Ernie Hartling [REDACTED]
Sent: June 4, 2025 3:52 PM
To: Board, NSUARB <Board@novascotia.ca>
Subject: Fwd: Formal Complaint – Mishandling of Personal Information and Inadequate Customer Support

You don't often get email from [REDACTED] Learn why this is important
<<https://aka.ms/LearnAboutSenderIdentification>>

**** EXTERNAL EMAIL / COURRIEL EXTERNE **** Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Elizabeth Hartling

[REDACTED]
[REDACTED]
[REDACTED]
Date: June 4 2025

Subject: Formal Complaint Against Nova Scotia Power – Data Breach, Billing Interruption, and Customer Abandonment

To the Nova Scotia Utility and Review Board,

I am writing to formally submit a complaint against Nova Scotia Power Inc. (NS Power) regarding the company's recent handling of a data breach incident and its lack of customer communication and accountability.

I was recently notified by NS Power via letter that I may have been affected by an identity theft incident, which possibly included exposure of highly sensitive personal data such as my Social Insurance Number, financial and banking information, and my full identity profile.

Following this, NS Power has ceased all direct customer service, instead directing me to TransUnion for credit protection. For over three months, I have not received a power bill, and I have had no way to speak with a representative about my account status, service, or the potential breach. I have been assured via automated message that I will not be charged interest during this time, but this is little comfort in the face of such a serious breach of privacy and complete lack of transparency.

As a customer of NS Power for over 30 years with a flawless payment history, I feel abandoned and betrayed. The lack of access to basic customer support, paired with the magnitude of a potential identity theft, raises serious concerns about the utility's obligations to ratepayers and public accountability.

I respectfully request that the NSUARB:

1. Investigate NS Power's conduct during this data breach incident;
2. Require NS Power to restore full transparency and communication with affected customers;
3. Examine whether customers are entitled to financial compensation or restitution for the harm caused;
4. Consider whether NS Power is meeting its regulatory obligations to its ratepayers.

I am also submitting a complaint to the Office of the Privacy Commissioner of Canada and taking steps to protect myself independently. However, I believe NSUARB has a duty to ensure that NS Power remains answerable to the public it serves.

Thank you for your attention.

(See Below the email to NS Power)

Sincerely,
Elizabeth Hartling

Begin forwarded message:

From: Ernie Hartling [REDACTED]
Date: May 21, 2025 at 1:48:00 PM ADT
To: customerservice@nspower.ca
Subject: Formal Complaint – Mishandling of Personal Information and Inadequate Customer Support

Elizabeth Hartling
[REDACTED]

May 21, 2025

Customer Service
Nova Scotia Power Inc.
P.O. Box 910
Halifax, NS B3J 2W5
customerservice@nspower.ca

Dear Nova Scotia Power,

I am writing to express my deep concern and disappointment regarding a serious issue that has significantly impacted me as a long-standing and loyal customer of Nova Scotia Power.

Recently, I received written notification from NS Power indicating that my personal information — including, potentially, my Social Insurance Number, banking details, date of birth, and mailing address — may have been compromised due to a security incident. This is alarming, especially considering the highly sensitive nature of this data and the potential for identity theft.

To make matters worse, I have not received a power bill in over three months, and all attempts to reach your customer service department by phone have been met with automated redirection to TransUnion. I was instructed that NS Power is not accepting calls while this matter is “under review.” As someone who has been a reliable customer for over 30 years and has never missed a payment, I find this complete lack of communication and support deeply troubling and unacceptable.

I also feel coerced into setting up an online account back in December due to concerns over a Canada Post disruption. This incident occurred shortly afterward, leaving me to believe that this digital transition may have been connected to the breach.

At this point, I am left in a state of uncertainty about my financial safety, my service status, and how or when this will be resolved. NS Power has offered no clear direction, no direct communication, and no support. While I

have been told there will be no late fees while this is sorted out, that is not sufficient reassurance — nor is it any form of accountability for the stress and potential harm I now face.

I am formally requesting:

1. A full explanation of how this breach occurred and what data of mine was compromised.
2. Immediate restoration of billing communication in a secure format.
3. Written confirmation that my credit and account status will not be negatively impacted.
4. An apology for the failure to provide accessible customer service during this critical time.
5. Consideration of financial compensation for the stress, potential identity theft exposure, and loss of access to services and support.

I expect a formal response to this complaint within 14 days. If no satisfactory response is received, I will escalate the matter to the Nova Scotia Utility and Review Board, the Office of the Privacy Commissioner of Canada, and other relevant bodies.

I hope NS Power will do the right thing and take this matter seriously.

Sincerely,
Elizabeth Hartling

General Complaint - NS Power and municipal electric utilities

Reference Number: 250604002

Submitted on: Wednesday, June 04 2025 at 05:41:05 PM (ADT)

Contact Information

Name on account: Lesley Hartman

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

I am writing to formally complain about Nova Scotia Power's handling of its recent security breach. According to the letter Nova Scotia Power sent, my personal information was affected, though the letter didn't specify exactly what information was taken. I am deeply concerned about both the theft of my personal information and Nova Scotia Power's inadequate response to this serious security breach. According to their letter: My personal data was stolen by an unauthorized third party on or around March 19, 2025. Nova Scotia Power discovered this breach on April 25, 2025. Nova Scotia Power didn't notify me of the breach or that my information had been stolen until May 13, 2025 – two months after the breach and almost one month after your organization knew about it. As mentioned, I received their notification letter on May 23, 2025. While their letter acknowledged that my personal data had been stolen by an unauthorized third party, it didn't meet acceptable standards for breach notification in several important ways: Lack of Specific Information: The letter mentioned broad categories of compromised data but didn't specify what particular information was stolen.

As a victim of the company's security breach, and according to the Personal Information Protection and Electronic Documents Act (PIPEDA), I have a legal right to know the full scope of my personal data exposure. Only today, when I finally got through to their incident response line, was I advised that my SIN number was breached because my letter included Social Insurance Number in the list of possibly breached information. I was advised that the other list of breached items was a generic list except for the SIN. I was informed that two generic letters had been sent out; one included the SIN and one did not. The letter was misleading and vague; despite the company knowing that my SIN was breached, that was not stated. No Guidance on Next Steps: their letter provided no guidance on what steps to take to protect myself from potential identity theft or fraud resulting from this breach. Minimal Support and Resources: The only support Nova Scotia Power offered was "... a dedicated phone number 1-844-818-0376 for customers who have questions about this incident," and a code to set up an account with TransUnion credit monitoring services.

When I called the number, I was connected with TransUnion. This limited response is not enough support for victims of a data breach of this size. Maintenance of my SIN online without my consent, and despite this being wholly unnecessary: I have been a NS Power customer for 30+ years. This means that the company was provided my SIN before electronic data storage, which means that this sensitive information was transferred online and stored for that long without my consent. In closing, I request that you urge Nova Scotia Power to: Provide me with a detailed, specific account of exactly what personal information of mine was compromised in this breach. Explain the delay between discovering the breach (April 25) and notifying me (May 13). Offer comprehensive identity protection services beyond basic credit monitoring, and for an adequate length of time (I have been advised by experts that I could experience identity theft at any point over the course of my lifetime). Provide clear, detailed guidance on all steps I should take to protect myself from potential consequences of this data exposure.

