Nova Scotia POWER
An Emera Company

102 W Service Rd
384 Champlain NY
12919

June 06, 2025

00766-ADFSON L001 AUTO *000003

MT2563501
000003

[redacted]

NOTICE OF DATA BREACH

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

What Happened?

On May 8, 2025, Nova Scotia Power determined that an unauthorized third party acquired customer information that may have included some of your personal information.

What Information Was Involved?

The types of impacted 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, customer account history (such as power consumption, service requests, customer payment, billing and credit history, and customer correspondence), driver's license number, and Canadian 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.

What We Are Doing.

Immediately following detection of the incident, 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. We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future.

Additionally, we have made arrangements with Cyberscout®, a TransUnion® brand to provide you with a two-year subscription to a United States comprehensive credit monitoring service at no cost to you to help protect your identity. Please refer to Attachment A included with this notice for additional information about Cyberscout®, including details about how to activate your subscription.

What You Can Do.

We encourage you to remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts or phone calls), including messages that appear to be from Nova Scotia Power, asking you to provide your personal information. Please avoid clicking on suspicious web links or downloading attachments without confirming they are from a legitimate source. Regardless of whether you elect to enroll in the credit monitoring service, we strongly recommend that you remain vigilant for incidents of fraud and identity theft, including by regularly reviewing and monitoring your credit history and credit reports to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity.

Please refer to Attachment B for more information about steps you can take to protect yourself against potential fraud and identity theft.

00766-ADFSON-189107-L001 AUTO_000003-000013-000-1/3

For More Information.

Protecting the privacy and security of information held by Nova Scotia Power is something we take very seriously. Please be assured that we are taking steps to address the incident and to protect the security of your data. We have established a dedicated number 1-844-818-0376 for customers who have questions about this incident, and you can also contact us at PO Box 910, Halifax, Nova Scotia, B3J 2WE.

Sincerely,

Peter Gregg

President & CEO

Nova Scotia Power

ATTACHMENT A

[redacted]

We have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a **24-month** subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

https://bfs.cyberscout.com/activate

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 enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud.
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-432-7463.

00766-ADFSON-189107-L001 AUTO_000003-000015-000-2/3

MT25635001

ATTACHMENT B

Additional Information

To protect against possible fraud, identity theft, or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the U.S. Federal Trade Commission ("FTC").

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit **www.annualcreditreport.com** or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:
Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the FTC for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General, or the FTC.

Maryland Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or **http://www.oag.state.md.us**.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: The Attorney General can be contacted at 1-800-771-7755 or **https://ag.ny.gov/**. The Department of State Division of Consumer Protection can be contacted at 1-800-697-1220 or **https://dos.ny.gov/**.

North Carolina Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or **http://www.ncdoj.gov**.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or **http://www.riag.ri.gov/**. You may also file or obtain a police report by contacting local or state law enforcement agencies.

00766-ADFSON-189107-L001 AUTO_000003-000017-000-3/3

MT25635001

Nova Scotia POWER
An Emera Company

102 W Service Rd
384 Champlain NY
12919

June 06, 2025

00766-ADFSON L001 AUTO *000004

MT2563501
000004

[redacted]

NOTICE OF DATA BREACH

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

What Happened?

On May 8, 2025, Nova Scotia Power determined that an unauthorized third party acquired customer information that may have included some of your personal information.

What Information Was Involved?

The types of impacted 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, 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.

What We Are Doing.

Immediately following detection of the incident, 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. We are working hard to continue strengthening the security of our systems by implementing additional safeguards to help prevent similar incidents in the future.

Additionally, we have made arrangements with Cyberscout®, a TransUnion® brand, to provide you with a two-year subscription to a comprehensive United States credit monitoring service at no cost to you to help protect your identity. Please refer to Attachment A included with this notice for additional information about Cyberscout®, including details about how to activate your subscription.

What You Can Do.

We encourage you to remain vigilant and cautious about any unsolicited communications (such as emails, text messages, social posts or phone calls), including messages that appear to be from Nova Scotia Power, asking you to provide your personal information. Please avoid clicking on suspicious web links or downloading attachments without confirming they are from a legitimate source. Regardless of whether you elect to enroll in the credit monitoring service, we strongly recommend that you remain vigilant for incidents of fraud and identity theft, including by regularly reviewing and monitoring your credit history and credit reports to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity.

Please refer to Attachment B for more information about steps you can take to protect yourself against potential fraud and identity theft.

00766-ADFSON-189107-L001 AUTO_000004-000019-000-1/3

For More Information.

Protecting the privacy and security of information held by Nova Scotia Power is something we take very seriously. Please be assured that we are taking steps to address the incident and to protect the security of your data. We have established a dedicated number 1-844-818-0376 for customers who have questions about this incident, and you can also contact us at PO Box 910, Halifax, Nova Scotia, B3J 2WE.

Sincerely,

Peter Gregg

President & CEO

Nova Scotia Power

ATTACHMENT A

[redacted]

We have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a **24-month** subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

https://bfs.cyberscout.com/activate

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 enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud.
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-432-7463.

00766-ADFSON-189107-L001 AUTO_000004-000021-000-2/3

MT25635001

ATTACHMENT B

Additional Information

To protect against possible fraud, identity theft, or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the U.S. Federal Trade Commission ("FTC").

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit **www.annualcreditreport.com** or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:
Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the FTC for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General, or the FTC.

Maryland Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or **http://www.oag.state.md.us**.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: The Attorney General can be contacted at 1-800-771-7755 or **https://ag.ny.gov/**. The Department of State Division of Consumer Protection can be contacted at 1-800-697-1220 or **https://dos.ny.gov/**.

North Carolina Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or **http://www.ncdoj.gov**.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or **http://www.riag.ri.gov/**. You may also file or obtain a police report by contacting local or state law enforcement agencies.

00766-ADFSON-189107-L001 AUTO_000004-000023-000-3/3

MT25635001