Yellow Corporation Provides Notice of Data Event

Overland Park, KS – June 26, 2026. Yellow Corporation and its affiliated debtors and debtors-in-possession ("Yellow") under their jointly administered chapter 11 cases (Case No. 23-11069 (Bankr. D. Del. (CTG)) ("Yellow") is issuing notice of an event that may impact the security of information related to certain individuals.

On around March 27, 2025, Yellow identified suspicious activity on its computer network. In response, Yellow promptly launched 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 its review, Yellow identified that certain files on the computer network were accessed and exfiltrated without permission on March 27, 2025. After identifying the files that were involved, Yellow undertook a comprehensive review of the files to determine what information was contained in them, and to whom the information related.

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. However, Yellow did identify that the affected information may include some of or all of the following: name, Social Security 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, medical information, and health insurance information.

Yellow is notifying potentially affected individuals via this media release and by posting notice on its website. Yellow is also notifying relevant regulators where necessary. If individuals have questions about this matter, we have a dedicated assistance line with agents ready to answer their questions. Please contact our toll-free 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 visit www.myyellow.com or https://dm.epiq11.com/case/yellowcorporation/info for more information about this matter, or may write to Yellow at Yellow Corporation, 11500 Outlook Street, Suite 400, Overland Park KS 66211.

Notice of Data Security Event

Date: June 26, 2026

Yellow Corporation and its affiliated debtors and debtors-in-possession ("Yellow") under their jointly administered chapter 11 cases (Case No. 23-11069 (Bankr. D. Del. (CTG)) ("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 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? Due to the historical nature of the data involved, Yellow was not able to identify and/or sufficient 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, 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, 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

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax: www.equifax.com and 1-888-298-0045

Experian: www.experian.com and 1-888-397-3742
TransUnion: www.transunion.com and 1-833-799-5355
Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. To file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202;1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.