Implement improved cybersecurity protocols and procedures, and explain what those are, to ensure any future incidents are handled quickly, transparently, and appropriately. Data security breaches are serious and can have lasting consequences for those of us affected by them. Nova Scotia Power's customers deserve better protection of their personal information and, when breaches happen, a response that prioritizes speed, transparency, specific details, and comprehensive support. The utility's current approach doesn't adequately address the legitimate needs and concerns for specific information about my stolen data. I look forward to your reply. Sincerely, Lesley Hartman

Did they contact the utility? Yes

How did the utility respond?

How do they want the complaint resolved?

I request that you urge Nova Scotia Power to: Provide me with a detailed, specific account of exactly what personal information of mine was compromised in this breach. Explain the delay between discovering the breach (April 25) and notifying me (May 13). Offer comprehensive identity protection services beyond basic credit monitoring, and for an adequate length of time (I have been advised by experts that I could experience identity theft at any point over the course of my lifetime). Provide clear, detailed guidance on all steps I should take to protect myself from potential consequences of this data exposure. Implement improved cybersecurity protocols and procedures, and explain what those are, to ensure any future incidents are handled quickly, transparently, and appropriately. Data security breaches are serious and can have lasting consequences for those of us affected by them. Nova Scotia Power's customers deserve better protection of their personal information and, when breaches happen, a response that prioritizes speed, transparency, specific details, and comprehensive support.

The utility's current approach doesn't adequately address the legitimate needs and concerns for specific information about my stolen data.

Appeal - NS Power Dispute Resolution Officer (DRO)

Reference Number: 250605001

Submitted on: Thursday, June 05 2025 at 03:14:19 PM (ADT)

Contact Information

Name on account: Danielle Maillet

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

DRO made decision on: 00/00/0000

Type of complaint: Billing Issues

Additional details: I am writing to formally raise a complaint regarding Nova Scotia Power's recent failure to provide reliable service access, their handling of a data breach, and billing practices that I believe fall short of the standards required of a regulated utility. I've emailed their complaints resolution team on May 28th, but I've yet to receive a reply. Since their system breach in April 2025, I have experienced ongoing issues accessing my NS Power online account. This includes the inability to review my billing history, track usage, or manage payments. These disruptions have continued for weeks, and I have received no adequate or proactive communication from NS Power regarding timelines, transparency, or my rights as a consumer. Most recently, I was issued a large bill with no prior notice, explanation, or ability to verify or dispute the charges online. I had no access to usage data or historical comparisons, which I consider essential for fair and informed billing. To make matters worse, NS Power has offered a complimentary two-year TransUnion "myTrueIdentity" credit monitoring subscription as a supposed remedy for the privacy breach.

This subscription retails for nearly \$600 over two years, yet I was never asked whether I wanted this third-party service. Many Canadians already receive similar coverage at no cost through their banks or credit card providers. I believe this "compensation" is not only inadequate but also inappropriate, especially in lieu of offering direct support such as billing relief or customer credits. To add to this, since the breach with NSPower, I've had security issues related to my personal bank, which have never occurred beforehand. I respectfully request the Board to investigate the following: Whether NS Power is fulfilling its obligation to provide accessible, transparent billing tools and account management. Whether its billing during a period of service disruption is fair and justifiable. Whether the use of a third-party identity monitoring service as compensation—without customer consent—meets the ethical or regulatory expectations for a provincial utility. What remedies or relief should be offered to customers impacted by the ongoing system outage and privacy breach. As a consumer and ratepayer, I believe NS Power should be held to a higher standard, particularly when handling private data and billing responsibilities.

I hope the Board will review this matter with the seriousness it deserves and help restore transparency and accountability. Sincerely, Danielle Kristine Maillet

How do they want the complaint resolved?

To summarize, I am demanding the following: A full waiver of my current bill, which I consider unreasonably high given the service and communication failures. A credit of \$598.80 (+ tax) to my NS Power account, in place of the unsolicited TransUnion subscription. A freeze or waiver on all future charges until full online access to account services has been restored and proven secure. Written confirmation that no late fees, interest, or negative credit impacts will apply during this disruption period.

Supporting documents uploaded:

- Notice - NSPower - Danielle Maillet - May 28th 2025.pdf

Danielle Kristine Maillet

NSPower Account #: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

To: NS Power Customer Service

CC: Privacy Office, Billing Department, Legal Department

Re: Data Breach, Billing Disruption, and Compensation Demand

Dear NS Power,

I am writing to formally express my serious concern over NS Power's recent data breach and the continued inaccessibility of your online account services, which have directly impacted my ability to manage my account and access my billing.

For several weeks now, I have been unable to access my online account, receive proper billing notices, or make informed decisions about my energy usage and payments. During this period, I have now received a substantial bill with no warning or ability to track or dispute it in real time.

Additionally, your offer of a complimentary two-year subscription to *TransUnion myTrueIdentity*, as stated in your letter, is not an appropriate remedy. This service retails for \$24.95 per month, totaling **\$598.80 plus applicable taxes**. I neither requested this service nor find it of any practical or trustworthy value, especially as many consumers already receive comparable or better protection through their banking institutions at no cost. As such, I am **formally demanding** this amount be **credited directly to my NS Power bill** in lieu of an unwanted third-party service.

To summarize, I am demanding the following:

1. A **full waiver of my current bill**, which I consider unreasonably high given the service and communication failures.
2. A **credit of \$598.80 (+ tax)** to my NS Power account, in place of the unsolicited TransUnion subscription.
3. A **freeze or waiver on all future charges** until full online access to account services has been restored and proven secure.

4. Written confirmation that no late fees, interest, or negative credit impacts will apply during this disruption period.

If I do not receive a satisfactory resolution within **5 business days**, I will escalate this matter by filing complaints with:

- The **Office of the Privacy Commissioner of Canada**
- The **Nova Scotia Utility and Review Board**
- And I will be seeking **legal consultation** regarding a potential claim stemming from your mishandling of personal information and the prolonged disruption of service access.

I expect a written response outlining next steps and your resolution plan.

Sincerely,

Danielle Kristine Maillet

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Assistance
Date: June 9, 2025 8:50:35 AM

From: [REDACTED]
Sent: June 6, 2025 4:44 PM
To: Wallace, Lisa <Lisa.Wallace@novascotia.ca>
Subject: Assistance

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hi Lisa,

My name is Sabrina Walker. I am a customer of Nova Scotia Power. I was not able to become a customer unless I sent copies of my ID to them. I did so in March.

As you know they had a breach. I did not receive any letter or anything. I called today to see if I had been one of the customers breached. They could not tell me when I first called. I asked to speak with a supervisor. I was told it was not possible. I was told there wasn't one.

The employee stated he would get me a call back from the supervisor. I asked if I could have a reference number or incident number for the call. He refused, and said there wasn't one. I asked who they answered to and then he said he'd get a supervisor. I said I thought there wasn't one, he backtracked and said there wasn't. The conversation could be referenced in a master class in futility.

I am disabled. If someone uses my ID nefariously I will suffer immeasurably. As a disabled person I already get blamed for things I didn't do. I can't afford any costs incurred, I can barely afford food.

I got a call back from the same rep, not his supervisor and was told that I wasn't one of the people hacked.

I don't think allowing the same people who messed up in the first place be responsible for the "clean up" and disclosure is a good practice. They have more to gain from not telling people than telling people.

I would like to ask that you address the issues of reporting and of not having reference numbers for customers for accountability with future issues that may occur because of their negligence.

I understand that these security issues are frequent in almost every field now. I would just like to ensure nothing nefarious happens using my ID. I don't want harm to come to anyone because of me, or my name.

