



WAYNE, Pa. — October 26, 2026—[Frontline Education](#), a leading provider of administration software purpose-built for K-12, today announced that it has begun sending notification letters to individuals whose data was impacted in the August 2026 cybersecurity incident involving Frontline Central and School Health Management. The incident has been fully remediated. Frontline launched a webpage to provide additional information about the security incident.

What happened:

On August 14, 2026, our security team identified a vulnerability in a third-party software product we use that allowed unauthorized access to a portion of the environment beginning on August 14, 2026. We promptly investigated the issue with the assistance of an independent cybersecurity firm, remediated the vulnerability, engaged with law enforcement, and took steps to further reinforce the security of our systems. The last day of unauthorized activity was August 15. We remain committed to protecting the security of our customers' data and continuously strengthening our security practices.

What Personal Information was involved:

Frontline conducted a thorough and time-intensive analysis of the impacted files to determine what personal information they contained and to whom that information belongs. Although the information for each individual varies, we have determined that the following data elements were impacted: Social Security number, dates of birth, driver's license number, passport number, other government ID, Medicaid ID, Student ID.

What we are doing:

Frontline has notified affected school districts and, in cooperation with those districts, has begun notifying individuals whose personal information was affected via email or by letter sent via the U.S. Postal Service, as required and where available. The company is offering adults in the U.S. two years of credit monitoring and cyber monitoring for minors at no cost through TransUnion. The notices provide the nature of the information involved and contact details for the dedicated TransUnion call center established to assist with enrollment for eligible individuals and to address any inquiries related to the incident. Individual notifications were issued starting on or about October 26, 2026.

In addition to the comprehensive security measures the company had in place prior to the incident, it has taken steps to further safeguard its systems, including enhancing its security and monitoring controls. The company will continue to advance its IT security and data privacy controls to stay ahead of the ever-evolving threat landscape.

What you can do:

In addition to enrolling in the credit monitoring services being offered to eligible individuals whose data was impacted at no charge, the company encourages affected individuals to take additional precautions:

- Remain vigilant against threats of identity theft or fraud and regularly review and monitor account statements and credit histories for any signs of unauthorized transactions or activity.
- Individuals who suspect they are the victim of identity theft or fraud should contact their local police.

For more information:

Frontline has established a dedicated call center to answer questions about the cybersecurity event as well as the TransUnion services that we are offering to those whose personal data was impacted. If you have any questions, please call the TransUnion call center at 1-800-759-7279 from 8 a.m. to 8 p.m. ET Monday through Friday, excluding major U.S. holidays.