



Blainville, August 31, 2026

NOTICE TO EMPLOYEES – CONFIDENTIALITY INCIDENT

Dear Colleagues,

We are writing to inform you of a confidentiality incident involving certain personal information of Neopharm Labs' current and former employees. This notice is provided in accordance with the *Act respecting the protection of personal information in the private sector* (Law 25).

Description of the Incident

On July 15, 2026, Neopharm detected unauthorized activity affecting certain parts of its IT infrastructure, subsequently confirmed to be a ransomware attack where data was exfiltrated and published online by an unauthorized threat actor.

As a result of systems being brought back online following this incident, certain human resources files were accessible internally without the usual access restrictions during the period from August 1 to August 10, 2026, on which date access was immediately restricted.

While we are unable to confirm whether any of these files were accessed, we are providing you with this notice to enable you to take the necessary precautions.

Personal Information That May Be Involved

The categories of employee personal information that may have been affected include:

- personal contact information (name, address, telephone number, email);
- employment information (position, hire dates, status);
- compensation and payroll information (including T4 slips);
- banking and direct deposit information;
- social insurance numbers and other government identifiers;
- benefits information;
- medical or leave-related information;
- disciplinary or performance-related information; and
- copies of or information from identity documents.

Please note that not all of these categories necessarily apply to each employee. A detailed data mining analysis is underway to determine precisely which information related to each individual was published online without authorization. We will provide a supplemental notice if the data

mining confirms that personal information beyond the categories listed above was published online.

Measures Taken by Neopharm

Upon detecting the incident, Neopharm took the following measures:

- immediate isolation of affected systems to contain the incident;
- engagement of specialized cybersecurity firms to conduct the investigation and system restoration;
- reset of compromised credentials;
- implementation of enhanced infrastructure monitoring;
- re-implementation of internal permission to access files;
- engagement of external legal counsel to support the notification and compliance process; and
- commencement of a data mining exercise to comprehensively identify the information involved.

Protective Measures Offered to Employees

We have retained the assistance of Trans Union of Canada, Inc. (“TransUnion Canada”), one of Canada’s leading consumer reporting agencies, and arranged a twenty-four (24) month subscription to myTrueIdentity®, an online credit monitoring and identity restoration service, at no cost to you.

We encourage you to activate this service by enrolling online at: www.mytrueidentity.ca. To get started, enter the following activation code: **FMXTBSSZHTYF**

Already have an active myTrueIdentity account? Log in to your account to redeem your activation code and extend your subscription at: www.mytrueidentity.ca/login.

Please ensure your activation code is redeemed by January 31, 2027 to take advantage of the service.

Once you complete the online enrolment process, you’ll have access to the following features to help protect against identity theft and fraud:

- ✓ **Your TransUnion Canada credit report** – View your credit report, including available payment history and account activity, updated daily.
- ✓ **Your CreditVision® Risk Score** – Your credit score reflects the information in your TransUnion Canada credit report at a specific point in time.
- ✓ **Credit monitoring** – Receive email alerts about key changes on your TransUnion Canada credit report.
- ✓ **Educational tools and resources** – Learn more on mitigating identity theft and managing credit and get guidance if you become a victim of fraud.

- ✓ **Identity Restoration support** – Speak with restoration specialists who can answer questions about identity theft and assist you in restoring your identity if fraud occurs. This service includes up to \$1,000,000 of expense reimbursement insurance¹.
- ✓ **Dark Web Monitoring** – Scans the dark web and other online sources and provides notifications if the personal or financial information you provide is detected.

If you experience technical difficulties during the online enrolment process, please contact TransUnion Canada for support at 1-888-228-4939.

Steps You Can Take

We recommend the following measures to reduce the risk of harm:

- monitor your bank and credit card statements for any unauthorized transactions;
- check your credit file with the credit reporting agencies (Equifax, TransUnion);
- change your passwords, particularly if you use passwords similar to those for your work accounts;
- be vigilant against phishing attempts by email, telephone or text message; and
- enroll in the credit monitoring service offered by Neopharm.
- in addition to enrolling in the TransUnion credit monitoring service, place a fraud alert or credit freeze directly with Equifax Canada (www.equifax.ca or 1-800-465-7166) at no cost to you. Equifax and TransUnion are independent agencies and do not share fraud alerts or credit freezes with each other.

Contact Person

For any questions regarding this notice or to obtain more specific information about your personal situation, please contact Marie N'Dri or Josée Plouffe à rh@neoparmlabs.com.

Neopharm takes this incident very seriously and is committed to protecting the personal information of its employees.

Neopharm Labs Management

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