Thanks,

Sabrina

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Nova Scotia Power Cyber Incident
Date: June 10, 2025 11:52:00 AM

From: [REDACTED]
Sent: June 10, 2025 10:25 AM
To: Board, NSUARB <Board@novascotia.ca>
Subject: Nova Scotia Power Cyber Incident

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Good Day,

I am writing this morning about the recent Nova Scotia Power cyber incident.

After this issue came to light, NSP sent a form letter to customers advising what general kinds of information may have been accessed. It is my strong opinion that NSP should be expected to provide each customer with a detailed list of the personal information that was part of the hack. For example, I have no idea whether NSP had my SIN in their records. The steps people need to take to protect their personal information will depend on exactly what was stolen. I sent an email to the NSP Privacy Officer several weeks ago, but have not received even an acknowledgement of receipt of it.

In today's world it is possible for any organization to have its computers hacked, but NSP should be accountable for providing full disclosure to its customers and regulatory bodies. They should also be forced to explain why they were holding customer SINs in their files. It is unbelievable that they have been allowed to not give a proper answer to this question. Infuriating.

Best regards,

Clarence Whynot

[REDACTED]

General Complaint - NS Power and municipal electric utilities

Reference Number: 250610001

Submitted on: Tuesday, June 10 2025 at 04:10:04 PM (ADT)

Contact Information

Name on account: Ben Filipkowski

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

NS Power's response to a major a cybersecurity incident that led to the release of customer personally identifiable information is completely unacceptable. NS Power's response to valid questions and mounting public frustration over not only their handling of PII but the lack of accountability is unacceptable. Customers should not be on the hook for any losses accrued as a result of this outage.

Did they contact the utility? No

How did the utility respond?

How do they want the complaint resolved?

NS Power should not be permitted to increase rates to compensate themselves for the costs of their failures.

Supporting documents uploaded:

From: [Board, NSUARB](#)
To: [Henwood, Crystal D](#)
Cc: [Painting-MacLean, Kimberly](#)
Subject: FW: Matter # M12273
Date: June 18, 2025 8:10:51 AM

From: Susanne Roy [REDACTED]
Sent: June 17, 2025 4:41 PM
To: Board, NSUARB <Board@novascotia.ca>
Subject: Matter # M12273

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

To whom it may concern

I am writing to express my concerns about the data breach at Nova Scotia Power and their response to this serious matter. I entrusted my personal information to this company and am very concerned they did not properly protect this information and now it is on the dark web with no idea of who has access to it which will cause me to worry for the rest of my life about people using this information to ruin my credit or possibly commit crimes using my identity.

While Nova Scotia Power is busy patting itself on the back saying they are giving affected customers two years of credit monitoring I am left wondering what is to happen once that two years is up. Am I expected to shoulder the cost of now paying for this service since my information is out there forever? I feel that I am left to worry for the rest of my life about what is happening to my information while Nova Scotia Power walks away from this after two years.

I am not sure of what power you have over this company and the terrible position they have placed their customers in but feel that they should be paying for a lifetime of credit monitoring services to ease our minds.

Yours Truly,
Susanne Roy

From: [Board, NSUARB](#)
To: [Henwood, Crystal D](#)
Cc: [Painting-MacLean, Kimberly](#)
Subject: FW: Fraud protection
Date: June 18, 2025 11:44:03 AM
Attachments: [image001.png](#)

From: [REDACTED]
Sent: June 18, 2025 11:41 AM
To: Peter Gregg <peter.gregg@nspower.ca>
Subject: Fraud protection

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercice caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

June 18, 2025,

Dear President of Nova Scotia Power,

I am writing to express my deep frustration with Nova Scotia Power regarding their handling of personal data security and fraud protection. Their offer to cover fraudulent activity on my account for only two years is entirely unsatisfactory.

I firmly believe that NSP should take full responsibility for any fraud resulting from this issue, regardless of how many years have passed. It is unacceptable for customers to bear the consequences of their security lapses. As a consumer, I expect a commitment to long-term accountability and robust protection of personal information.

I urge you to address this matter with the seriousness it deserves and ensure that Nova Scotia Power implements policies that provide ongoing protection for affected customers.

Sincerely,
John Robert Bona



Cc'd – Claudia Chender NDP, Derek Mombourquette Liberal, Kody Blois MP, John MacDonald MLA, NS Energy Board, Tim Houston Premier, Scott Balfour CEO Emera, Mark Carney Prime Minister.

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Accountability and Transparency
Date: June 27, 2025 3:41:47 PM

From: J Char [REDACTED]
Sent: June 27, 2025 10:50 AM
To: Board, NSUARB <Board@novascotia.ca>
Subject: Accountability and Transparency

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Accountability breeds Responsibility, while Transparency increases credibility and fosters open communication. I agree with this as sure you will. Is it important to teach our children these principles.

Yet while we look to keep these principles close to the heart, sometimes we appear to forget; however, we always strive to achieve and improve them.

In light of the responsibilities, Nova Scotia Power is going through a major data breach. Open communication is very very important with their clients in Nova Scotia. It is not only essential but is vital.

Unfortunately this is not happening NS Power has little capability in this matter. The only way a customer can reach out to NSP is by phone and this has its issues not only for clients but also for NSP.

Major organizations like Bell, Telus, BMO, Eastlink, Manitoba Hydro, Hydro One in Ontario, etc. all allow multiple ways for customers to contact them. All strive for open communication and transparency.

Some have online templates where customers can enter text where there would be no security risk to their systems. Others accept email.

Is it possible to request NSP to improve this relationship or have this issue brought table for discussion?

I am sure many Nova Scotians would agree that more openness and transparency including being

able to reach out to NSP especially in times like a major data breach would go along way in improving social responsibility.

Please let me know if this is a concern to the Board. All I am really asking and if you are correct point of contact that it be discussed within your group. The situation with NSP may not change I understand.

Jim Charumski



General Complaint - NS Power and municipal electric utilities

Reference Number: 250627001

Submitted on: Friday, June 27 2025 at 05:13:06 PM (ADT)

Contact Information

Name on account: Sheldon L Glick

Account number: *****

Business contact: n/a

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

corporate responsibility: 1) why did the NSP inform myself of a cyber attack and cover the customer for 2 yrs by email but NO EMAIL for the 5 year coverage. 2) if one does not have overdraft protection they would be charged a penalty (because of double billing) what is the NSP to do. I was informed that they would cover it. So where is the email. NO EMAIL NSP wants to not inform the customers or the public (it's, lets be quiet let's not inform the public of what we can do)

Did they contact the utility? Yes

How did the utility respond?

How do they want the complaint resolved?

self evident in my comments

Supporting documents uploaded:

-----Original Message-----

From: Betty [REDACTED]

Sent: July 17, 2025 3:16 PM

To: Board, NSUARB <Board@novascotia.ca>

Subject: CBC News : What's going on with Nova Scotia Power's billing in wake of ransomware attack

[You don't often get email from [REDACTED] Learn why this is important at <https://aka.ms/LearnAboutSenderIdentification>]

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

<https://can01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cbc.ca%2Fnews%2Fcanada%2Fnova-scotia%2Fnova-scotia-power-billing-1.7584646&data=05%7C02%7CKimberly.Painting-MacLean%40novascotia.ca%7C08c992d35d15485d98c208ddc9102247%7C8eb23313ce754345a56a297a2412b4db%7C0%7C0%7C638887793304809278%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMilslkFOljo1TWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=RSuO5UVxleHBkh9Nk%2F%2Bum5jP%2BsyKsZXzSilkc2B8UR8%3D&reserved=0>

INCOMPETENT NOVA SCOTIA POWER NEEDS TO BE COMPLETELY INVESTIGATED FROM TOP TO BOTTOM 🤬🤬👎🤬🤬👎 NON-STOP OVER BILLING BILLS COMING ALMOST EVERY WEEK!!!!!!!!!!!!

