



<<TransUnion Return Address>>

<< First Name>> << Last Name>>

<<Address1>>, <<Address2>>

<<City>>, <<State>> <<Zip>>

<<DATE>>

Re: Notice of Data Security Incident

Dear << First Name>> << Last Name>>:

We are writing to you as one of our valued guests regarding a recent data security incident experienced by WestJet, an Alberta Partnership ("WestJet"). Although our investigation is ongoing, we reviewed the data that was potentially involved and determined that your personal information may have been affected. We then worked to notify you about the incident as soon as possible.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this 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.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report without written authorization. However, 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.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies:

Equifax Security Freeze: P.O. Box 105788, Atlanta, GA 30348, 1-800-685-1111, www.equifax.com

Experian Security Freeze: P.O. Box 9701, Allen, TX 75013, 1-888-397-3742, www.experian.com/freeze/center.html

TransUnion Security Freeze: P.O. Box 2000, Chester, PA, 19016, 1-888-909-8872, freeze.transunion.com

In order to request a security freeze, you will need to provide the following information:

1. Full name and any suffixes;
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The consumer reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a request to the consumer reporting agencies and include proper identification (name, address, and Social Security Number) and the PIN or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The consumer reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a request to each of the three consumer reporting agencies and include proper identification (name, address, and Social Security Number) and the PIN or password provided to you when you placed the security freeze. The consumer reporting agencies have three (3) business days after receiving your request to remove the security freeze. No fee is required to be paid to any of the consumer reporting agencies to place, lift or remove a security freeze.

In order to determine whether any unauthorized credit was obtained with your information, you may obtain a copy of your credit report at www.annualcreditreport.com or 1-877-322-8228. You may also request information on how to place a fraud alert by contacting any of the above consumer reporting agencies. A fraud alert is intended to alert you if someone attempts to obtain credit in your name without your consent. It is recommended that you remain vigilant for any incidents of fraud or identity theft by reviewing credit card account statements and your credit report for unauthorized activity. You may also contact the Federal Trade Commission (FTC) to learn more about how to prevent identity theft:

FTC, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

As an additional measure, and to provide further peace of mind, WestJet is offering an identity theft and monitoring solution free of charge for 24 months. These services provide you with alerts for any changes to your information for 24 months from the date of enrollment. These services also provide you with proactive fraud assistance resources to help with any questions that you might have. In the unlikely event that you become a victim of fraud; a personal restoration specialist will help to resolve any identity theft. This service includes up to \$1,000,000 of expense reimbursement insurance. Please find enclosed your personal activation code and detailed instructions on how to enroll in these services. Once set up, this monitoring service will allow you to identify any potentially fraudulent activity.

If you are a WestJet Rewards Member, information linked to your membership may have also been affected. This could include your WestJet Rewards ID number and points balance on the date of the incident, as well as other information linked to the use of your account. Importantly, your password to access Rewards accounts was not affected. WestJet has no reason to believe that your points may be at risk.

If you are a WestJet RBC Mastercard, WestJet RBC World Elite Mastercard, or WestJet RBC World Elite Mastercard for Business cardholder, additional information linked to your WestJet Rewards account may have also been involved. This may include a credit card identifier type (e.g. "World Elite"), and information about changes to your WestJet points balance. Your credit card number, expiration date and CVV are not affected.

To the extent that any of your travel information is linked to other individuals (such as family members or others travelling under the same booking number) you may wish to make them aware of the incident. If they have questions or concerns, they can contact us using contact information provided below.

If you receive any suspicious emails, text messages or calls from someone purporting to be from WestJet please visit our [Scams and fraudulent schemes page](#) on our website or contact local authorities.

As a general recommendation, and not in connection with this incident, we would encourage you to follow best practice from a security perspective, including the below steps:

- Check your flight information ahead of any upcoming trips
- Continue to be alert to the risk of phishing and fraudulent emails asking you to enter login credentials, provide financial information or give up any other personal data.
- Check your bank statement regularly for any unusual activity that you do not recognize.
- Check your credit file regularly for newly opened accounts or credit searches that you do not recognize.
- Use strong passwords and change them regularly. Use passwords that are at least eight characters long and use numbers, upper case, lower case and symbols.
- Never give out personal details over the phone unless you are sure who you are speaking to.

Please note we would never contact you by email to ask you to provide us with any payment card information

If you have questions or need assistance, please call **1 833-294-7065**. Representatives are available Monday through Friday from 8:00 am – 8:00 pm Eastern Time.

We take this event and the security of information in our care seriously. We regret any concern or inconvenience this incident may cause you.

Sincerely,

WestJet, an Alberta Partnership

<<WestJet Address>>

Services Description

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:

XXXX-XXXX-XXXX-XXXX

Please ensure that you redeem your activation code before November 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, Monday to Friday, between 8:00 a.m. and 8:00 p.m. Eastern Standard Time.

W{Unique ID #}