February 13, 2026

SUBSTITUTE NOTICE OF DATA BREACH

As previously described in our 8-K on August 18, 2025 and our subsequent SEC filings, Inotiv experienced a cybersecurity incident in early August 2025. While we currently have no indication that personal information has been misused, this notification provides details of the incident and our response, the resources we are making available to individuals whose personal information has been identified as potentially involved, and additional steps individuals can take if they believe their personal information was potentially involved.

What Happened?

On August 5, 2025, we detected unusual activity on certain Inotiv systems and promptly initiated an investigation. On August 8, 2025, we determined that this unusual activity was due to unauthorized actions by a threat actor. Our investigation determined that between approximately August 5-8, 2025, a threat actor gained unauthorized access to Inotiv's systems and may have acquired certain data.

Upon learning of the potential data acquisition, Inotiv took prompt action to identify and review the data and identify individuals whose personal information may have been involved. We subsequently determined that certain data may have been acquired by the threat actor during this incident, including personal information.

What Information Was Involved?

Inotiv maintains certain data related to current and former employees of Inotiv and their family members, as well as certain data related to other individuals who have interacted with Inotiv or companies it has acquired. Our review determined that the personal information potentially involved included names, Social Security numbers, tax identification numbers, driver's license numbers, other government-issued identification numbers or details, dates of birth, financial account information, payment card information, health insurance information, medical information, biometric data, passport information, digital signatures, and contact information, among other types of information.

What We Are Doing.

Upon detecting the unusual activity, we promptly took steps to contain it and launched an investigation with the support of external cybersecurity specialists. We also notified regulators and U.S. law enforcement. Notification was not delayed as a result of a law enforcement investigation.

We have notified individuals whose personal information was potentially involved via mail and email where such contact information was available, and have offered complimentary credit monitoring to these individuals. We are also providing this additional notification for the limited number of individuals whose information was potentially involved but for whom Inotiv could not locate valid contact information.

What You Can Do.

We recommend that individuals remain vigilant for incidents of fraud and identity theft, including by regularly reviewing and monitoring their credit history and credit reports to detect any errors and guard against any unauthorized transactions or activity. We also recommend that individuals closely monitor their account statements and notify their financial institution if they suspect any unauthorized activity. Please find below a **Reference Guide** regarding steps you can take to protect yourself against potential fraud and identity theft, including specific information for U.S. residents.

For More Information.

Please be assured that we have taken steps to address the incident and to further enhance our security measures to protect individuals' data. If you have any questions about this notice or the incident and believe your information may have been potentially involved, please feel free to contact us at (833) 745-1485 (U.S. residents, toll-free) or (214) 393-3323 (individuals outside the U.S.) Monday through Friday, from 8 am to 8 pm Central Time (excluding major U.S. holidays) or dataprivacymanager@inotiv.com. Please be prepared to provide engagement number B158971.

REFERENCE GUIDE

To protect against possible fraud, identity theft, or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. consumer reporting agencies and additional information about steps you can take to obtain a free credit report and place a fraud alert or credit freeze on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your state's Attorney General, or the U.S. Federal Trade Commission ("FTC").

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major consumer reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A
FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:
Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts one year but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a credit freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Pursuant to 15 U.S.C. § 1681c-1, you have a right to obtain a freeze on your credit report free of charge. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five (5) 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 (e.g., state driver's license or ID card, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you may be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the FTC for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th Street SW, Washington, DC 20024; telephone 1-877-382-4357; or http://www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General, or the FTC.

District of Columbia Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at the Office of the Attorney General, 400 6th Street NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.

Maryland Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or https://www.marylandattorneygeneral.gov/.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident.

North Carolina Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at 1-800-771-7755 or https://ag.ny.gov/. The Department of State Division of Consumer Protection can be contacted at 1-800-697-1220 or https://dos.ny.gov/.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or http://www.riag.ri.gov/. You may also file or obtain a police report by contacting local or state law enforcement agencies.