NO COMPETITION EQUALS ROBBERY.

Betty Ann O'Halloran

General Complaint - NS Power and municipal electric utilities

Reference Number: 250718001

Submitted on: Friday, July 18 2025 at 07:11:18 AM (ADT)

Contact Information

Name on account: Gregory B MacKenzie

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

I received a letter from NSPower dated May 13, 2025 in which I was told "certain customer information stored on the impacted servers was accessed and later taken by an unauthorized third party." NSP did not identify what information of mine was taken. I have to assume critical information including my Social Insurance Number was taken. The problem with NSPs response is that two years of credit monitoring is completely unsatisfactory as this is going to affect the rest of my life and NSP gets to walk away after two years without any consequences or responsibility. This has to be addressed and a solution provided for NSP customers which resolves this situation in a way that protects us.

Did they contact the utility? No

How did the utility respond?

How do they want the complaint resolved?

NSP has to assume responsibility and shield customers, whose information was stolen, over the remainder of their lives from the consequences of that data breach.

Supporting documents uploaded:

From: Tim Leary [REDACTED]
Sent: July 18, 2025 4:18 PM
To: Privacy Officer <privacy.officer@nspower.ca>
Cc: Board, NSUARB <Board@novascotia.ca>
Subject: Re: Nova Scotia Power Cyber Incident

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

To: "Privacy Officer" (otherwise unnamed) at Nova Scotia Power

From: Timothy Leary, N.S. Power customer in Halifax

RE: Your letter to me (contained herein, below)

CC: NSUAB

Following two previous attempts to get a NS Power official to contact me with information I've requested, and having been promised that I would receive a call from NS Power, my third attempt appears to have resulted in your letter to me (below) to which this is my response. My request was simply that you give me the precise information that NS Power has on file on my account. Your letter provides various categories of information that you *may have* and that *may have* been compromised in the breach of your security. You state "... it is not possible to determine precisely what specific personal information, if any, of yours was affected as a result of this incident." However, I did not ask for what information was *affected*, I asked precisely *what information you have on file* on my account that was on file when the breach occurred.

I must assume that when this "incident" occurred, the information did not disappear or somehow evaporate: it must still be in your records, retrievable, and I would like to know what it is. I believe it is my right to have that information.

Further, your letter gives some instruction on contacting the organization that is charged with credit monitoring, or using your verification system to access that organization (TransUnion). Unfortunately, I am unable to get verification - the system rejects my attempts, stating I cannot be verified. I do not recall if I had signed onto the credit monitoring program as suggested in your first letter to me about the "incident." Also, I do not see a way to get in touch with TransUnion.

I look forward to your providing timely solutions to these two outstanding issues.

Yours truly,

Timothy Leary

+++++

On 2025-07-15 3:01 p.m., Privacy Officer wrote:

Dear Mr. Leary,

We are writing in response to your request for a detailed account of what personal information of yours may have been compromised in the cyber attack that recently affected Nova Scotia Power's systems.

First, we want to assure you that protecting your personal information remains our highest priority. We understand the seriousness of this situation and appreciate your patience as we continue our investigation with the support of cybersecurity experts.

Unfortunately, at this time it is not possible to determine precisely what specific personal information, if any, of yours was affected as a result of this incident. Due to the nature of the breach and the complexity of the systems involved, and despite our comprehensive investigative efforts, the data cannot be definitively identified on an individual basis.

However, if we are able to determine more specific information in the future, we remain committed to keeping our customers informed and will communicate any material updates directly.

From our investigation, we do know that the server that was accessed by the unauthorized third party held various types of personal information of our customers that included 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 SIN. 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. The types of affected information depended, in large part, on the information that a customer provided to Nova Scotia Power.

While we continue to work diligently to understand the full scope of the breach, we strongly encourage you to sign up for the five-year subscription to TransUnion's comprehensive credit monitoring service that has been provided by Nova Scotia Power. Details on how to activate your subscription are set out in the notice you would have received by mail. Even if you did not receive a letter from us, Nova Scotia Power is also now 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. To receive your unique activation

code that will enable you to sign up for credit monitoring, please use our Customer Verification Form available on our website (<https://www.nspower.ca/home---cyber/customer-verification-form>).

In addition, we encourage you to take other precautions to help safeguard your information, including monitoring your financial accounts for unusual activity, placing fraud alerts on your credit files, and being cautious of unsolicited communications that ask for personal or financial information.

We apologize that this has happened and thank you for your patience as we work through this incident.

Regards,

Privacy Officer | Nova Scotia Power

1223 Lower Water Street | Halifax, NS B3J 3S8

E: privacy.officer@nspower.ca



Before printing this e-mail, please consider if it is necessary to do so.

Confidentiality Notice - The email communication is considered confidential and is intended only for the recipient(s). If you received this email in error, please contact the sender and delete the email. Unauthorized disclosure or copying of this email is prohibited.

Attachment Limits - Emera will not accept email larger than 50MB or emails containing high risk attachments like ZIP, EXE or others that could contain viruses. If you have a business need to send such an email, please contact the recipient for instructions.

--

Tim Leary

Crispulanti bis circa pateram et accuminatum in utraque extremitate

From: [Henwood, Crystal D](#)
To: [Henwood, Crystal D](#)
Subject: FW: Complaint
Date: August 11, 2025 9:30:28 AM

From: Mike Balcom <[REDACTED]>
Sent: August 8, 2025 3:29 PM
To: home@nspower.ca
Cc: Board, NSUARB <Board@novascotia.ca>; Premier <PREMIER@novascotia.ca>;
[REDACTED]
Subject: Complaint

Some people who received this message don't often get email from [REDACTED]. [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

To NS Power, copy to Nova Scotia Energy and Regulatory Boards Tribunal, copy to Premier Houston, copy to Brian Wong, my MLA

Hello

Back in May I received the NS Power letter regarding the cyber incident. I tried setting up an account with TransUnion online as the letter requested. That didn't work and I was told to call a number. I called that number and there was a wait so I was told I would receive a call back. Someone called me back a couple hours later. She told me her computer wasn't working and I would have to call the number again to be put back in the queue. I asked her why she called me back if her computer wasn't working and she said that is how their system works and there was nothing she could do about it, I needed to call back. I was extremely frustrated with the whole system.

Today, after 3 months I found the letter again and decided to try again. I tried going to mytrueidentity.ca on my computer, I had an email and password already entered so I entered that and was told my account has been suspended. That response is below. I called that number and spoke to a lady who asked me to update my security question, she asked me my grandfather's name. I gave it to her and she said she updated it but I then had to call 1-800-663-9980 to update the security question. I asked why she couldn't as she just added it, She said she couldn't, I needed to call the number. I called that number and spoke to a guy who asked me all the questions again and then put me on hold and came back and said he couldn't help. I needed to call 1-888-228-4939. I called that number, same thing, questions, I was put on hold again then he came back and said he couldn't help. I need to call 1-800-663-9980 and they would help for sure. I told him that is who gave me your number and they couldn't help.

Then I called NS Power who listened to my story but was again unable to help, he gave me a number 1-844-818-0376 to call. I called that number, again the same response after 20 minutes and the same questions, they couldn't help. He transferred me to someone else who again couldn't help but told me to call 1-855-889-4293. I called that number and they were unable to help. I asked for an email address so I could add them to this complaint but she said they won't disclose their email address. Obviously this is because of the number of complaints they would receive.

