

Reena Bajowala
Tel 312.456.1018
Reena.Bajowala@gtlaw.com

September 29, 2025

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
via email at consumer@ag.iowa.gov

Re: Notification of Data Security Incident

To Whom It May Concern:

We represent WestJet, an Alberta Partnership (“WestJet”), located at 22 Aerial Place NE, Calgary, AB T2E 3J1, Canada, and are writing to notify your office of an incident that may affect the security of some personal information of 367 Iowa residents. Although the threshold number of affected Iowa residents was not met, WestJet elected to notify your office out of an abundance of caution, given that the state of residence for certain individuals could not be confirmed. While WestJet is notifying you of this incident, WestJet does not waive any rights or defenses relating to the incident, this notice, or the applicability of Iowa law on personal jurisdiction.

On June 13, 2025, WestJet identified suspicious activity within its systems. WestJet immediately investigated and determined that these were the actions of a sophisticated criminal third party who gained unauthorized access to WestJet’s systems. With the assistance of internal and external experts, WestJet took immediate steps to secure its environment and started a technical and forensic investigation to identify the nature and scope of the event. This included identifying any data that may have been affected. The investigations to date have established that the unauthorized third party obtained certain data from WestJet’s network. Since making that determination, WestJet diligently conducted an extensive analysis of that data to identify specific data elements and locate current contact information for certain United States residents who were impacted. As of September 15, 2025, WestJet completed its analysis and as a result is providing this notice.

WestJet takes the security of all information in its systems very seriously, and it has already taken steps to prevent a recurrence. Among other actions, the company has increased monitoring, further improved security controls, and reinforced its systems. On or about September 29, 2025, WestJet will begin sending notifications and provide substitute notice to all potentially affected individuals. An example of the letter notification is attached.

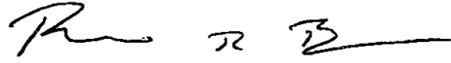
Office of the Attorney General

September 29, 2025

Page 2

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me for any additional information.

Best Regards,

A handwritten signature in black ink, appearing to read 'Reena Bajowala', with a long horizontal flourish extending to the right.

Reena Bajowala

Shareholder



<<TransUnion Return Address>>

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

<<Address1>>, <<Address2>>

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

<<DATE>>

Re: Notice of Data Breach /Data Security Incident

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

As you may be aware, WestJet, an Alberta Partnership (“WestJet”) recently experienced a cybersecurity incident. We are writing to update you on our investigation, which involved some of our systems which hold your personal information. This incident is now resolved.

Please read this notice carefully as it provides up-to-date information on what happened, how your personal information may be involved, the steps we have taken, and some steps you can take, including how to obtain free monitoring and identity theft protection services.

Importantly, credit card or debit card numbers, expiry dates and CVV numbers, and guest user passwords, were not compromised, and our systems are fully secure. At no time was the safety and integrity of our operations ever in question.

What Happened?

On June 13, 2025, we identified suspicious activity on our WestJet systems. We immediately investigated and determined that these were the actions of a sophisticated criminal third party, who gained unauthorized access to our systems. With the assistance of internal and external experts, we took immediate steps to secure our environment and started a technical and forensic investigation to identify the nature and scope of the event. This included identifying any data that may have been affected. The investigations to date have established that the unauthorized third party obtained certain data from our network. Since making that determination, we diligently conducted an extensive analysis of that data to identify specific data elements and locate current contact information for certain United States residents who were impacted. As of September 15, 2025, we completed our analysis and as a result are providing this notice.

What Information Was Involved?

The types of personal information involved by this incident vary by individual but may include your name, date of birth, mailing address, information about the travel document you used when travelling with WestJet (such as your passport or other government issued identification document or number) and other information associated with your travel needs such as accommodations requested or complaints filed. No credit card or debit card numbers, expiry dates or CVV numbers or account passwords were involved.

If you are a WestJet Rewards Member, information linked to your membership may have also been involved. 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 involved. 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 involved.

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 the contact information provided below.

We continue to work alongside our technical experts to determine the full extent of the incident. While investigations of this nature are complicated and take time to complete, we have worked as quickly as possible to review the data we understand to be involved and to ascertain whether any of your personal information has been involved.

What Are We Doing?

We are treating this incident with the utmost urgency and attention. We take the security of information in our care very seriously. As soon as we discovered this incident, we took the steps described above and examined our system to minimize the risk of a similar incident occurring in the future. We have reported the incident to law enforcement, including the Federal Bureau of Investigation, and are cooperating in their investigation.

What You Can Do.

You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through TransUnion by using the unique code provided below.

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.

You can follow the recommendations on the following page to help protect your personal information.

For More Information.

Should you have any questions regarding this notice or if you would like more information, please do not hesitate to call, Monday to Friday, between 8:00 a.m. and 8:00 p.m. Eastern Standard Time:

1 833-294-7065

The security of personal data is a critical priority at WestJet. We have been doing, and will continue to do, everything we can to ensure the ongoing resilience of our systems and to prevent this type of incident from occurring again.

Sincerely,

WestJet, an Alberta Partnership
22 Aerial Place NE
Calgary, AB T2E
Canada
1-888-937-8538

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”). Out of an abundance of caution, if you would like to take additional measures to protect against identity theft, the FTC provides general advice here: <https://consumer.ftc.gov/features/identity-theft>.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

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.

Services Description

We have arranged a 24-month subscription to myTrueIdentity®, which specializes in online credit monitoring and remediation services, at no cost to you.

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

www.mytrueidentity.com

When prompted please provide the following unique code to receive services:

<CODE HERE>

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

Enrollment requires an internet connection and e-mail account and is not available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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

- ✓ Unlimited online access to your TransUnion 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 TransUnion VantageScore 3.0 Credit Score, updated daily. A credit score is a three-digit number calculated based on the information contained in your TransUnion credit report at a particular point in time.
- ✓ Credit monitoring, which provides you with email notifications to key changes on your TransUnion 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 information and helps protect you against identity theft.

Should you require technical support with myTrueIdentity®, please contact TransUnion, at 1-844-787-4607, Monday to Friday, between 8:00 a.m. and 8:00 p.m. Eastern Standard Time.

C{Unique ID #}

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