doxim [redacted]

Test

[redacted]

00695-ADFFIN G0539 L001 AUTO *000007

MT251M5051 000007

[redacted]

Dear [redacted]

Doxim Solutions ULC ("Doxim" or "we") experienced a security incident in August 2024 that resulted in unauthorized access to certain computer systems supporting our Canadian operations. We have been investigating this incident with the help of external cybersecurity experts, and our investigation revealed that a number of personnel files may have been downloaded during the incident. After a thorough review of the files contained on these systems, we have identified files containing your personal information.

We want to reassure you that we have no evidence at this time that any personal information has been misused as a result of this incident, nor do we have any reason to think this is likely to occur. That being said, we did want to send this letter to you out of an abundance of caution in order to:

- Communicate what happened.
- Identify the personal information involved.
- Provide details on how to enroll in 24 months of credit and identity monitoring services we are offering to you at no charge.

What Happened? On August 20, 2024, Doxim experienced a security incident affecting the portion of its computer network supporting its Canadian operations. Upon detecting the incident with our security tools, we promptly took our entire Canadian network offline, notified law enforcement, and engaged industry-leading cybersecurity experts to investigate. As part of our investigation, we determined that files had been taken from our network. Over the past few months, our experts have been conducting an in-depth review of the files to determine what information may have been impacted. We notified you as soon as possible once we learned your information was contained within these files.

What Are We Doing? We are working with cybersecurity experts to fortify our cybersecurity defenses, and to monitor the "dark web" for information that affects us. These efforts are all ongoing. We have no evidence that any files, including those containing your personal information, have been published to date or that any information has been misused.

What Information Was Involved? Information you or a family member may have provided to Human Resources for tax or benefits purposes, including [redacted]

[redacted]

[redacted]

[redacted]

MT251M5051

What You Can Do? We have enclosed an Identity Protection Reference Guide to make you aware of ways to monitor and protect your personal information. You will also find information on how to enroll in credit monitoring and identity protection services we are offering you, free of charge, if you are interested in these services.

For More Information. If you have any questions about this incident, or to activate your credit monitoring offer, please review the materials below or reach out to our dedicated support team at [redacted], Monday through Friday 9:00 am – 9:00 pm EST, (excluding major holidays).

Sincerely,

Mike Hennessy
CEO

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze. There is no cost to place a security freeze.

00695-ADFFIN-G0539-L001 AUTO_000007-000039-000-2/3

MT2S1M5851

4. Request an IP PIN from the IRS. Although the IRS is capable of identifying suspicious tax returns, taxpayers may choose to take proactive steps to prevent fraud, including obtaining an Identity Protection PIN (IP PIN) from the IRS. The IP PIN is a 6-digit number that, when active, will be required to file a tax return using the taxpayer's SSN or ITIN. To request an IP PIN, visit https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

In addition, taxpayers may opt in to ID.me, an identity verification service that requires a photo ID or live video session before logging in to submit a tax return online.

Finally, taxpayers may submit IRS Form 14039, Identity Theft Affidavit online if they received IRS correspondence indicating they might be a victim of tax-related identity theft or if their e-file tax return was rejected as a duplicate. After submitting the form, the IRS will refer the taxpayer's case to the Identity Theft Victim Assistance organization to investigate the case, remove fraudulent returns, and process the correct return and refund.

5. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

6. You can also further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov; 1-877-ID-THEFT (877-438- 4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-866-366-8343 or (410) 576-6491, https://www.marylandattorneygeneral.gov

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/

EQUIFAX®

Enter your Activation Code: [redacted]
Enrollment Deadline: [redacted]

Equifax Credit Watch™ Gold

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

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] 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[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- 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[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of [redacted] then click "Submit"

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.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]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. [2]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. [3]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 [4]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-G0539-L001 ADTO_000007-000041-000-3/3

MT2S1M5851