I am retired and I have spent a good part of a day trying to get an account with them, I give up. What about all the people that don't have the time I have?

I now expect NS Power to resolve this issue on my behalf as you have hired this company. I also must say that everyone I spoke to at TransUnion I could hardly understand, I try not to be racist and it certainly isn't their fault, they are just doing a job. I even apologized to one guy and said you probably don't understand me any better.

I am expecting a reply from NS Power and Nova Scotia Energy and Regulatory Boards Tribunal the as the regulator of NS Power.

Mike Balcom



Your myTrueIdentity account has been temporarily suspended.

In order to protect your privacy, access to your account has been temporarily suspended.

What to do now:

- Contact any of our customer service representatives Monday through Friday, 8:00 a.m. - 8:00 p.m. ET, except holidays at 1-888-228-4939



General Complaint - NS Power and municipal electric utilities

Reference Number: 250814001

Submitted on: Thursday, August 14 2025 at 01:19:34 PM (ADT)

Contact Information

Name on account: David MacLeod

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:	Other
Additional details:	The NSP cyber breach occurred on 19 March 2025, but NSP only became aware on 25 April 2025, 37 days later. My notification was received 63 days after the event. By failing to act in a timely way, NSP has failed to adhere to the intent of the Personal Information Protection and Electronic Documents Act (PIPEDA). NSP customers were exposed for months. NSP cannot call this effective notification. On 26 May 2025, I wrote to NSP's Privacy Officer requesting what information of mine had been captured by the cyber criminals. On 13 June 2025, 18 days later, I received an email from the Privacy Officer and was informed that another 30 days was required. I waited until 18 July and complained in a letter to Peter Gregg. On 24 July, the NSP Privacy Officer sent me an email in which a screen shot of my billing information was enclosed. This tardy and incomplete response hardly met the purpose, in that I had to provide my SIN to NSP when I bought my home in 2009.
Did they contact the utility?	Yes
How did the utility respond?	
How do they want the complaint resolved?	I require a complete answer concerning my information liability and exposure. In other words, what information of mine did the cyber criminals take?
Supporting documents uploaded:	• NSP Privacy Officer.pdf • 2025-07-18 Peter Gregg.docx

Thursday, August 14, 2025 at 1:17:29 PM Atlantic Daylight Time

Subject: RE: Cyber Breach
Date: Thursday, July 24, 2025 at 16:47:58 Atlantic Daylight Time
From: Privacy Officer
To: David MacLeod
Attachments: David Mac_Redacted.pdf

Dear David MacLeod,

This email is in response to your request to access your personal information held by Nova Scotia Power.

As previously communicated, we required additional time to gather and review your records and we appreciate your patience and understanding. Please be assured that we take your privacy seriously and are committed to responding in accordance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

With additional time, we were able to gather the attached records associated with your account. In accordance with PIPEDA, please note that we have redacted personal information within these records that would contain personal information of another individual.

Due to the recent cyber incident, certain IT systems remain inaccessible. If you would like us to search these systems once access is restored and provide you with records containing your personal information (if any), please let us know. We will then follow up with you when access to them is restored.

Regards,

Privacy Officer
Nova Scotia Power Incorporated

From: David MacLeod [REDACTED] >
Sent: Monday, May 26, 2025 1:33 PM
To: Privacy Officer <privacy.officer@nspower.ca>
Subject: Cyber Breach

[REDACTED]

David T. MacLeod CD MA

[REDACTED]

26 May 2025

Nova Scotia Power Privacy Officer
PO Box 910
Halaifax, NS
B3J 2W5

RE: Nova Scotia Power (NSP) Cyber Breach

Nova Scotia Power (NSP) knows, or should know, that Canada is a target for cyber criminals and hostile governments such as China, Russia, Iran, and North Korea. NSP, a critical infrastructure corporation, failed to adequately protect our information.

Intruders can breach security in a matter of minutes. Yet, the NSP breach occurred on 19 March 2025, but NSP only became aware on 25 April 2025, 37 days later. Some notifications to customers were received 63 days after the event. By failing to act in a timely way, NSP failed to adhere to the intent of the Personal Information Protection and Electronic Documents Act (PIPEDA). NSP customers were exposed for months. NSP cannot call this effective notification.

Clearly, NSP's system lacked sufficient monitoring and threat hunting. Security procedures like real-time threat detection, intrusion hunting, and behavior analysis are effective against attacks. A zero-trust architecture can stop social engineering attacks. I'm informed that these procedures are not fully employed by NSP.

Questions where I require an immediate answer:

- Is the data breach ongoing?
- Why was there a delay in response? (The breach occurred on 19 March 2025, but NSP only became aware on 25 April?)
- How were your security procedures bypassed? (For example, social engineering, malware, tech failure etc.)
- Was this a deliberate attack or was this human error?

I request that NSP provide:

- Detailed list of my information that was accessed.
- The NSP account is in my name, but my wife pays this bill. Was my wife's information compromised? (Katarin MacLeod).

In a hostile 21st century, it is only reasonable to expect critical infrastructure corporations to protect my information.

David T. MacLeod CD MA

Attachment Limits - Emera will not accept email larger than 50MB or emails containing high risk attachments like ZIP, EXE or others that could contain viruses. If you have a business need to send such an email, please contact the recipient for instructions.

David MacLeod



18 July 2025

Peter Gregg
1223 Lower Water St,
Halifax, NS, B3J 2S8

Dear Peter Gregg,

Why should I pay my power bill? I realize the question seems trite, but it is sincere. Months after Nova Scotia Power's (NSP) cyber incident, I still do not know what data of mine was compromised.

As of 18 July 2025, the NSP website states NSP does not know, or is unwilling to reveal, an individual's information liability caused by NSP's cyber incident.

"The types of impacted personal information varied by individual customer and may have included your customer account history, such as power consumption, service requests, payments, billing and credit history, and customer correspondence."

The NSP cyber incident occurred on 19 March 2025, but NSP only became aware on 25 April 2025, 37 days later. My notification arrived 63 days after the event. On 26 May 2025, I wrote to NSP's Privacy Officer requesting information. On 13 June 2025, 18 days later, I received an email from the Privacy Officer and was informed that another 30 days was required. It has been 35 days since the Privacy Officer's email and still no reply or update.

As of the date of this letter, I have waited 121 days to have NSP identify to me what information of mine was taken.

My original question remains: why should I pay my power bill? NSP appears unwilling, or unable, to reveal what data of mine was stolen. It feels as though my data, and data exposure, is being held hostage by both cyber criminals and Nova Scotia Power.

I eagerly await your written reply.

David T MacLeod CD MA



General Complaint - NS Power and municipal electric utilities

Reference Number: 250908001

Submitted on: Monday, September 08 2025 at 11:27:25 PM (ADT)

Contact Information

Name on account: Nathan Smart

Account number: *****

Business contact:

Account address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Email Address: *****

Mailing address:

Address 1: *****

Address 2: *****

City: *****

Province: *****

Postal code: *****

Country: *****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

I was notified that my personal information was compromised in the spring 2025 data breach and was sent a link for identity theft protection. Not only did this link not work, but even after numerous phone calls, I was unable to register for the protection service. This a huge waste of my time trying to resolve a problem that NSP created, and I am deeply concerned that my identity has already been compromised while I have no way of protecting myself.

Did they contact the utility? Yes

How did the utility respond?

How do they want the complaint resolved?

I would like to be registered for the credit protection I'm entitled to, and compensated for undue stress and time I've wasted trying to navigate their faulty registration system.

