NOTICE OF DATA BREACH

TriZetto Provider Solutions ("TPS") recently experienced a cybersecurity incident that affected certain protected health information of certain of its healthcare provider customers' patients. TPS provides billing-related services to healthcare providers, such as hospitals, health systems, and physician practices.

This notice explains the incident, the measures TPS has taken in response, and the steps individuals can take for further protection.

What Happened?

On October 2, 2025, TPS became aware of suspicious activity within a web portal that some of TPS's healthcare provider customers use to access its systems. Upon discovering the incident, TPS quickly launched an investigation and took steps to mitigate the issue. TPS also engaged external cybersecurity experts and notified law enforcement.

TPS determined that, beginning in November 2024, an unauthorized actor began accessing some records related to insurance eligibility verification transactions that healthcare providers process to assess insurance coverage for treatment services they provide to patients. A thorough review of the affected data was conducted to identify what information was involved and the individuals to whom the data related.

What information was involved?

The affected data varied by individual and may have included the following information for patients and primary insureds: name, address, date of birth, Social Security number, health insurance member number (which, for some individuals, may be a Medicare beneficiary identifier), health insurer name, primary insured or dependent information, and other demographic, health, and health insurance information. The incident did not affect any payment card, bank account, or other financial information. At this time, TPS is not aware of any identity theft or fraud related to the use of any affected individual's information.

What TPS is doing?

After becoming aware of the incident, TPS immediately took additional protective measures to safeguard its systems and worked with leading cybersecurity experts to conduct a comprehensive investigation of the incident. TPS notified law enforcement and implemented additional security protocols designed to enhance the security of its services.

TPS notified affected providers beginning on December 9, 2025, and offered to make all legally required notices on their behalf. For those providers that accepted the offer, TPS is currently notifying affected individuals at their last known addresses.

TPS is offering affected individuals complementary identity monitoring services including credit monitoring, fraud consultation, and identity theft restoration services.

What can affected individuals do?

If you believe that you may have been affected by this incident and would like to enroll in credit monitoring services at no charge, click the activate now button on the right-hand side of the page or call the dedicated, toll-free call center at (844) 572-2725 between 8:00 a.m. and 5:30 p.m. Central Time, excluding major U.S. holidays.

In order for you to receive the Kroll services, you must enroll by May 8, 2026.

Although TPS has no evidence that any affected individual's information has been subject to identity theft or fraud, TPS encourages individuals to remain vigilant against incidents of identity theft and fraud, review account statements, and monitor their free credit reports for suspicious activity and to detect errors. Instructions and general information about identity theft protection are provided below.

TPS regrets that this incident occurred and any concern it may cause. TPS takes the confidentiality and security of personal information very seriously and will continue to take steps to prevent a similar incident from occurring in the future.

By clicking "Activate Now," I certify I believe I am potentially impacted by this incident.

To activate monitoring services for adults the age of 18 and over click here.

Adult Activate Now

To activate monitoring services for minors under the age of 18, click here.

Minor Activate Now

Activate Adult Identity Monitoring Services:

Single Bureau

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft. To receive credit services, you must be over the age of 18 and have

established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Activate Minor Identity Monitoring Services:

Minor Identity

Minor Identity Monitoring detects when names, aliases, or addresses become associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history. To activate services, a U.S. Social Security number and U.S. residential address is required.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Frequently Asked Questions

- Steps You Can Take To Help Protect Your Information

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.
Credit Reports. Under federal law, you are entitled to one free copy of your credit report

every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling 1-877-322-8228. You also may complete the Annual Credit Report Request Form available at https://www.annualcreditreport.com/manualRequestForm.action, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may contact the nationwide credit reporting agencies at:

- Equifax, P.O. Box 105788 Atlanta, GA 30348, www.equifax.com, 1-800-525-6285
- Experian, P.O. Box 9554 Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a security freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1- 202-727-3400, www.oag.dc.gov.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1- 888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888- 743-0023.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, 1-914-834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, https://ncdoj.gov, 1-877- 566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 1-401-274-4400 or file a police report by contacting 1-401-444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know

that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.