

NOTICE OF DATA PRIVACY EVENT

Updated: June 5, 2025

Frontier Central School District (“Frontier”) is providing notice of a data privacy event that occurred at one of its third-party vendors.

What Happened? Frontier hired InStream, LLC (“InStream”), a digitization company, to digitize for electronic storage certain microfilm/microfiche and paper personnel records of Frontier. InStream indicates that it became aware of performance issues impacting certain systems in InStream’s Buffalo office and immediately began an investigation. InStream states that its investigation determined that an unknown actor accessed certain systems in Instream’s Buffalo office between July 20, 2024 and July 25, 2024, and during this time files were copied.

As part of the investigation, InStream indicates that it conducted a thorough review of the files to determine what clients of Instream and information were involved, and to whom the information relates. Instream’s review concluded on or about April 23, 2025.

What Information Was Involved: Although the information varies by individual, the review identified the following types of information: name, address, date of birth, Social Security number, government-issued identification, financial account information, medical information, health insurance information, as well as other information contained in Frontier’s records.

What We Are Doing: Frontier takes this event very seriously and, once Frontier was notified by InStream of this data privacy event in late April 2025 following Instream’s investigation, Frontier moved quickly to understand the event’s scope and impact. Frontier’s investigation is ongoing.

Instream has indicated that its internal investigative actions included steps to access and secure the network, taking certain systems offline, reviewing the involved systems and files, notifying law enforcement, and notifying potentially involved clients and individuals as information became available. Instream also indicates that as part of its ongoing commitment to information security, Instream is reviewing and enhancing its existing policies, procedures, and security tools to reduce the likelihood of a similar event from occurring in the future.

Frontier is working with InStream to provide notice of this event to potentially impacted individuals identified in the review of Frontier’s records. In addition to this website notice, notices were mailed to individuals, where address information is available, and Instream provided notice of the data privacy event to the media. As an added precaution, potentially impacted individuals were provided access to complimentary credit monitoring services and resources to consider to protect personal information.

What You Can Do: You should remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, healthcare provider, financial institution and/or the company with which the account is maintained. Additional information and resources may be found below in the *Steps You Can Take to Protect Personal Information* section of this notice.

For More Information: To direct questions to Instream on this notice or if you believe you may be impacted by this event, you may contact Instream's dedicated assistance line at 833-931-7884. In addition, for questions directed to Frontier, you may contact William Bruton at wbruton@frontiercsd.org or 716-926-1798.

STEPS YOU CAN TAKE TO PROTECT PERSONAL 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 1-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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>.