Supporting documents uploaded:

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: Complaint Regarding Lack of Customer Communication on NS Power's Free TransUnion Credit Monitoring
Date: September 10, 2025 10:32:58 AM

From: Michelle Boutilier [REDACTED]
Sent: September 9, 2025 7:39 PM
To: Board, NSUARB <Board@novascotia.ca>
Subject: Complaint Regarding Lack of Customer Communication on NS Power's Free TransUnion Credit Monitoring

You don't often get email from [REDACTED]. [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

To the Nova Scotia Utility and Review Board,

I am writing as a Nova Scotia Power customer to raise a concern about how NS Power is handling its response to the recent cyber incident.

While NS Power has made five years of free TransUnion credit monitoring available to all current and former customers, the company has failed to provide direct communication or clear instructions to customers on how to access this service.

Instead, NS Power has relied on customers to discover this information on their own through its website or scattered media coverage. Many customers will never know they are eligible, which defeats the purpose of offering credit monitoring in the first place. I had to ask ChatGPT how I get it because I was wondering why I never got any mail or email with instructions after hearing about it in the media previously.

Given the seriousness of a data breach and the risk of identity theft, I believe NS Power should be required to:

1. Proactively notify all customers—past and present—about their eligibility.
2. Provide clear step-by-step enrollment instructions via mail or email to every account holder.

3. Demonstrate accountability by documenting how they have informed customers, instead of relying on self-discovery.

I am requesting that the Utility and Review Board review this matter and hold NS Power to a higher standard of customer communication. Customers deserve transparency and accessible protections, not hidden links buried on a website.

Thank you for your attention to this concern.

Michelle Boutilier; 



General Complaint - NS Power and municipal electric utilities

Reference Number: 250913001

Submitted on: Saturday, September 13 2025 at 10:52:17 AM (ADT)

Contact Information

Name on account: David MacLeod

Account number: *****

Business contact:

Account address:

Address 1:	*****
Address 2:	*****
City:	*****
Province:	*****
Postal code:	*****
Country:	*****

Email Address: *****

Mailing address:

Address 1:	*****
Address 2:	*****
City:	*****
Province:	*****
Postal code:	*****
Country:	*****

Telephone number: *****

Alternate phone number: *****

Complaint Information

Type of complaint:

Other

Additional details:

Primary Complaint is attempted Secrecy. On July 18, 2025, I wrote to Peter Gregg and asked a simple, sincere question: “Why should I pay my power bill?” Months after Nova Scotia Power’s (NSP) cyber incident, I still do not know what data of mine was compromised. NSP has asked for secrecy in the cybersecurity inquiry, and now it is asking ratepayers to pay more. NSP owes Nova Scotians an apology, a full explanation, and a moratorium on any rate increase for at least two years. The warnings were clear and repeated. Canadian cyber threat bulletins have long identified the electricity sector as a persistent target of state sponsored cybercriminals. The threat actors named in those bulletins include groups tied to China, Russia, and Iran. Attacks on utilities are rarely opportunistic; they are targeted, strategic, and aimed at infrastructure and communications that can be exploited to gather intelligence or to disrupt commercial, private, or military operations. Supply chain risk is a central part of that threat. Utilities sometimes rely on equipment—such as power inverters and telecommunications components—sourced from global vendors such as China.

Investigations elsewhere have found undocumented communication modules embedded in such devices that can bypass network defences. If NSP uses components with these vulnerabilities, the problem is not only mismanagement but a systemic exposure that demands more than an apology. The purpose of targeting utility telecommunications is clear: harvest internal communications, map response procedures, and identify weak points. For NSP, that could mean intercepted messages between management, staff, and contractors—information that would help adversaries plan future intrusions or time disruptive attacks. A successful disruption of the grid would not be an abstract risk; it could cripple industries, maritime commerce, and even affect operations at strategic sites such as CFB Halifax. NSP’s cyber security failures compound the threat. Effective cyber defence requires real time threat detection, active intrusion hunting, behaviour analytics, and a zero trust architecture—measures that detect and limit the damage of targeted campaigns. I am informed these measures are not fully in place at NSP.

Equally troubling is the pace of NSP's response: the breach occurred on March 19, 2025, but NSP only became aware on April 25, 2025 — a full 37 days after the initial intrusion — and some customers did not receive notifications until 63 days after the event. That delay is not a minor lapse; it undercuts the intent of PIPEDA and exposes customers to extended periods of risk without the information they need to protect themselves.

Requesting secrecy from Nova Scotia Energy Board inquiry only deepens the breach of trust. Transparency is not an optional nicety for Nova Scotia Power; it is an essential condition of public utilities' social licence to operate. NSP should take concrete, immediate steps to repair that licence. First, a public, independent forensic report must be completed and released in full to Nova Scotians (redactions only where required for security), so customers know exactly what was taken and how the company will prevent recurrence. Second, NSP should refrain from any request for secrecy and commit to regular, plain language public updates on remediation progress (The last update on NSPs website was 8 July). T

Third, a two year moratorium on any rate increases is a reasonable and necessary measure while trust is being rebuilt. Finally, regulators should require a third party audit of NSP's supply chain and cyber defences. Longer term, this incident should prompt legislative and regulatory changes: mandatory breach notification timelines that match the speed of modern threats (minutes not weeks), stronger requirements for supply chain security, and enforceable standards for operational cyber defences in critical infrastructure. Nova Scotians should not have to wait for another crisis to demand systems designed for the threats we already know exist. As I asked Peter Gregg on July 18: why should I pay my power bill? The answer cannot be a promise to do better later, a closed process, or higher bills to cover the costs of avoidable failure. Paying for essential services is part of a social contract — one that presupposes competence, candour, and accountability. If NSP cannot meet those basic conditions, customers and regulators must insist on remedies that restore both security and trust on terms the public can accept.

Did they contact the utility? No

**How did the utility
respond?**

**How do they want the
complaint resolved?**

The Board inquiry into the cyber security breach must be public in it's entirety.

**Supporting documents
uploaded:**

- image.png

From: [Board, NSUARB](#)
To: [Painting-MacLean, Kimberly](#)
Cc: [Henwood, Crystal D](#)
Subject: FW: The Spring 2025 ctber attack on NS Power & customer contact
Date: September 17, 2025 4:43:48 PM

From: Weldon Young [REDACTED]
Sent: September 17, 2025 2:28 PM
To: Board, NSUARB <Board@novascotia.ca>
Subject: The Spring 2025 ctber attack on NS Power & customer contact

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Dear Sir,

I'm not sure if this concern falls under the preview of your organization, but here it is in a nut shell: NS Power had a widespread cyber attach with access to thier computer systems for a long period of time before they were aware of it. Appearently a great deal of customer personal information became vulnerable. Yet NS Power has not informed customer exactly what personal information NS Power has on each customer. Given all customer information was vulnerable, isn't it incumbent on NS Power to inform each of its cutomers (and possible where possible former customers) exactly what personal information it had retained on each? Particularly as some can still be used after the laps of the security monitoring.

Sincerely,
Weldon Young

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: M12273 FW: NS power
Date: November 28, 2025 1:21:01 PM

From: Jessica Bradstock-Young [REDACTED]
Sent: November 19, 2025 12:41 PM
To: Fisher, Darren - M.P. <darren.fisher@parl.gc.ca>; tony.mancini@halifax.ca; Ombudsman <Ombudsman@novascotia.ca>; Trish@TrishPurdy.ca; trish.purdy@halifax.ca; nspdisputeresolution@gmail.com; Board, NSUARB <Board@novascotia.ca>; Wallace, Lisa <Lisa.Wallace@novascotia.ca>; peter.gregg@nspower.ca; david.pickles@nspower.ca; news@bellmedia.ca; news@haligoniacanada.ca
Subject: NS power

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hey!

