[redacted]

[redacted]

00695-ADFFIN L001 AUTO *000001

[redacted]

Waratah Capital Advisors Ltd.

Dear [redacted]

Re: Notice of Cybersecurity Incident

Waratah Capital Advisors Ltd. ("Waratah") takes the privacy and security of personal information seriously. As such, we are writing to inform you of a cybersecurity incident that we recently experienced which may have involved some of your personal information. You are receiving this letter because you hold or have held investment funds managed by Waratah, in your portfolio directly or with your investment dealer. This letter is to inform you of this incident, the steps we are taking in response, and the steps that you may consider to help protect your information.

What Happened?

On June 24, 2025, we discovered that an unauthorized third-party had accessed certain Waratah information. Upon investigation, we determined that the unauthorized access involved our back-up systems managed by our third-party IT provider and was not a result of a direct intrusion on our internal network. Following the discovery of the incident, we took steps to secure our back-up systems. We also engaged legal counsel and a third-party cybersecurity expert to further investigate, protect our systems and mitigate the impact on our clients. We have reported the incident to law enforcement and will be reporting to the relevant regulatory authorities. Waratah then conducted a robust review of the files to identify individuals whose personal information may have been contained in the files.

What Information Was Involved?

On August 14, 2025, we completed our review and concluded that certain information in regard to your Waratah holdings may have been affected in the incident, including your name, date of birth, driver's license, passport number, banking information, and Social Security Number.

To date, we are not aware of any evidence that this information has been misused or further disclosed in connection with the incident. The incident has been contained, and security protocols have been reinforced.

What We Are Doing.

In addition to our existing security safeguards, such as penetration testing, employee training, and advanced firewalls, we are working closely with our third-party IT service provider and consultants retained as part of this investigation, to further strengthen our existing security safeguards and help prevent a similar incident from happening again.

As a precaution, we are offering you a complimentary 24-month credit monitoring membership through Equifax. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. Equifax is completely free to you and enrolling in this program will not hurt your credit score.

[redacted]

What You Can Do.

We encourage you to review the additional information on Equifax, including instructions on how to activate your complimentary 24-month credit monitoring membership, as well as information on additional steps you can take in response to this incident, on the pages that follow this letter.

For More Information.

Waratah takes the personal information seriously. If you have questions, please contact [redacted], Monday through Friday between 9am to 9pm EST, excluding major holidays. While we understand that news of this nature may be concerning, we want to assure you that we are taking all necessary steps to address the situation responsibly. Thank you for your understanding.

Sincerely,

Waratah Capital Advisors Ltd.

CREDIT MONITORING ACTIVATION INSTRUCTIONS

EQUIFAX®

Activation Code: [redacted]
Enrollment : [redacted]

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.
5. **You're done!**
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features

[1] *The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.*

[2] *Credit monitoring from Experian and TransUnion will take several days to begin.*

[3] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[4] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[5] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[6] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

00695-ADFFIN-196389-L001 AUTO_000001-000003-000-2/4

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-833-799-5355 P.O. Box 2000 Chester, PA 19016 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699- 9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274- 4400.

For Texas Residents: You may contact and obtain information from your state attorney general at: Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identity-theft or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island Residents: You have the right to file or obtain a police report regarding this incident. No Rhode Island residents were impacted by this incident.

00695-ADFFIN-196389-L001 AUTO_000001-000005-000-3/4

FAQ – INCIDENT BACKGROUND AND RESPONSE

1. What happened?

On June 24, 2025, we discovered that an unauthorized third-party had accessed certain Waratah information. Upon investigation, we determined that the breach involved our back-up systems managed by our third-party IT service provider and was not a result of direct intrusion on our internal network. Following the discovery of the incident, we promptly secured our network and engaged third party cybersecurity experts to further investigate, mitigate and protect our environment. The firm's operations and service provider connectivity were not impacted. We have reported the incident to law enforcement and will be reporting to the relevant regulatory authorities.

The incident has been contained and there is no evidence of persistent threats and further unauthorized activity or misuse.

2. Why am I receiving this notification?

You are receiving this letter because you are or have invested in Waratah-managed funds, either directly or through your investment advisor. As result, your personal information may have been stored within Waratah's systems at the time of the incident.

Your letter details information that was stored in our back-up systems at the time of the incident and that may have been impacted. The review of the impacted records is complete, and we do not anticipate any additional findings pertaining to your information. To date, we are not aware of any evidence that this information has been misused or further disclosed.

Should we learn that additional information was impacted, we will inform those impacted accordingly.

3. I am no longer invested in the Waratah Funds, is my information still stored?

We are required to retain records for prescribed periods of time, even after an investor ceases to be a client. These retention periods vary depending on the applicable jurisdiction and the requirements of the relevant regulatory or legal authorities.

4. Timing of notification

As soon as the incident was identified, we launched an investigation, with the assistance of cybersecurity experts, to determine the scope of the incident. This involved a thorough review and validation of all systems and data. The investigation remains ongoing.

As soon as it was determined that personal information may be involved, we worked to identify the type of information impacted and those that were impacted. This process took some time to complete, and notification was provided as soon as possible under these circumstances.

5. Does this mean I am a victim of identity theft?

No. The fact that your information may have been impacted does not mean you are a victim of identity theft or that the information has been accessed to commit fraud. To protect yourself, remain vigilant by periodically reviewing your credit reports and financial statements, remaining alert to unusual charges or activity, and following the recommended steps in the letter provided to you.

6. How were you alerted to this incident?

We were alerted to this incident when our third-party IT service provider discovered the unusual activity. An internal investigation was launched, and the activity was quickly determined to be unauthorized. We immediately deployed countermeasures to prevent further unauthorized access.

7. Do you know the root cause of the incident?

While our investigation into the cause and scope of the incident is ongoing, currently we can provide the following updates:

- The incident involved an unknown actor
- The incident did not impact our internal systems/network or servers.
- Internal Waratah credentials were not compromised.
- The information was accessed and copied through our backup systems without authorization during the incident.

8. Why didn't your IT security stop the intrusion?

Unfortunately, due to rapidly evolving nature of cyber threats, it is not always possible to prevent against all forms of attack.

In addition to our existing safeguards, such as penetration testing, employee training and advanced firewalls, we are working closely with our service providers to further strengthen our safeguards, including the protections around our back-up systems.

We are also working with third party cybersecurity experts, and we have secured our IT environment and back-up processes.

9. When will the forensic investigation be completed?

Our forensic investigation into the incident is ongoing. We anticipate it will take some time to complete, potentially several weeks, as the investigation involves a thorough review and validation process, focused on a full assessment of the overall security of our back-up systems and a broad evaluation of other opportunities to improve our cyber defenses.

10. Support for potentially impacted individuals

As a precaution, individuals potentially impacted by the incident are being offered complimentary credit monitoring service with Equifax for a period of 24 months. See page 3 of this package for further details.

Equifax provides credit monitoring and fraud prevention services directly to consumers. The service does require your permission to be enrolled and will ask you a series of questions to verify your identity. Waratah is not permitted to enroll you on your behalf.

11. Contact for additional information

We understand concerns arising from this situation. If you have any questions or would like to discuss the situation further, please contact 877-250-2783, Monday through Friday between 9am to 9pm EST, excluding major holidays.

00695-ADFFIN-196389-L001 AUTO_000001-000007-000-4/4