Orrick, Herrington & Sutcliffe LLP
401 Union Street
Suite 3300
Seattle, WA 98101-2668

+1 206 839 4300

orrick.com

Aravind Swaminathan

E aswaminathan@orrick.com
D +1 206 839 4340
F +1 206 839 4301

October 26, 2026

VIA U.S. POSTAL MAIL and EMAIL

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
ag@riag.ri.gov

RE: Notice of Data Security Event – Frontline Education

To Whom It May Concern:

I am writing on behalf of our law firm's client, Frontline Education ("Frontline"), a private company with its principal place of business at 550 E Swedesford Road, Suite 360, Wayne, PA 19087, to provide notice of a security event.

On August 14, 2026, Frontline's security team identified a vulnerability in a third-party software product it uses that allowed unauthorized access to a portion of Frontline's environment beginning August 14, 2026. Frontline 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. On September 23, 2026, Frontline determined the unauthorized actor acquired certain personal information of staff and students for a number of school districts located in Rhode Island.

Frontline has determined that the personal information of approximately 8,258 Rhode Island residents was affected in the incident. The affected data includes Social Security number, driver's license number, and Medicaid ID.

Frontline has issued a press release and posted information about this incident on its website.[1] Frontline has also established a dedicated call center to answer questions related to this incident. Individual notifications via e-mail and postal mail will begin October 26, 2026. Frontline is offering two years of complimentary credit monitoring services to adults and cyber monitoring services for minors. A sample individual notice is attached as Exhibit A.

[1] https://www.frontlineeducation.com/news/frontline-education-notice-of-data-breach/

While Frontline has a number of safeguards in place to protect personal information from unauthorized access, it is always working to further enhance security so it can stay ahead of this type of activity.

If your office requires any further information regarding this matter, please do not hesitate to contact me at +1 (206) 839 4340 or at aswaminathan@orrick.com.

Respectfully,

/s/ Aravind Swaminathan
Partner, Orrick Herrington & Sutcliffe LLP

EXHIBIT A

Frontline Education
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

October 26, 2026

Re: Notice of Data Breach

Dear [redacted]:

Frontline Education (the "Company") is a leading provider of K-12 school administration software, that works with [redacted]. Unfortunately, we are writing to inform you of a recent cybersecurity event affecting some of your personal information, which we process in connection with services we provide that school district. We deeply regret this incident and the concern it may cause. Please read this notice carefully as it provides up-to-date information on what happened and what we are doing.

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 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. We remain committed to protecting the security of our customers' data and continuously strengthening our security practices.

What Personal Information was involved:

The Company has been conducting a thorough and time-intensive analysis of the impacted files to determine what personal information they contained and to whom that information belongs. We have determined that your [redacted] were obtained.

What we are doing:

We are offering you at no cost a 24-month membership to TransUnion's credit monitoring. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: January 31, 2027 (Your code will not work after this date).
- Visit the TransUnion website to enroll.
- For Adults: www.mytrueidentity.com
- Provide your activation code (see attachment A)

You must enroll by January 31, 2027 to receive these services.

Please see Attachment A for additional details regarding these services.

Draft

In addition to the enterprise-wide security measures the Company had in place prior to the incident, we have taken steps to further safeguard our systems, including enhancing our security and monitoring controls. The Company will continue to advance its IT security and data privacy controls to stay ahead of an ever-evolving threat landscape.

What you can do:

In addition to enrolling in the credit monitoring being offered to you at no charge, we encourage you to take the following precautions:

- Remain vigilant against threats of identity theft or fraud and regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is contained in Attachment B.

For more information:

The Company has established a dedicated call center to answer questions about the cybersecurity event as well as the TransUnion services that we are offering to you. 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.

Sincerely,

Frontline Education
550 E Swedesford Road, Ste. 360
Wayne, PA 19087
(877) 765-5656

Draft

Puede encontrar una plantilla de esta carta en español, que no incluye los datos específicos suyos que se vieron afectados, en: www.frontline-transunion.com/Spanish

Attachment A – ADDITIONAL DETAILS REGARDING YOUR 24-MONTH TRANSUNION CREDIT MONITORING SERVICES

To activate your membership and start monitoring your personal information please follow the steps below:

For adults:

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to www.mytrueidentity.com and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Draft

Attachment B– MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. customers are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free +1 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR A SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below 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.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security 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. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or a security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 378-8228	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

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 those prior five (5) years;
5. Proof of current address such as a current utility bill or a telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission (FTC) for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357 or 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.

California residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft. The Attorney General can be contacted at Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Colorado Residents: The Attorney General can be contacted at the Office of the Attorney General, Colorado Department of Law, Ralph L. Carr Judicial Building, 1300 Broadway, 10th Floor, Denver, Colorado 80203; +1 (720) 508-6000 or https://coag.gov/.

Delaware Residents: The Attorney General can be contacted at Delaware Attorney General, Carvel State Office Building, 5th Floor, 820 N. French St., Wilmington, DE 19801, https://attorneygeneral.delaware.gov/, Telephone: 1-302-577-8500.

District of Columbia residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; +1 (202) 727-3400, oag@dc.gov and www.oag.dc.gov.

Florida residents: The Attorney General can be contacted at the Office of Attorney General of Florida, PL-01, The Capitol, Tallahassee, Florida, 32399-1050; +1 (866) 966-7226 or www.myfloridalegal.com.

Iowa residents: The Attorney General can be contacted at the Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319; +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky residents: The Attorney General can be contacted at the Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

Maryland residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023 or www.marylandattorneygeneral.gov.

Massachusetts residents: Under Massachusetts law, you have the right to obtain any police report filed in connection with the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Missouri Residents: The Attorney General can be contacted at the Attorney General Office of Missouri, Supreme Court Building, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, https://ago.mo.gov/, Telephone: 1-573-751-3321.

North Carolina residents: The Attorney General can be contacted at the Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400 or www.ncdoj.gov.

New Jersey Residents: The Attorney General can be contacted at the Office of the Attorney General – New Jersey State Division of Consumer Affairs, Richard J. Hughes Justice Complex, 25 Market Street, Trenton, New Jersey 08611, https://www.njoag.gov/, Telephone: 973-504-6200.

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.ftc.gov/system/files/ftc_gov/pdf/fcra-march-2026.pdf or www.ftc.gov.

New York residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; +1 (800)-771-7755 or www.ag.ny.gov.

Oregon residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Pennsylvania Residents: The Attorney General can be contacted at the Pennsylvania Office of the Attorney General, Strawberry Square, Harrisburg, PA 17120, https://www.attorneygeneral.gov/, Telephone: 1-800-441-2555.

Rhode Island residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400 or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.

Texas residents: The Attorney General can be contacted at the Office of the Attorney General, 300 W 15th St, Austin, Texas 78701; +1 (512) 463-2100 or www.texasattorneygeneral.gov.

Virginia Residents: The Attorney General can be contacted at the Office of the Attorney General of Virginia, 202 North Ninth Street, Richmond, VA 23219, https://www.oag.state.va.us/, Telephone: 804-786-2071.

Washington Residents: The Attorney General can be contacted at the Office of the Attorney General, 1125 Washington St. SE, P.O. Box 40100, Olympia, WA 98504-0100, https://www.atg.wa.gov/, Telephone: 1-360-753-6200.

For Arizona, California, District of Columbia, Iowa, Montana, North Carolina, Washington and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Draft

Puede encontrar una plantilla de esta carta en español, que no incluye los datos específicos suyos que se vieron afectados, en: www.frontline-transunion.com/Spanish