I am writing to make a formal complaint and request a full and transparent audit for NS power. How do I go about doing this?

A political party vowing to investigate NS power seems like a conflict of interest.

They not only sold SIN numbers, they lied about the number, and are still sending out notices as of this week. There is zero accountability. Zero transparency. You literally cannot even find an email address for a CEO or director online, nor can you find one on RJSC or any other avenues. The fact that the company hides these individuals that are millionaires and straight up CROOKS is disgusting and unacceptable.

In addition to their privacy breach, they forced NS smart meters on us, knowing that they catch fire and have in NB and NS. Putting NS families in harm's way, due to their houses potentially catching fire. The only way to opt out is to pay an additional fee, creating for financial stress on top of back-to-back rate increases.

If that isn't enough, now they are estimating people's power bills, resulting in under and over estimates, also causing financial pressures for families that cannot afford to feed their children let alone heat their house.

I have never seen a more incompetent business in my entire life. This has gone too far.

I am asking that all parties involved complete an IN DEPTH FINANCIAL AND OPERATIONAL REVIEW AND AUDIT OF THEIR FINANCES, THEIR CEO'S MAKING MILLIONS A YEAR WHILE 25% OF NOVA SCOTIAN'S ARE GOING TO FOOD BANKS. MEANWHILE THE RICH GET RICHER, AND PROTECED BY A UTILITY BOARD THAT KEEPS APPROVING INSANELY UNACCEPTABLE RATE INCREASES.

Signed,

A single mom of two kids on the verge of losing my house.

Jessica

A solid black rectangular box used to redact the signature.

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: M12273 - FW: system security breach unmentioned publicly may be because nova scotia power doesn't realize it yet.
Date: December 22, 2025 11:13:02 AM

From: [REDACTED]
Sent: December 16, 2025 11:26 AM
To: Brown, Rebecca <Rebecca.Brown@novascotia.ca>
Subject: system security breach unmentioned publicly may be because nova scotia power doesn't realize it yet.

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hello, to whom it may concern, I pre-apologize for my grammar. this is an email i'm sending to be brought forward to the top levels of nova scotia power to understand and let people know that your recent cyber attack that you mentioned was a hack to get inside and grab personal information might not have been just that, it seems apparent to me and the lady that day I spoke to on the phone, that not only did they go into your system, but it seems they to this day might still be there. For me this was made a reality when a little while after you announced to the public what had happened with the breach and that you were dealing with it, i'd say about a month or month and a half later, i had to call in, i had to find out what my balance was, because i was paying a deposit when i moved in here 2 years ago, and in order to have that deposit back, i required to make payments on time and in full amounts, which i had done up to that point, and was worried about losing that deposit if i didn't make the payments on time, so regardless that nova scotia power told us not to worry at that time about those payments and that we'd not have to worry about getting power shut off for not paying, I still wanted to not chance that and make a payment. So, i called in to the system and went through the phone system to contact a representative to find out what my amount owing was. Eventually, I found myself talking to a gentleman, who sounded of India decent with the accent, who preceded to ask me WAY more than enough person information questions, to the point i had to question him about why all the questions just to verify my account, and i mean way more information, it almost seemed like there was really no end to the questions, but i had to question him about it to which he said it was fine and asked how he could help me today, i said i simply wanted to know my balance on my account, to which he quickly replied, and i mean quickly, an amount of almost 400, if i remember correctly it was actually 384 or 386 dollars, to which i laughed and replied he must be stoned cuz i'd been living in my same place for like 2 years and paid ever bill and that my biggest bill ever was 160 and on average was only about 100 and i demanded to talk to a supervisor. He said fine and i heard a click and was prompted back out to the very start of the phone system to have to wait and come

through it all over again, to this time speak to a lady, who with talking with for only a matter of a minute, we both realized there was a serious problem, she quickly informed me that she didn't, nor anyone else really, had access to our accounts at that time and could not disclose any kind of a balance on an account, which led me to the realization that the individual was definitely not an employee of nova scotia power at all that quoted me the amount to be paid. I really don't believe for a second that nova scotia power has trained anyone or has anyone working that would have done that at that time, i'm pretty sure all representatives would have informed us that they could not access our accounts at that time because of the security breach that was ongoing at that time, but also I notice there was no mention of the system being breached to the point of calls being intercepted and what i fear, could still be in your system and I feel the public needs to know this is something that has happened and may still be happening. You are more than welcome to reach out to me if you need any follow up questions or if maybe i've not explained things very well.

D.J.(customer)

From: [Painting-MacLean, Kimberly](#)
To: [Painting-MacLean, Kimberly](#)
Subject: FW: NS power estimated billing
Date: December 22, 2025 1:44:18 PM

From: Irene & Stephen Cooper [REDACTED]
Sent: December 21, 2025 4:24 PM
To: Brown, Rebecca <Rebecca.Brown@novascotia.ca>
Subject: NS power estimated billing

You don't often get email from [REDACTED] [Learn why this is important](#)

**** EXTERNAL EMAIL / COURRIEL EXTERNE ****

Exercise caution when opening attachments or clicking on links / Faites preuve de prudence si vous ouvrez une pièce jointe ou cliquez sur un lien

Hello Rebecca,

As per our phone call I am submitting my thoughts on Nova Scotia Power's estimated billing.

I would like the Nova Scotia Energy Board in investigating excessive over estimated power bills to consider what good is finding them guilty after the fact. The power company have already gotten away with it to the detriment of their customers. There has to be significant consequences for doing allowing this to happen in the first place.

My power bill as well as my mother's power bills were estimated for our last billing period. In comparison to the billing period for the same time frame in 2024, my 2025 usage charged was double the 2024 usage, my mother's was one and a half times her 2024 usage.

The media coverage of statements from NS power CEO, referred to some overly complicated way of estimating usage, including differences in season. He knows full well that customers are comparing their usage from 2024 to usage being charged in 2025 for the same two month period. NS power should not be allowed to charge for more kilowatt hours usage as an estimate for billing than the usage was the year before. They have this information, since it is right on our bills for easy comparison. My bill shows Nov 2024 usage and every 2 months after that to Nov 2025.

The over estimation of usage allows Nova Scotia Power to collect more revenue for a service it has not provided. Yes, eventually when Nova Scotia Power gets around to actually providing a meter reading the customer will get caught up.

In media coverage the Nova Scotia Power CEO stated we will fix it, by March, probably an estimate and we all know how well they estimate. However, in the mean time, a lot of

customers will pay the overly inflated bills since it is easier to just take the bill in and pay it. Nova Scotia Power will have the money in their bank accounts making their accounts look better.

An even larger issue is for anyone heating their homes this winter with electric heat. My mother's usage in January 2025 and March 2025 was over 4000 kilowatt hours each. If the same thing happens as she did on November 2025's bill, then she will be billed for at least 10,000 kilowatt hours for January 2026 and again for March 2026. If she pays those inflated bills, how many bills afterwards will it take before Nova Scotia Power usage actually catches up since spring, summer and fall usage is significantly less.

In the statements made by Nova Scotia Power CEO, covered by the media I have not been impressed. The information sessions also covered by media seems to be nothing more than their way of explaining what is happening and why, but not changing anything for the customer. Yes, you can pay what you think as a customer you owe and they say they are not charging penalties. Media also reported on a customer having her bill go to a collection company after doing what a Nova Scotia power representative told her to do.

