

Notice of Data Security Event

Date: August 5, 2026

August 5, 2026 – Yellow Corporation (“Yellow”) is issuing notice of a recent event that may impact the security of information related to certain individuals. We are providing information about the event, our response, and steps potentially affected individuals may take to help protect their information.

What Happened? On or about March 27, 2025, Yellow identified suspicious activity on its computer network. In response, we promptly started an investigation, with the assistance of third-party cybersecurity specialists, briefly took the systems offline, securely restored them from backups, and reviewed this matter further. During our review, we identified that certain files on the computer network were accessed and exfiltrated without permission by an unauthorized third party on March 27, 2025. After identifying the files that were involved, we undertook a comprehensive review of the files to determine what information was contained in them, and to whom the information related. The review was completed and the substantial majority of the information identified is for former Yellow employees.

What Information Was Involved? For various reasons, including due to the historical nature of the data involved, Yellow was not able to identify and/or sufficiently verify contact information for individuals that were impacted and is therefore issuing this notice. However, Yellow did identify that the affected information may include some of or all of the following: name, Social Security Number or Social Insurance Number, date of birth, driver’s license or state identification card number, passport number, other government issued identification card numbers, financial account number, payment card number, email account address and password, medical information, and health insurance information.

What We Are Doing. We take the confidentiality, privacy, and security of information very seriously. We responded promptly by taking steps to further secure our systems, commencing a comprehensive investigation, and implementing additional technical safeguards to mitigate the reoccurrence of this type of event. Following our review, we are providing this notification to ensure individuals are aware of this matter. Additionally, we are providing free resources and guidance to help protect information.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. To assist with this process, you may review the *Steps You Can Take To Help Protect Your Information* section below, which has free resources and guidance on how to monitor and protect personal information. We also encourage you to report promptly any suspicious activity to your credit card company, bank, healthcare/insurance provider, or other applicable institution.

For More Information. If you have questions about this matter, you may contact our dedicated assistance line at 833-289-4340, Monday through Friday from 9:00 am to 9:00 pm EST (excluding U.S. Holidays). Individuals may also write to us at Yellow Corporation, 11500 Outlook Street, Suite 400, Overland Park KS 66211.

Steps You Can Take To Help Protect Your Information (Canada)

Obtain a copy of your credit report: you may obtain a free copy of your credit report without signing up for a credit monitoring service by contacting the two Canadian credit reporting agencies:

Equifax Canada National Consumer Relations P.O. Box 190 Montreal, QC H1S 2Z2 www.consumer.equifax.ca/personal/contact-us/ 1-800-465-7166	TransUnion Canada TransUnion Consumer Relations Department P.O. Box 338, LCD1 Hamilton, ON L8L 7W2 https://www.transunion.ca/customer-support/contact-us 1-800-663-9980 1-877-713-3393 (Quebec residents)
--	--

Be cautious with communications: remain vigilant, as always, when engaging with any unsolicited or unexpected communications, particularly those that request personal information or that refer you to a webpage that asks for your personal information, even if that communication appears to come from a source that you know and trust.

Review your account statements and notify law enforcement of suspicious activity: remain vigilant, as always, to the possibility of fraud and identity theft by reviewing your financial statements and accounts regularly for any unauthorized activity.

If you believe you are the victim of identity theft or fraud or have reason to believe your personal information has been misused, it is generally recommended that you consider the following steps:

1. **File a complaint with the police** and ask for the case reference number and the officer's name and telephone number. If you obtain a copy of the police report, make sure it states your name and the information involved.
2. **Contact the Canadian Anti-Fraud Centre** at 1-888-495-8501 or on their website to report fraud or for advice and assistance about identity theft.
3. **Contact Canada's two national credit reporting agencies** to ask for a copy of your credit report. Review it for any suspicious activity and contact the agencies to discuss what can be done.
4. **Inform your bank and creditors** by phone and in writing about any irregularities you identify.
5. **Report any irregularities in your mail delivery to Canada Post**, such as open envelopes or missing financial statements or documents.
6. **Contact Service Canada** if you suspect that your Social Insurance Number is being used fraudulently. They will inform you of the required documents and provide you with help.

Place a credit freeze (Quebec and Ontario only): Quebec and Ontario residents can request, free of charge, a freeze on their credit file by contacting the two Canadian credit reporting agencies. This temporarily blocks the transmission of your information to companies or individuals who attempt to consult or modify your credit file.

Alert the CRA: you can place an alert with the Canada Revenue Agency by calling 1-800-959-8281.