Nova Scotia Power should not be allowed to get away with this. There should be severe consequences to the company and compensation paid to the customers. It is not OK to ask customers to wait until March for the power company to "Fix It".



Appeal - NS Power Dispute Resolution Officer (DRO)

Reference Number: 251115002

Submitted on: Saturday, November 15 2025 at 11:33:51 AM (AST)

Contact Information

Name on account:	Shelly LeBlanc	
Account number:	*****	
Business contact:		
Account address:	Address 1:	*****
	Address 2:	*****
	City:	*****
	Province:	*****
	Postal code:	*****
	Country:	*****
Email Address:	*****	
Mailing address:	Address 1:	*****
	Address 2:	*****
	City:	*****
	Province:	*****
	Postal code:	*****
	Country:	*****
Telephone number:	*****	
Alternate phone number:	*****	

Complaint Information

DRO made decision on:	May
Type of complaint:	Other
Additional details:	I am writing to have it on record that the data breach has literally RUINED us and the billing is out of control for us who live in NS. During all of this while our credit was being ruined because of NS Power my husband was going through very rare kidney cancer. So on top of trying to catch up after fraud on our bank account which cause so much extra stress and anxiety, we had to beg and borrow money just to be able to get to Halifax from Cape Breton. Not to mention having to sleep in our vehicle because we could not afford a hotel room while he was in hospital. It's disgusting that nothing has been done except to give us credit monitoring so that every time someone tries to use our info we get information which just heightens the anxiety.
How do they want the complaint resolved?	Our hope is it will be resolved in the courts.
Supporting documents uploaded:	● f8818369-ced5-4b2c-9535-8a71bea1677d.pdf

To: Clerk of the Board, Nova Scotia Energy Board

Re: Matter M12600 — Inquiry into the impact of the cyber incident on Nova Scotia Power Incorporated's collection and retention of customer information

I am a Nova Scotia Power ratepayer and I am filing this Letter of Comment in Matter M12600. I ask the Board to put a specific set of questions to Nova Scotia Power Incorporated as Information Requests, because the public record in this proceeding does not currently establish where customer personal information is stored, which vendors and subprocessors hold it, in what jurisdiction, or what exposure that creates to foreign legal process.

Why this is within the inquiry's scope and the Board's mandate. This inquiry concerns NS Power's collection and retention of customer information. Where that information physically resides, and who can compel access to it, is a core retention question — not a peripheral one. It is also a ratepayer-prudence question: the customer analytics, Meter Data Management System, and Customer Information System platforms that handle this data are funded through the revenue requirement and recovered from ratepayers. The 2025 breach has already imposed costs on ratepayers (multi-year credit monitoring, system rebuild, and related expenses). Whether customer data is held on vendor infrastructure outside Canada, or on Canadian infrastructure operated by a foreign-owned vendor subject to foreign disclosure law, bears directly on whether NS Power's data-handling arrangements reflect prudent utility practice. The public record should answer it.

What I ask the Board to require. I respectfully request that the Board direct NS Power to answer the following as Information Requests, and that the jurisdiction-level answers (which country; whether subject to foreign legal process) be placed on the public record even where granular technical specifics are filed confidentially. A confidentiality claim over implementation detail should not be permitted to withhold the basic fact of where Nova Scotians' data lives.

Question 1 — Vendor and processor inventory Provide a complete inventory of every third party (vendor, service provider, processor, and subprocessor) that stores, processes, transmits, or has access to Nova Scotia Power customer personal information. For each, state: (a) legal name; (b) jurisdiction of incorporation and head office; (c) the function performed; and (d) the categories of customer personal information each receives (e.g., name, address, interval/meter data, billing history, banking information, SIN, driver's licence).

Question 2 — Storage and processing location, by entity For each entity identified in Question 1, identify the physical location(s) — by country, and by cloud region code where applicable (e.g., AWS `ca-central-1`, `us-east-1`) — at which NS Power customer personal information is (a) stored at rest, (b) processed, and (c) backed up or replicated. Where a single entity uses multiple regions, identify each and the data category held in each.

Question 3 — Bidgely Inc., specifically With respect to Bidgely Inc. and any of its products in use or under contract by NS Power (including UtilityAI, Analytics Workbench, MyEnergy Insights integration, the IQ Detection and Prioritization Agent, and the Edge Intelligence Platform): (a) Confirm whether customer data supplied to Bidgely (including interval/meter, billing, and account data) is hosted in an AWS Canada region (**ca-central-1** / **ca-west-1**) or in any United States or other non-Canadian region. (b) Produce the contractual provision governing data-residency, or confirm in writing that the contract contains no data-residency restriction. (c) State whether any Bidgely-derived data (e.g., disaggregation outputs, household-level insights) is stored or processed outside Canada, even where the source data is not.

Question 4 — Subprocessors and onward transfer For each primary vendor identified in Question 1, identify every subprocessor (including cloud infrastructure providers, support contractors, and offshore operations) that may store, process, or access NS Power customer personal information, and the jurisdiction of each. State whether NS Power maintains a current subprocessor list and produce it.

Question 5 — Transfer safeguards and key custody For each cross-border transfer or storage of customer personal information identified in Questions 2 through 4, identify: (a) the contractual and technical safeguards in place (encryption at rest and in transit); (b) who holds the encryption keys and in what jurisdiction; (c) any contractual restriction on onward transfer or vendor use of the data. Produce the governing data-processing agreement or transfer terms.

Question 6 — Foreign legal process exposure State whether any customer personal information held in a third-party or vendor-hosted environment is subject to foreign legal process, including but not limited to the U.S. CLOUD Act, FISA Section 702, or National Security Letters — including where data is physically stored in Canada but the vendor or its cloud provider is U.S.-owned. Identify what assessment NS Power has performed of this exposure and produce any legal opinion or assessment addressing foreign-government access to customer data.

Question 7 — Privacy Impact Assessment State whether NS Power has completed a Privacy Impact Assessment (or equivalent) addressing the cross-border transfer and storage of customer personal information. If yes, produce it (redacted as required). If no, explain why none was conducted.

Question 8 — Vendor environments within breach scope With respect to the 2025 cyber incident: (a) state whether any vendor-hosted or third-party-processed environment containing customer personal information was within the scope of the incident; (b) state whether each such environment was assessed for compromise as part of the incident response; (c) produce the scoping determination or the portion of the forensic assessment addressing third-party environments.

Question 9 — Capital-project systems Identify which systems associated with AMI Matter M08349, capital matter M11003 / CI 47124, the Meter Data Management System replacement, and the Customer Information System replacement store or process customer personal

information. For each, provide the storage and processing location per Question 2 and the vendor per Question 1.

Question 10 — Customer-facing disclosure State whether NS Power discloses to customers the jurisdiction(s) in which their personal information is stored or processed, and identify where that disclosure appears (privacy policy clause, terms of service, notification). Produce the disclosure. If NS Power does not disclose this, state so.

Question 11 — Affordability / eligibility analytics State whether any premises-level affordability, arrears-risk, or energy-burden eligibility analytics (including Bidgely's Income-Qualified and Affordability program or the IQ Detection and Prioritization Agent) are processed by a vendor, and identify the storage and processing location of the underlying customer data and the analytic outputs.

I recognize the Board may receive a confidentiality request over some of this material. I ask only that the basic jurisdictional facts — the country in which customer data is stored and processed, and whether it is exposed to foreign legal process — be answered on the public record, and that any confidentiality claim be limited to genuine security implementation detail rather than extended to the underlying facts.

Thank you for considering this comment.

Graham Charles

